SUSE Linux Riferimento

www.novell.com

10.0 | 13.09.2005

Riferimento

Autori: Jörg Arndt, Stefan Behlert, Frank Bodammer, James Branam, Volker Buzek, Klara Cihlarova, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Thorsten Dubiel, Torsten Duwe, Thomas Fehr, Stefan Fent, Werner Fink, Kurt Garloff, Joachim Gleißner, Carsten Groß, Andreas Grünbacher, Berthold Gunreben, Franz Hassels, Andreas Jaeger, Jana Jaeger, Klaus Kämpf, Andi Kleen, Hubert Mantel, Lars Marowsky-Bree, Chris Mason, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Edith Parzefall, Peter Pöml, Thomas Renninger, Hannes Reinecke, Thomas Rölz, Heiko Rommel, Marcus Schäfer, Thomas Schraitle, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz

Per consigli e suggerimenti, scrivere a documentation@suse.de.

Sommario

Informazioni su questa guida

In questo manuale, destinato principalmente ad amministratori di sistema e utenti privati con conoscenze di base sull'amministrazione di un sistema, vengono fornite informazioni generali su SUSE Linux. Vengono illustrate alcune applicazioni di uso quotidiano e vengono descritti in dettaglio scenari di configurazione e installazione avanzati.

Scenari di distribuzione avanzati
Viene descritto come distribuire SUSE Linux in ambienti complessi.

Internet, Multimedia, Programmi per l'ufficio e Immagini
Vengono presentate le più importanti applicazioni utilizzate da un utente privato.

Mobilità
Viene fornita un'introduzione sull'uso di dispositivi portatili con SUSE Linux e viene descritto come configurare le varie opzioni per l'elaborazione wireless, la gestione del risparmio energetico e la gestione di profili.

Amministrazione
Viene descritto come rendere più sicuro SUSE Linux e come gestire i controlli dell'accesso al file system. Vengono inoltre presentate alcune importanti utility per gli amministratori di Linux.

Sistema
Vengono fornite un'introduzione ai componenti del sistema Linux e una descrizione più dettagliata della relative modalità di interazione.

Servizi
Viene descritto come configurare i vari servizi di rete e file inclusi in SUSE Linux.

1 Feedback

Saremo lieti di ricevere commenti e suggerimenti su questo manuale e sulla documentazione allegata al prodotto. Per inserire i commenti, utilizzare l'apposita funzionalità disponibile in fondo a ogni pagina della documentazione in linea oppure visitare il sito Web all'indirizzo http://www.novell.com/documentation/feedback.html.

2 Documentazione aggiuntiva

Per questo prodotto SUSE Linux sono disponibili altri manuali, accessibili in linea all'indirizzo `http://www.novell.com/documentation/` oppure nel sistema installato nel percorso `/usr/share/doc/manual/`:

Guida di riferimento
In questa guida vengono fornite informazioni di base su SUSE Linux. Una versione in linea di questo documento è disponibile all'indirizzo `http://www.novell.com/documentation/suse10/`.

Novell AppArmor Powered by Immunix 1.2 Installation and QuickStart Guide
In questa guida viene illustrata la procedura di installazione iniziale di *AppArmor*. Una versione in linea di questo documento è disponibile all'indirizzo `http://www.novell.com/documentation/apparmor/`.

Novell AppArmor Powered by Immunix 1.2 Administration Guide
In questa guida sono disponibili informazioni dettagliate sull'esecuzione di *AppArmor* nell'ambiente in uso. Una versione in linea di questo documento è disponibile all'indirizzo `http://www.novell.com/documentation/apparmor/`.

3 Convenzioni adottate nella documentazione

Nel presente manuale vengono utilizzate le convenzioni tipografiche riportate di seguito.

- `/etc/passwd`: nomi di file e directory
- *`placeholder`*: sostituire *`placeholder`* con il valore appropriato
- `PATH`: PERCORSO della variabile d'ambiente
- `ls`, `--help`: comandi, opzioni e parametri
- `user`: utenti e gruppi
- Alt, Alt + F1: un tasto da premere o una combinazione di tasti

- *File*, *File* → *Salva con nome*: voci di menu, pulsanti
- *Dancing Penguins* (Chapter Penguins, ↑*Reference*): riferimento a un capitolo in un altro libro.

4 Ringraziamenti

Gli sviluppatori di Linux collaborano a livello mondiale con grande impegno volontario per promuovere lo sviluppo di questo prodotto. A loro vanno i nostri sentiti ringraziamenti. Senza la loro dedizione questa distribuzione non sarebbe possibile. Ringraziamo inoltre Frank Zappa e Pawar. Un grazie speciale, naturalmente, a Linus Torvalds.

Buona lettura

Il team di SUSE

Parte I. Scenari di distribuzione avanzati

1 Installazione remota

È possibile installare SUSE Linux in molti modi diversi. Oltre alla procedura di installazione più comune mediante CD o DVD descritta nel Capitolo *Installazione con YaST* (↑Avvio), è possibile scegliere tra numerosi tipi di approccio basati sulla rete, nonché adottare un approccio completamente automatico per l'installazione di SUSE Linux.

Ogni metodo viene introdotto da due brevi elenchi di controllo. In uno sono elencati i prerequisiti per la procedura, mentre nell'altro viene illustrata la procedura di base. Vengono inoltre forniti ulteriori dettagli su tutte le tecniche utilizzate in questi scenari di installazione.

NOTA

Nelle sezioni seguenti, il sistema per l'installazione del nuovo SUSE Linux viene indicato come *sistema di destinazione* o *destinazione dell'installazione*. Il termine *origine dell'installazione* viene utilizzato per tutte le origini dei dati di installazione. Tra queste vi sono i supporti fisici, quali CD e DVD, e i server di rete che distribuiscono i dati di installazione all'interno della rete in uso.

1.1 Scenari di installazione remota

In questa sezione vengono introdotti gli scenari di installazione più comuni relativi alle installazioni remote. Per ogni scenario, verificare attentamente l'elenco dei prerequisiti e seguire la procedura corrispondente indicata. Se per un determinato passaggio sono necessarie istruzioni più dettagliate, seguire il collegamento fornito per ogni passaggio.

IMPORTANTE

La configurazione di X Window System non fa parte di alcun processo di installazione remota. Al termine dell'installazione, eseguire il login nel sistema di destinazione come root, immettere `init 3` e avviare SaX2 per configurare l'hardware grafico come descritto nella Sezione 35.1, «Configurazione di X11 con SaX2» (p. 553).

1.1.1 Installazione remota semplice tramite VNC - Configurazione di rete statica

Questo tipo di installazione richiede ancora un certo grado di accesso fisico al sistema di destinazione per l'avvio dell'installazione. L'installazione stessa viene interamente controllata mediante una workstation remota utilizzando VNC per la connessione al programma di installazione. L'interazione dell'utente è necessaria come per l'installazione manuale descritta nel Capitolo *Installazione con YaST* (↑Avvio).

Per questo tipo di installazione, verificare che i requisiti seguenti siano soddisfatti:

- Origine dell'installazione remota: NFS, HTTP, FTP oppure SMB con una connessione di rete funzionante.
- Sistema di destinazione con una connessione di rete funzionante.
- Sistema di controllo con una connessione di rete funzionante e un software visualizzatore VNC o un browser con supporto Java (Firefox, Konqueror, Internet Explorer oppure Opera).
- Supporto di avvio fisico (CD o DVD) per avviare il sistema di destinazione.
- Indirizzi IP statici validi precedentemente assegnati all'origine dell'installazione e al sistema di controllo.
- Indirizzo IP statico valido da assegnare al sistema di destinazione.

Per eseguire questo tipo di installazione, procedere come indicato di seguito:

1. Configurare l'origine dell'installazione come descritto nella Sezione 1.2, «Configurazione del server contenente le origini dell'installazione» (p. 31).

2 Avviare il sistema di destinazione mediante il primo CD o DVD del kit di supporti di SUSE Linux.

3 Quando viene visualizzata la schermata di avvio, utilizzare il prompt delle opzioni di avvio per impostare le opzioni VNC appropriate e l'indirizzo dell'origine dell'installazione. Questo passaggio è descritto dettagliatamente nella Sezione 1.4, «Avvio del sistema di destinazione per l'installazione» (p. 51).

   Il sistema di destinazione viene avviato in un ambiente basato su testo che fornisce l'indirizzo di rete e il numero di display al quale è possibile indirizzare l'ambiente grafico di installazione tramite un visualizzatore VNC o un browser. Le installazioni VNC vengono annunciate come OpenSLP e possono essere individuate tramite Konqueror in modalità `service://` o `slp://`.

4 Nella workstation di controllo, aprire il visualizzatore VNC oppure un browser Web e connettersi al sistema di destinazione come descritto nella Sezione 1.5.1, «Installazione VNC» (p. 56).

5 Eseguire l'installazione come descritto nel Capitolo *Installazione con YaST* (↑Avvio) .

   Dopo averlo riavviato, è necessario connettersi nuovamente al sistema di destinazione per la parte finale dell'installazione.

6 Completare l'installazione.

1.1.2 Installazione remota semplice tramite VNC - Configurazione di rete dinamica tramite DHCP

Questo tipo di installazione richiede ancora un certo grado di accesso fisico al sistema di destinazione per l'avvio dell'installazione. La configurazione di rete viene effettuata tramite DHCP (Dynamic Host Configuration Protocol). L'installazione stessa viene interamente controllata mediante una workstation remota utilizzando VNC per connettersi al programma di installazione, ma richiede ancora l'interazione dell'utente per il processo di configurazione effettivo.

Per questo tipo di installazione, verificare che i requisiti seguenti siano soddisfatti:

- Origine dell'installazione remota: NFS, HTTP, FTP oppure SMB con una connessione di rete funzionante.
- Sistema di destinazione con una connessione di rete funzionante.
- Sistema di controllo con una connessione di rete funzionante e un software visualizzatore VNC o un browser con supporto Java (Firefox, Konqueror, Internet Explorer oppure Opera).
- Supporto di avvio fisico (CD, DVD o un disco di avvio personalizzato) per avviare il sistema di destinazione.
- Server DHCP in esecuzione con fornitura degli indirizzi IP.

Per eseguire questo tipo di installazione, procedere come indicato di seguito:

1. Configurare l'origine dell'installazione come descritto nella Sezione 1.2, «Configurazione del server contenente le origini dell'installazione» (p. 31). Scegliere un server di rete SNFS, HTTP o FTP. Per un'origine dell'installazione SMB, vedere la Sezione 1.2.5, «Gestione di un'origine dell'installazione SMB» (p. 40).

2. Avviare il sistema di destinazione mediante il primo CD o DVD del kit di supporti di SUSE Linux.

3. Quando viene visualizzata la schermata di avvio, utilizzare il prompt delle opzioni di avvio per impostare le opzioni VNC appropriate e l'indirizzo dell'origine dell'installazione. Questo passaggio è descritto dettagliatamente nella Sezione 1.4, «Avvio del sistema di destinazione per l'installazione» (p. 51).

   Il sistema di destinazione viene avviato in un ambiente basato su testo che fornisce l'indirizzo di rete e il numero di display al quale è possibile indirizzare l'ambiente grafico di installazione tramite un visualizzatore VNC o un browser. Le installazioni VNC vengono annunciate come OpenSLP e possono essere individuate tramite Konqueror in modalità `service://` o `slp://`.

4. Nella workstation di controllo, aprire il visualizzatore VNC oppure un browser Web e connettersi al sistema di destinazione come descritto nella Sezione 1.5.1, «Installazione VNC» (p. 56).

5 Eseguire l'installazione come descritto nel Capitolo *Installazione con YaST* (↑Avvio) .

   Dopo averlo riavviato, è necessario connettersi nuovamente al sistema di destinazione per la parte finale dell'installazione.

6 Completare l'installazione.

1.1.3 Installazione remota tramite VNC - Avvio PXE e Wake on LAN

Questo tipo di installazione è completamente automatico. Il computer di destinazione viene avviato in remoto. L'interazione dell'utente è necessaria solo per l'installazione effettiva. Questo approccio è consigliato per la distribuzione intersito.

Per eseguire questo tipo di installazione, verificare che i requisiti seguenti siano soddisfatti:

- Origine dell'installazione remota: NFS, HTTP, FTP oppure SMB con una connessione di rete funzionante.
- Server TFTP.
- Server DHCP in esecuzione per la rete in uso.
- Sistema di destinazione abilitato all'avvio PXE, al networking e al Wake on LAN, collegato e connesso alla rete.
- Sistema di controllo con una connessione di rete funzionante e un software visualizzatore VNC o un browser con supporto Java (Firefox, Konqueror, Internet Explorer oppure Opera).

Per eseguire questo tipo di installazione, procedere come indicato di seguito:

1 Configurare l'origine dell'installazione come descritto nella Sezione 1.2, «Configurazione del server contenente le origini dell'installazione» (p. 31). Scegliere un server di rete NFS, HTTP, FTP oppure configurare un'origine dell'installazione SMB come descritto nella Sezione 1.2.5, «Gestione di un'origine dell'installazione SMB» (p. 40).

2 Configurare un server TFTP che contenga un'immagine di avvio che può essere ricavata dal sistema di destinazione. Questo passaggio viene descritto nella Sezione 1.3.2, «Configurazione di un server TFTP» (p. 43).

3 Configurare un server DHCP per la fornitura di indirizzi IP a tutti i computer e rivelare la posizione del server TFTP al sistema di destinazione. Questo passaggio viene descritto nella Sezione 1.3.1, «Configurazione di un server DHCP» (p. 41).

4 Preparare il sistema di destinazione per l'avvio PXE. Questo passaggio è descritto dettagliatamente nella Sezione 1.3.5, «Preparazione del sistema di destinazione per l'avvio PXE» (p. 50).

5 Iniziare il processo di avvio del sistema di destinazione tramite Wake on LAN. Questo passaggio viene descritto nella Sezione 1.3.7, «Wake on LAN» (p. 50).

6 Nella workstation di controllo, aprire l'applicazione visualizzatore VNC oppure un browser Web e connettersi al sistema di destinazione come descritto nella Sezione 1.5.1, «Installazione VNC» (p. 56).

7 Eseguire l'installazione come descritto nel Capitolo *Installazione con YaST* (↑Avvio) .

   Dopo averlo riavviato, è necessario connettersi nuovamente al sistema di destinazione per la parte finale dell'installazione.

8 Completare l'installazione.

1.1.4 Installazione remota semplice tramite SSH - Configurazione di rete statica

Questo tipo di installazione richiede ancora un certo grado di accesso fisico al sistema di destinazione per l'avvio dell'installazione e per la determinazione degli indirizzi IP della destinazione dell'installazione. L'installazione stessa viene interamente controllata mediante una workstation remota utilizzando SSH per la connessione al programma di installazione. L'interazione dell'utente è necessaria come per la normale installazione descritta nel Capitolo *Installazione con YaST* (↑Avvio).

Per questo tipo di installazione, verificare che i requisiti seguenti siano soddisfatti:

- Origine dell'installazione remota: NFS, HTTP, FTP oppure SMB con una connessione di rete funzionante.
- Sistema di destinazione con una connessione di rete funzionante.
- Sistema di controllo con una connessione di rete funzionante e un software visualizzatore VNC o un browser con supporto Java (Firefox, Konqueror, Internet Explorer oppure Opera).
- Supporto di avvio fisico (CD, DVD o un disco di avvio personalizzato) per il sistema di destinazione.
- Indirizzi IP statici validi precedentemente assegnati all'origine dell'installazione e al sistema di controllo.
- Indirizzo IP statico valido da assegnare al sistema di destinazione.

Per eseguire questo tipo di installazione, procedere come indicato di seguito:

1. Configurare l'origine dell'installazione come descritto nella Sezione 1.2, «Configurazione del server contenente le origini dell'installazione» (p. 31).
2. Avviare il sistema di destinazione mediante il primo CD o DVD del kit di supporti di SUSE Linux.
3. Quando viene visualizzata la schermata di avvio del sistema di destinazione, utilizzare il prompt delle opzioni di avvio per impostare i parametri appropriati per la connessione di rete, l'indirizzo dell'origine dell'installazione e l'abilitazione a SSH. Questo passaggio è descritto dettagliatamente nella Sezione 1.4.3, «Uso delle opzioni di avvio personalizzate» (p. 53).

   Il sistema di destinazione viene avviato in un ambiente basato su testo che fornisce l'indirizzo di rete e il numero di display al quale è possibile indirizzare l'ambiente grafico di installazione tramite un client SSH.
4. Nella workstation di controllo, aprire una finestra di terminale e connettersi al sistema di destinazione come descritto nella sezione chiamata «Connessione al programma di installazione» (p. 59).
5. Eseguire l'installazione come descritto nel Capitolo *Installazione con YaST* (↑Avvio) .

Dopo averlo riavviato, è necessario connettersi nuovamente al sistema di destinazione per la parte finale dell'installazione.

6 Completare l'installazione.

1.1.5 Installazione remota semplice tramite SSH - Configurazione di rete dinamica tramite DHCP

Questo tipo di installazione richiede ancora un certo grado di accesso fisico al sistema di destinazione per l'avvio dell'installazione e per la determinazione degli indirizzi IP della destinazione dell'installazione. L'installazione stessa viene interamente controllata mediante una workstation remota utilizzando VNC per connettersi al programma di installazione, ma richiede ancora l'interazione dell'utente per il processo di configurazione effettivo.

Per questo tipo di installazione, verificare che i requisiti seguenti siano soddisfatti:

- Origine dell'installazione remota: NFS, HTTP, FTP oppure SMB con una connessione di rete funzionante.
- Sistema di destinazione con una connessione di rete funzionante.
- Sistema di controllo con una connessione di rete funzionante e un software visualizzatore VNC o un browser con supporto Java (Firefox, Konqueror, Internet Explorer oppure Opera).
- Supporto di avvio fisico (CD o DVD) per avviare il sistema di destinazione.
- Server DHCP in esecuzione con fornitura degli indirizzi IP.

Per eseguire questo tipo di installazione, procedere come indicato di seguito:

1 Configurare l'origine dell'installazione come descritto nella Sezione 1.2, «Configurazione del server contenente le origini dell'installazione» (p. 31). Scegliere un server di rete SNFS, HTTP o FTP. Per un'origine dell'installazione SMB, vedere la Sezione 1.2.5, «Gestione di un'origine dell'installazione SMB» (p. 40).

2 Avviare il sistema di destinazione mediante il primo CD o DVD del kit di supporti di SUSE Linux.

3 Quando viene visualizzata la schermata di avvio del sistema di destinazione, utilizzare il prompt delle opzioni di avvio per passare i parametri appropriati per la connessione di rete, la posizione dell'origine dell'installazione e l'abilitazione a SSH. Vedere la Sezione 1.4.3, «Uso delle opzioni di avvio personalizzate» (p. 53) per istruzioni dettagliate sull'utilizzo di questi parametri.

   Il sistema di destinazione viene avviato in un ambiente basato su testo che fornisce l'indirizzo di rete al quale è possibile indirizzare l'ambiente grafico di installazione tramite un client SSH.

4 Nella workstation di controllo, aprire una finestra di terminale e connettersi al sistema di destinazione come descritto nella sezione chiamata «Connessione al programma di installazione» (p. 59).

5 Eseguire l'installazione come descritto nel Capitolo *Installazione con YaST* (↑Avvio) .

   Dopo averlo riavviato, è necessario connettersi nuovamente al sistema di destinazione per la parte finale dell'installazione.

6 Completare l'installazione.

1.1.6 Installazione remota tramite SSH - Avvio PXE e Wake on LAN

Questo tipo di installazione è completamente automatico. Il computer di destinazione viene avviato in remoto.

Per eseguire questo tipo di installazione, verificare che i requisiti seguenti siano soddisfatti:

- Origine dell'installazione remota: NFS, HTTP, FTP oppure SMB con una connessione di rete funzionante.
- Server TFTP.

- Server DHCP in esecuzione per la rete in uso, che fornisce un indirizzo IP statico all'host che deve essere installato.
- Sistema di destinazione abilitato all'avvio PXE, al networking e a Wake on LAN, collegato e connesso alla rete.
- Sistema di controllo con una connessione di rete funzionante e un client SSH.

Per eseguire questo tipo di installazione, procedere come indicato di seguito:

1. Configurare l'origine dell'installazione come descritto nella Sezione 1.2, «Configurazione del server contenente le origini dell'installazione» (p. 31). Scegliere un server di rete SNFS, HTTP o FTP. Per la configurazione di un'origine dell'installazione SMB, vedere la Sezione 1.2.5, «Gestione di un'origine dell'installazione SMB» (p. 40).
2. Configurare un server TFTP che contenga un'immagine di avvio che può essere ricavata dal sistema di destinazione. Questo passaggio viene descritto nella Sezione 1.3.2, «Configurazione di un server TFTP» (p. 43).
3. Configurare un server DHCP per la fornitura di indirizzi IP a tutti i computer e rivelare la posizione del server TFTP al sistema di destinazione. Questo passaggio viene descritto nella Sezione 1.3.1, «Configurazione di un server DHCP» (p. 41).
4. Preparare il sistema di destinazione per l'avvio PXE. Questo passaggio è descritto dettagliatamente nella Sezione 1.3.5, «Preparazione del sistema di destinazione per l'avvio PXE» (p. 50).
5. Iniziare il processo di avvio del sistema di destinazione tramite Wake on LAN. Questo passaggio viene descritto nella Sezione 1.3.7, «Wake on LAN» (p. 50).
6. Nella workstation di controllo, avviare il client VCN e connettersi al sistema di destinazione come descritto nella Sezione 1.5.2, «Installazione SSH» (p. 58).
7. Eseguire l'installazione come descritto nel Capitolo *Installazione con YaST* (↑Avvio) .

   Dopo il suo riavvio, è necessario connettersi nuovamente al sistema di destinazione per la parte finale dell'installazione.
8. Completare l'installazione.

1.2 Configurazione del server contenente le origini dell'installazione

In base al sistema operativo in esecuzione nel computer da utilizzare come origine dell'installazione di rete per SUSE Linux, vi sono varie opzioni per la configurazione del server. Il modo più semplice per configurare un server per l'installazione è di utilizzare YaST in SUSE LINUX Enterprise Server 9 o SUSE Linux 9.3 e versioni successive. Per le altre versioni di SUSE LINUX Enterprise Server o SUSE Linux, configurare l'origine dell'installazione manualmente.

SUGGERIMENTO

È anche possibile utilizzare un computer Microsoft Windows come server di installazione per la distribuzione di Linux. Per informazioni, vedere la Sezione 1.2.5, «Gestione di un'origine dell'installazione SMB» (p. 40).

1.2.1 Configurazione di un server di installazione con YaST

In YaST è disponibile uno strumento grafico per la creazione di origini dell'installazione di rete. Sono supportati server di installazione di rete HTTP, FTP e NFS.

1. Eseguire il login come root al computer che deve svolgere la funzione di server di installazione.
2. Avviare *YaST* → *Varie* → *Server di installazione*.
3. Selezionare il tipo di server (HTTP, FTP o NFS).

   Il servizio di server selezionato viene avviato automaticamente a ogni avvio del sistema. Se un servizio del tipo selezionato è già in esecuzione nel sistema in uso e si desidera configurarlo manualmente per il server, disattivare la configurazione automatica del servizio di server mediante *Non configurare alcun servizio di*

rete. In entrambi i casi, definire la directory in cui i dati dell'installazione dovrebbero essere disponibili nel server.

4 Configurare il tipo di server necessario.

Questo passaggio si riferisce alla configurazione automatica dei servizi di server e viene ignorato quando la configurazione automatica è disattivata. Definire un alias per la directory radice del server FTP o HTTP in cui si trovano i dati dell'installazione. L'origine dell'installazione verrà in seguito posizionata in `ftp://Server-IP/Alias/Name` (FTP) oppure in `http://Server-IP/Alias/Name` (HTTP). *`Name`* indica il nome dell'origine dell'installazione, descritta nel passaggio successivo. Se nel passaggio precedente è stato selezionato NFS, definire i caratteri jolly e le opzioni di esportazione. Il server NFS sarà accessibile in `nfs://Server-IP/Name` . Per informazioni su NFS e sulle esportazioni, vedere il Capitolo 42, *Condivisione di file system con NFS* (p. 673).

5 Configurare l'origine dell'installazione.

Prima di copiare i supporti di installazione nella destinazione corrispondente, definire il nome dell'origine dell'installazione, possibilmente mediante un'abbreviazione del prodotto e della versione facile da ricordare. In YaST è possibile fornire immagini ISO dei supporti invece delle copie dei CD di installazione. Se si sceglie questa soluzione, attivare la casella di controllo corrispondente e specificare il percorso di directory in cui è possibile trovare i file ISO localmente. In base al prodotto da distribuire mediante il server di installazione, potrebbero essere necessari CD aggiuntivi o CD con service pack per installare il prodotto completamente. Se si attiva *Prompt per CD aggiuntivi*, YaST chiede automaticamente all'utente di fornire questi supporti. Per annunciare in rete il server di installazione in uso tramite OpenSLP, attivare l'opzione corrispondente.

SUGGERIMENTO

Valutare la possibilità di annunciare l'origine dell'installazione tramite OpenSLP se la configurazione di rete in uso supporta tale opzione. In questo modo è possibile evitare di immettere il percorso di installazione della rete in ogni computer di destinazione. I sistemi di destinazione vengono avviati semplicemente utilizzando l'opzione di avvio tramite SLP (Service Location Protocol) e individuano l'origine dell'installazione di

rete senza ulteriori configurazioni. Per informazioni su questa opzione, vedere la Sezione 1.4, «Avvio del sistema di destinazione per l'installazione» (p. 51).

6 Caricare i dati di installazione.

Il passaggio più lungo nella configurazione di un server di installazione è la copia dei CD di installazione. Inserire i supporti in base alla sequenza richiesta da YaST e attendere la fine della procedura di copia. Quando le origini sono state interamente copiate, tornare alla panoramica delle origini dell'installazione esistenti e chiudere la configurazione selezionando *Fine*.

Il server di configurazione in uso è ora completamente configurato e pronto al servizio e viene avviato automaticamente a ogni avvio del sistema. Non sono necessari altri interventi. È necessario solo configurare e avviare il servizio manualmente in modo corretto se la configurazione automatica del servizio di rete selezionato con YaST è stata disattivata nel passaggio iniziale.

Per disattivare un'origine dell'installazione, selezionare *Modifica* nella panoramica per passare a un elenco di tutte le origini dell'installazione disponibili. Selezionare la voce da rimuovere, quindi selezionare *Cancella*. Questa procedura si riferisce solo alla disattivazione del servizio di server. I dati di installazione rimangono nella directory scelta. È tuttavia possibile rimuoverli manualmente.

Se il server di installazione in uso deve fornire dati di installazione a più di un prodotto o di una versione di prodotto, avviare il modulo YaST per il server di installazione e selezionare *Configura* nella panoramica delle origini dell'installazione esistenti per configurare la nuova origine dell'installazione.

1.2.2 Configurazione manuale di un'origine dell'installazione NFS

La configurazione di un'origine dell'installazione NFS è costituita essenzialmente da due passaggi. Nel primo passaggio, creare la struttura della directory che contiene i dati di installazione e copiare i supporti di installazione in tale struttura. In secondo luogo, esportare in rete la directory con i dati di installazione.

Per creare una directory con i dati di installazione, procedere come indicato di seguito:

1. Eseguire il login come radice.

2. Creare una directory destinata in seguito a contenere i dati di installazione e passare a questa directory. Ad esempio:

   ```
   mkdir install/product/productversion
   cd install/product/productversion
   ```

   Sostituire *product* con un'abbreviazione del nome del prodotto (in questo caso SUSE Linux) e *productversion* mediante una stringa contenente il nome e la versione del prodotto.

3. Per ogni CD contenuto nel kit di supporti, eseguire i comandi seguenti:

   a. Copiare l'intero contenuto del CD di installazione nella directory del server di installazione:

      ```
      cp -a /media/path_to_your_CD-ROM_drive .
      ```

      Sostituire *path_to_your_CD-ROM_drive* con il percorso effettivo al quale è indirizzato il CD o DVD in uso. In base al tipo di drive utilizzato nel sistema, può essere indicato `cdrom`, `cdrecorder`, `dvd` oppure `dvdrecorder`.

   b. Rinominare la directory con il numero del CD:

      ```
      mv path_to_your_CD-ROM_drive CDx
      ```

      Sostituire *x* con il numero effettivo del CD in uso.

Per esportare le origini dell'installazione tramite NFS utilizzando YaST, procedere come indicato di seguito:

1. Eseguire il login come radice.

2. Avviare *YaST → Servizi di rete → Server NFS*.

3. Selezionare *Avvia il server NFS* e *Apri porta nel Firewall*, quindi fare clic su *Avanti*.

4. Selezionare *Aggiungi directory* e immettere il percorso della directory che contiene i dati di installazione, in questo caso */productversion*.

5 Selezionare *Aggiungi host* e immettere i nomi host del computer nel quale esportare i dati di installazione. Invece di specificare i nomi host, è possibile utilizzare caratteri jolly, intervalli di indirizzi di network o semplicemente il nome di dominio della rete in uso. Immettere le opzioni di esportazione appropriate oppure lasciare quelle di default, che funzionano correttamente nella maggior parte delle configurazioni. Per ulteriori informazioni sulla sintassi utilizzata per l'esportazione delle condivisioni NFS, leggere la documentazione relativa a `export`.

6 Fare clic su *Fine*.

Il server NFS che contiene le origini dell'installazione di SUSE Linux viene avviato e integrato automaticamente nel processo di avvio.

Se si preferisce esportare manualmente le origini dell'installazione tramite NFS invece di utilizzare il modulo YaST per il server NFS, procedere come indicato di seguito:

1 Eseguire il login come radice.

2 Aprire il file `/etc/exports` e immettere la riga seguente:

```
/productversion *(ro,root_squash,sync)
```

In questo modo la directory `/productversion` viene esportata in un host che faccia parte di questa rete o in un host che possa essere connesso a questo server. Per limitare l'accesso a questo server, utilizzare maschere di rete o nomi di dominio al posto del carattere jolly generico `*`. Per informazioni, vedere la documentazione relativa a `export`. Salvare e uscire da questo file di configurazione.

3 Per aggiungere il servizio NFS all'elenco di server avviati durante l'avvio del sistema, eseguire i comandi seguenti:

```
insserv /etc/init.d/nfsserver
```

```
insserv /etc/init.d/portmap
```

4 Avviare il server NFS utilizzando il comando seguente:

```
rcnfsserver start
```

Se si desidera modificare la configurazione del server NFS successivamente, modificare il file di configurazione e riavviare il daemon NFS mediante `rcnfsserver restart`.

L'annuncio del server NFS tramite OpenSLP rende il suo indirizzo noto a tutti i client della rete in uso.

1. Eseguire il login come radice.
2. Immettere la directory `/etc/slp.reg.d/`.
3. Creare un file di configurazione `install.suse.nfs.reg` contenente le righe seguenti:

   ```
   # Register the NFS Installation Server
   service:install.suse:nfs://$HOSTNAME/path_instsource/CD1,en,65535
   description=NFS Installation Source
   ```

   Sostituire *`path_instsource`* con il percorso effettivo dell'origine dell'installazione nel server in uso.
4. Salvare il file di configurazione e avviare il daemon OpenSLP mediante il comando seguente:

   ```
   rcslpd start
   ```

Per ulteriori informazioni su OpenSLP, consultare la documentazione relativa ai pacchetti in `/usr/share/doc/packages/openslp/` o vedere il Capitolo 39, *Servizi SLP in rete* (p. 639).

1.2.3 Configurazione manuale di un'origine dell'installazione FTP

La creazione di un'origine dell'installazione FTP è molto simile alla creazione di un'origine dell'installazione NFS. Anche le origini dell'installazione FTP possono essere annunciate in rete tramite OpenSLP.

1. Creare una directory contenente le origini dell'installazione come descritto nella Sezione 1.2.2, «Configurazione manuale di un'origine dell'installazione NFS» (p. 33).

2. Configurare il server FTP per la distribuzione dei contenuti della directory di installazione in uso:

   a. Eseguire il login come root e installare il pacchetto `pure-ftpd` (un server FTP pulito) utilizzando il programma di gestione dei pacchetti YaST.

   b. Immettere la directory radice del server FTP:

      ```
      cd /srv/ftp
      ```

   c. Creare una sottodirectory contenente le origini dell'installazione nella directory radice di FTP:

      ```
      mkdir instsource
      ```

      Sostituire *`instsource`* con il nome del prodotto.

   d. Copiare il contenuto di tutti i CD di installazione nella directory radice del server FTP. Questa procedura è simile a quella descritta nella Sezione 1.2.2, «Configurazione manuale di un'origine dell'installazione NFS» (p. 33), al Passo 3 (p. 34)).

      In alternativa, montare i contenuti dell'archivio di installazione già esistente nell'ambiente di modifica radice del server FTP:

      ```
      mount --bind
      path_to_instsource /srv/ftp/instsource
      ```

      Sostituire *`path_to_instsource`* e *`instsource`* con i valori corrispondenti alla configurazione in uso. Se si desidera che questa sostituzione sia permanente, aggiungerla a `/etc/fstab`.

e Avviare pure-ftpd:

```
pure-ftpd &
```

3 Annunciare l'origine dell'installazione tramite OpenSLP, se supportato dalla configurazione di rete in uso:

a Creare un file di configurazione denominato `install.suse.ftp.reg` in `/etc/slp/reg.d/`, contenente le righe seguenti:

```
 # Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/srv/ftp/instsource/CD1,en,65535
description=FTP Installation Source
```

Sostituire *`instsource`* con il nome effettivo della directory dell'origine dell'installazione nel server in uso. La riga `service:` deve essere immessa come un'unica riga continua.

b Salvare il file di configurazione e avviare il daemon OpenSLP mediante il comando seguente:

```
rcslpd start
```

1.2.4 Configurazione manuale di un'origine dell'installazione HTTP

La creazione di un'origine dell'installazione HTTP è molto simile alla creazione di un'origine dell'installazione NFS. Anche le origini dell'installazione HTTP possono essere annunciate in rete tramite OpenSLP.

1 Creare una directory contenente le origini dell'installazione come descritto nella Sezione 1.2.2, «Configurazione manuale di un'origine dell'installazione NFS» (p. 33).

2 Configurare il server HTTP per la distribuzione dei contenuti della directory di installazione in uso:

a Eseguire il login come root e installare il pacchetto `apache2` utilizzando il programma di gestione dei pacchetti YaST.

b Immettere la directory radice del server HTTP (`/srv/www/htdocs`) e creare una sottodirectory per contenere le origini dell'installazione:

```
mkdir instsource
```

Sostituire *`instsource`* con il nome del prodotto.

c Creare un collegamento simbolico dalla posizione delle origini dell'installazione nella directory radice del server Web (`/srv/www/htdocs`):

```
ln -s /path_instsource /srv/www/htdocs/instsource
```

d Modificare il file di configurazione del server HTTP `/etc/apache2/default-server.conf` in modo che segua i collegamenti simbolici. Sostituire la riga seguente:

```
Options None
```

con

```
Options Indexes FollowSymLinks
```

e Riavviare il server HTTP mediante `rcapache2 restart`.

3 Annunciare l'origine dell'installazione tramite OpenSLP, se supportato dalla configurazione di rete in uso:

a Creare un file di configurazione denominato `install.suse.http.reg` in `/etc/slp/reg.d/`, contenente le righe seguenti:

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/srv/www/htdocs/instsource/CD1/,en,65535
description=HTTP Installation Source
```

Sostituire *`path_to_instsource`* con il percorso effettivo dell'origine dell'installazione nel server in uso. La riga `service:` deve essere immessa come un'unica riga continua.

b Salvare il file di configurazione e avviare il daemon OpenSLP mediante il comando `rcslpd restart`.

1.2.5 Gestione di un'origine dell'installazione SMB

L'uso di SMB (Samba) consente di importare le origini dell'installazione da un server Microsoft Windows e avviare la distribuzione di Linux anche senza nessun computer Linux.

Per configurare una condivisione Windows esportata contenente le origini dell'installazione di SUSE Linux, procedere come indicato di seguito:

1. Eseguire il login nel computer Windows in uso.
2. Avviare Esplora risorse e creare una nuova cartella che dovrà contenere tutto l'albero di installazione e nominarlo, ad esempio, `INSTALL`.
3. Esportare questa condivisione seguendo la procedura indicata nella documentazione Windows.
4. Immettere questa condivisione e creare una sottodirectory denominata *`product`*. Sostituire quindi *`product`* con il nome effettivo del prodotto (in questo caso SUSE Linux).
5. Copiare ogni CD di SUSE Linux in cartelle separate e nominarle `CD1`, `CD2`, `CD3` e così via.
6. Immettere la directory iniziale della condivisione esportata (in questo esempio `INSTALL`) e copiare i file e le cartelle seguenti da *`product`*`/CD1` nella cartella seguente: `content`, `media.1`, `control.xml` e `boot`.
7. Creare una nuova cartella in `INSTALL` e denominarla `yast`.
8. Immettere la cartella `yast` e creare i file `order` e `instorder`.
9. Aprire il file `order` e immettere la riga seguente:

   ```
   /NLD/CD1 smb://user:password@hostname/productCD1
   ```

   Sostituire *`user`* con il nome utente utilizzato nel computer Windows oppure utilizzare `Guest` per abilitare l'accesso a questa condivisione come ospite. Sostituire *`password`* con la password di accesso o con qualsiasi altra stringa

per l'accesso come ospite. Sostituire *hostname* con il nome di rete del computer Windows.

- Aprire il file `instorder` e aggiungere la riga seguente:

  `/product/CD1`

Per utilizzare una condivisione SMB montata, procedere come indicato di seguito:

1. Avviare la destinazione dell'installazione.
2. Selezionare *Installazione*.
3. Premere F4 per una selezione di origini dell'installazione.
4. Scegliere SMB e immettere il nome del computer Windows o l'indirizzo IP, il nome della condivisione (in questo esempio `INSTALL`), il nome utente e la password.

   Dopo aver premuto Enter, YaST verrà avviato automaticamente e sarà possibile eseguire l'installazione.

1.3 Preparazione dell'avvio del sistema di destinazione

In questa sezione vengono illustrate le attività di configurazione necessarie per scenari di avvio complessi. Vengono presentati esempi di configurazione pronti all'uso per DHCP, avvio PXE, TFTP e Wake on LAN.

1.3.1 Configurazione di un server DHCP

La configurazione di un server DHCP in SUSE Linux viene eseguita mediante la modifica manuale dei file di configurazione corrispondenti. In questa sezione viene illustrata l'estensione di una configurazione di un server DHCP esistente per fornire i dati necessari per il servizio in ambiente TFTP, PXE e WOL.

Configurazione manuale di un server DHCP

Oltre a fornire un'allocazione di indirizzo automatica ai client della rete in uso, il server DHCP annuncia l'indirizzo IP del server TFTP e il file che deve essere ricavato dalle routine di installazione nel computer di destinazione.

1. Eseguire il login come root nel computer che ospita il server DHCP.

2. Aggiungere le righe seguenti al file di configurazione del server DHCP in uso in `/etc/dhcpd.conf`:

   ```
   group {
     # PXE related stuff
     #
     # "next server" defines the tftp server that will be used
     next server ip_tftp_server:
     #
     # "filename" specifies the pxelinux image on the tftp server
     # the server runs in chroot under /srv/tftpboot
     filename  "pxelinux.0";
   }
   ```

   Sostituire *`ip_of_the_tftp_server`* con l'indirizzo IP effettivo del server TFTP.

   Per ulteriori informazioni sulle opzioni disponibili in `dhcpd.conf`, vedere la documentazione relativa a `dhcpd.conf`.

3. Riavviare il server DHCP eseguendo il comando `rcdhcpd restart`.

Se si prevede di utilizzare SSH per il controllo remoto di un'installazione PXE e Wake on LAN, specificare esplicitamente l'indirizzo IP che dovrebbe essere fornito alla destinazione dell'installazione da DHCP. A tale scopo, modificare la configurazione DHCP precedentemente indicata in base all'esempio seguente:

```
group {
  # PXE related stuff
  #
  # "next server" defines the tftp server that will be used
  next server ip_tftp_server:
  #
  # "filename" specifies the pxelinux image on the tftp server
  # the server runs in chroot under /srv/tftpboot
  filename "pxelinux.0";
  host test { hardware ethernet mac_address;
```

```
        fixed-address some_ip_address; }
}
```

L'istruzione host introduce il nome host della destinazione dell'installazione. Per associare il nome host e l'indirizzo IP a un host specifico, è necessario conoscere e specificare l'indirizzo hardware (MAC) del sistema. Sostituire tutte le variabili utilizzate in questo esempio con i valori effettivi che corrispondono all'ambiente in uso.

Dopo aver riavviato il server DHCP, viene fornito un indirizzo IP statico per l'host specificato che consente la connessione al sistema tramite SSH.

1.3.2 Configurazione di un server TFTP

La configurazione di un server TFTP può essere eseguita sia mediante YaST, sia manualmente in qualsiasi sistema operativo Linux che supporta xinetd e tftp. Il server TFTP fornisce l'immagine di avvio al sistema di destinazione quando questo viene avviato e invia una richiesta per l'immagine.

Configurazione di un server TFTP mediante YaST

1. Eseguire il login come radice.
2. Avviare *YaST* → *Servizi di rete* → *Server TFTP* e installare il pacchetto necessario.
3. Fare clic su *Abilita* per verificare se il server è stato avviato e incluso nelle routine di avvio. Non sono necessarie ulteriori azioni da parte dell'utente per garantire che xinetd esegua tftpd al momento dell'avvio.
4. Fare clic su *Apri porta nel Firewall* per aprire la porta corrispondente nel firewall in esecuzione nel computer in uso. Se nel server in uso non vi sono firewall in esecuzione, questa opzione non è disponibile.
5. Fare clic su *Sfoglia* per esplorare la directory dell'immagine di avvio.

   La directory di default `/tftpboot` viene creata e selezionata automaticamente.
6. Fare clic su *Fine* per applicare le impostazioni desiderate e avviare il server.

Configurazione manuale di un server TFTP

1. Eseguire il login come root e installare i pacchetti `tftp` e `xinetd`.
2. Se non sono disponibili, creare le directory `/srv/tftpboot` e `/srv/tftpboot/pxelinux.cfg`.
3. Aggiungere i file corrispondenti necessari per l'immagine di avvio come descritto nella Sezione 1.3.3, «Avvio PXE» (p. 44).
4. Modificare la configurazione di xinetd in `/etc/xinetd.d/` per verificare che il server tftp venga eseguito all'avvio:
   a. Se non esiste, creare un file denominato `tftp` in questa directory mediante il comando `touch tftp`. Quindi eseguire `chmod 755 tftp`.
   b. Aprire il file `tftp` e aggiungere le righe seguenti:

```
service tftp
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /tftpboot
        disable                 = no
}
```

   c. Salvare il file e riavviare xinetd mediante il comando `rcxinetd restart`.

1.3.3 Avvio PXE

Alcune informazioni tecniche generali, nonché le specifiche di PXE complete sono disponibili nel documento Preboot Execution Environment (PXE) Specification (ftp://download.intel.com/labs/manage/wfm/download/pxespec.pdf).

1 Passare alla directory dell'archivio di installazione in uso e copiare i file `linux`, `initrd`, `message` e `memtest` nella directory `/srv/tftpboot` immettendo quanto indicato di seguito:

```
cp -a boot/loader/linux boot/loader/initrd
      boot/loader/message boot/loader/memtest /srv/tftpboot
```

2 Installare il pacchetto `syslinux` direttamente dai CD o dai DVD di installazione mediante YaST.

3 Copiare il file `/usr/share/syslinux/pxelinux.0` nella directory `/srv/tftpboot` immettendo quanto indicato di seguito:

```
cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot
```

4 Passare alla directory dell'archivio di installazione in uso e copiare il file `isolinux.cfg` in `/srv/tftpboot/pxelinux.cfg/default` immettendo quanto indicato di seguito:

```
cp -a boot/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default
```

5 Modificare il file `/srv/tftpboot/pxelinux.cfg/default` e rimuovere le righe che iniziano con `gfxboot`, `readinfo` e `framebuffer`.

6 Inserire le voci seguenti nelle righe aggiuntive delle etichette di default `failsafe` e `apic`:

`insmod=e100`
Mediante questa voce, il modulo kernel per una scheda di rete Intel 100MBit/s viene caricato nei client PXE. Questa voce dipende dall'hardware del client e deve essere adattata di conseguenza. Nel caso di una scheda di rete Broadcom GigaBit, questa voce deve corrispondere a `insmod=bcm5700`.

`netdevice=eth0`
Questa voce definisce l'interfaccia di rete del client che deve essere utilizzata per l'installazione di rete. È necessario soltanto che il client sia dotato di più schede di rete e che sia adattato di conseguenza. Nel caso di una singola scheda di rete, questa voce può essere omessa.

`install=nfs://`*`ip_instserver`*`/`*`path_instsource`*`/CD1`
Questa voce definisce il server NFS e l'origine dell'installazione per l'installazione del client. Sostituire *`ip_instserver`* con l'indirizzo IP

effettivo del server di installazione in uso. Sostituire *path_instsource* con il percorso effettivo delle origini dell'installazione. Le origini HTTP, FTP o SMB vengono indirizzate in modo simile, ad eccezione del prefisso di protocollo, che deve essere `http`, `ftp` oppure `smb`.

IMPORTANTE

Se è necessario passare altre opzioni di avvio alle routine di installazione, quali i parametri di avvio SSH o VNC, aggiungerli alla voce `install`. Una panoramica dei parametri e alcuni esempi sono disponibili nella Sezione 1.4, «Avvio del sistema di destinazione per l'installazione» (p. 51).

Di seguito viene illustrato il file di esempio `/srv/tftpboot/pxelinux.cfg/default`. Modificare il prefisso di protocollo per l'origine dell'installazione in modo che corrisponda alla configurazione di rete in uso e specificare il metodo di connessione preferito al programma di installazione mediante l'aggiunta delle opzioni `vnc` e `vncpassword` o `ssh` e `sshpassword` alla voce `install`. Le righe separate da \ devono essere immesse come un'unica riga continua senza interruzione di riga e senza \.

```
default linux

# default
label linux
  kernel linux
     append initrd=initrd ramdisk_size=65536 insmod=e100 \
     install=nfs://ip_instserver/path_instsource/product

# failsafe
label failsafe
  kernel linux
  append initrd=initrd ramdisk_size=65536 ide=nodma apm=off acpi=off \
  insmod=e100 install=nfs://ip_instserver/path_instsource/product

# apic
label apic
  kernel linux
  append initrd=initrd ramdisk_size=65536 apic insmod=e100 \
  install=nfs://ip_instserver/path_instsource/product

# manual
label manual
  kernel linux
  append initrd=initrd ramdisk_size=65536 manual=1
```

```
# rescue
label rescue
  kernel linux
  append initrd=initrd ramdisk_size=65536 rescue=1

#  memory test
label memtest
  kernel memtest

# hard disk
label harddisk
  kernel
  linux append SLX=0x202

implicit     0
display      message
prompt       1
timeout      100
```

Sostituire *ip_instserver* e *path_instsource* con i valori utilizzati nella configurazione.

La sezione seguente rappresenta un breve riferimento alle opzioni PXELINUX utilizzate in questa configurazione. È possibile trovare ulteriori informazioni sulle opzioni disponibili nella documentazione del pacchetto `syslinux` in `/usr/share/doc/packages/syslinux/`.

1.3.4 Opzioni di configurazione di PXELINUX

Le opzioni elencate di seguito sono solo una parte di tutte le opzioni disponibili per il file di configurazione di PXELINUX.

Opzioni* DEFAULT *kernel

Consente di impostare la riga di comando del kernel di default. Se PXELINUX viene avviato automaticamente, agisce come se le voci che seguono DEFAULT fossero state digitate al prompt di avvio, ad eccezione dell'opzione auto che viene aggiunta automaticamente, indicando un avvio automatico.

Se non è presente il file di configurazione o in esso non è presente alcuna voce DEFAULT, per default il nome del kernel è «linux» senza opzioni.

Opzioni APPEND

Consente di aggiungere una o più opzioni alla riga di comando del kernel. Queste vengono aggiunte sia per l'avvio automatico, sia per quello manuale. Le opzioni vengono aggiunte all'inizio della riga di comando del kernel e solitamente possono essere ignorate dalle opzioni del kernel immesse esplicitamente.

***Opzioni* LABEL *label* KERNEL *image* APPEND**

Indica che se *label* viene immesso come kernel da avviare, PXELINUX deve invece eseguire *image* e le opzioni APPEND specificate devono essere utilizzate al posto di quelle specificate nella sezione generale del file prima del primo comando LABEL. L'impostazione di default di *image* è la stessa di *label* e, se non viene fornita alcuna opzione APPEND, per default viene utilizzata la voce generale, se presente. Sono ammesse fino a 128 voci LABEL.

Si noti che GRUB utilizza la sintassi seguente:

```
title mytitle
  kernel my_kernel
       my_kernel_options
  initrd myinitrd
```

mentre PXELINUX utilizza la sintassi seguente:

```
label mylabel
  kernel mykernel
  append myoptions
```

Le etichette vengono modificate come se fossero nomi di file e devono essere univoche dopo essere state modificate. Le due etichette «v2.1.30» e «v2.1.31», ad esempio, non sarebbero distinguibili in PXELINUX poiché entrambe vengono modificate e risultano nello stesso nome file DOS.

Non è necessario che il kernel sia un kernel Linux, può anche essere un settore di avvio o un file COMBOOT.

APPEND -

Indica che non vi sono aggiunte. APPEND seguito da un singolo trattino come argomento in una sezione LABEL può essere utilizzato per ignorare l'opzione APPEND generale.

LOCALBOOT *type*

In PXELINUX, se si specifica LOCALBOOT 0 invece dell'opzione KERNEL, viene chiamata questa etichetta e viene avviato il disco locale invece del kernel.

Argomento	Descrizione
0	Consente di eseguire un avvio normale.
4	Consente di eseguire un avvio locale mediante Universal Network Driver Interface (UNDI) ancora residente in memoria.
5	Consente di eseguire l'avvio locale mediante lo stack PXE completo, incluso il driver UNDI, ancora residente in memoria.

Tutti gli altri valori non sono definiti. Se non si conoscono gli stack UNDI o PXE, specificare `0`.

TIMEOUT *time-out*

Indica il tempo di attesa al prompt di avvio prima dell'avvio automatico, espresso in unità di 1/10 di secondo. Il timeout viene annullato non appena l'utente digita qualsiasi testo sulla tastiera, in base al presupposto che l'utente completi il comando iniziato. Un valore di timeout pari a zero disabilita completamente il timeout. Questa è anche l'impostazione di default.

Il valore massimo di timout possibile è 35996 (poco meno di un'ora).

PROMPT *flag_val*

Se `flag_val` è 0, il prompt di avvio viene visualizzato solo se vengono premuti i tasti Shift o Alt oppure se si imposta Bloc Maiusc o Bloc Scorr. Questa è l'impostazione di default. Se `flag_val` è 1, il prompt di avvio viene sempre visualizzato.

```
F2  filename
F1  filename
..etc...
F9  filename
F10 filename
```

Consente di visualizzare il file indicato sullo schermo quando viene premuto un tasto funzione al prompt di avvio. Può essere utilizzato per implementare la Guida in linea relativa al preavvio, presumibilmente per le opzioni della riga di comando del kernel. Per la compatibilità con versioni precedenti, è possibile inoltre immettere F10 come F0. Si noti che non esiste attualmente alcun modo per associare i nomi file a F11 e F12.

1.3.5 Preparazione del sistema di destinazione per l'avvio PXE

Preparare il BIOS del sistema per l'avvio PXE includendo l'opzione PXE nell'ordine di avvio del BIOS.

AVVERTIMENTO

Non posizionare l'opzione PXE all'inizio dell'opzione di avvio del disco rigido nel BIOS, altrimenti il sistema cercherà di reinstallarsi a ogni avvio.

1.3.6 Preparazione del sistema di destinazione per Wake on LAN

Con Wake on LAN (WOL) è necessario che l'opzione BIOS corrispondente sia abilitata prima dell'installazione. Trascrivere inoltre l'indirizzo MAC del sistema di destinazione. Questi dati sono indispensabili per avviare Wake on LAN.

1.3.7 Wake on LAN

Con Wake on LAN è possibile accendere un computer mediante uno speciale pacchetto di rete che viene inviato con l'indirizzo MAC del computer. Poiché ogni computer dispone di un identificatore MAC univoco, non si corre il rischio di accendere accidentalmente il computer sbagliato.

IMPORTANTE

Se il computer di controllo non si trova nello stesso segmento di rete della destinazione dell'installazione che si desidera attivare, configurare le richieste WOL da inviare come multidiffusioni oppure controllare un computer in remoto in quel segmento di rete per agire come mittente delle richieste.

1.3.8 Wake on LAN manuale

1. Eseguire il login come radice.
2. Start *YaST* → *Installare/togliere i pacchetti* e installare il pacchetto `netdiag`.
3. Aprire un terminale e immettere il comando seguente come root per attivare la destinazione:

   ```
   ether-wake mac_of_target
   ```

   Sostituire *`mac_of_target`* con l'indirizzo MAC effettivo della destinazione.

1.4 Avvio del sistema di destinazione per l'installazione

In generale vi sono due diversi modi di personalizzare il processo di avvio per l'installazione, oltre a quelli menzionati nella Sezione 1.3.7, «Wake on LAN» (p. 50) e nella Sezione 1.3.3, «Avvio PXE» (p. 44). È possibile utilizzare le opzioni di avvio di default e i tasti funzione oppure utilizzare il prompt delle opzioni di avvio della schermata di avvio dell'installazione per passare qualsiasi opzione di avvio di cui il kernel dell'installazione potrebbe avere bisogno a questo hardware specifico.

1.4.1 Uso delle opzioni di avvio di default

Le opzioni di avvio sono state descritte dettagliatamente nel Capitolo *Installazione con YaST* (↑Avvio) .

È in genere sufficiente selezionare *Installazione* per avviare il processo di avvio dell'installazione. Se si verificano problemi, le opzioni *Installazione - ACPI disabilitata* o *Installazione - Safe Settings* possono rivelarsi utili.

Per ulteriori informazioni sulla soluzione dei problemi relativi al processo di installazione, vedere la Sezione «Problemi di installazione» (Capitolo 9, *Problemi comuni e relative soluzioni*, ↑Avvio).

1.4.2 Uso dei tasti funzione

La barra dei menu nella schermata inferiore presenta alcune funzionalità avanzate necessarie in determinate configurazioni. L'uso dei tasti funzione consente di specificare opzioni aggiuntive da passare alle routine di installazione senza la necessità di conoscere la sintassi dettagliata di questi parametri, indispensabile invece se li si immette come opzioni di avvio (vedere la Sezione 1.4.3, «Uso delle opzioni di avvio personalizzate» (p. 53)).

Vedere la tabella seguente per un gruppo completo di opzioni disponibili.

Tabella 1.1 *Tasti funzione durante l'installazione*

Tasto	Scopo	Opzioni disponibili	Valore di default
F1	Consente di accedere alla Guida	Nessuna	Nessuna
F2	Seleziona la lingua per l'installazione	Tutte le lingue sono supportate	Inglese
F3	Consente di modificare la risoluzione dello schermo per l'installazione	• Text mode • VESA • resolution #1 • resolution #2 • ...	• I valori di default dipendono dall'hardware grafico
F4	Consente di selezionare l'origine dell'installazione	• CD-ROM/DVD • SLP • FTP	CD-ROM/DVD

Tasto	Scopo	Opzioni disponibili	Valore di default
		• HTTP • NFS • SMB • Disco rigido	
F5	Applica il disco di aggiornamento dei driver	Driver	Nessuna

1.4.3 Uso delle opzioni di avvio personalizzate

L'uso del gruppo appropriato di opzioni di avvio semplifica la procedura di installazione. Molti parametri possono essere configurati successivamente mediante le routine linuxrc, tuttavia l'uso delle opzioni di avvio è più semplice. In alcune configurazioni automatiche, le opzioni di avvio possono essere fornite mediante un file `initrd` o `info`.

La tabella seguente elenca tutti gli scenari di installazione indicati in questo capitolo con i parametri necessari per l'avvio e le opzioni di avvio corrispondenti. È sufficiente aggiungerli tutti nell'ordine di apparizione nella tabella per ottenere una stringa dell'opzione di avvio che viene passata alle routine di installazione. Ad esempio (tutto in una sola riga):

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

Sostituire tutti i valori (...) della stringa con i valori appropriati per la configurazione in uso.

Tabella 1.2 *Scenari di installazione (di avvio) utilizzati in questo capitolo*

Scenario di installazione	**Parametri necessari per l'avvio**	**Opzioni di avvio**
Capitolo *Installazione con YaST* (↑Avvio)	Nessuno: il sistema si avvia automaticamente	Non sono necessarie
Sezione 1.1.1, «Installazione remota semplice tramite VNC - Configurazione di rete statica» (p. 22)	• Posizione del server di installazione • Dispositivo di rete • Indirizzo IP • Maschera di rete • Gateway • Abilitazione VNC • Password VNC	• `install=(nfs,http,ftp,smb)://path_to_instmedia` • `netdevice=some_netdevice` (necessario solo se sono disponibili diversi dispositivi di rete) • `hostip=some_ip` • `netmask=some_netmask` • `gateway=ip_gateway` • `vnc=1` • `vncpassword=some_password`
Sezione 1.1.2, «Installazione remota semplice tramite VNC - Configurazione di rete dinamica tramite DHCP» (p. 23)	• Posizione del server di installazione • Abilitazione VNC • Password VNC	• `install=(nfs,http,ftp,smb)://path_to_instmedia` • `vnc=1` • `vncpassword=some_password`
Sezione 1.1.3, «Installazione remota tramite VNC - Avvio PXE e Wake on LAN» (p. 25)	• Posizione del server di installazione • Posizione del server TFTP • Abilitazione VNC	Non applicabile. Processo gestito mediante PXE e DHCP

Scenario di installazione	Parametri necessari per l'avvio	Opzioni di avvio
	• Password VNC	
Sezione 1.1.4, «Installazione remota semplice tramite SSH - Configurazione di rete statica» (p. 26)	• Posizione del server di installazione • Dispositivo di rete • Indirizzo IP • Maschera di rete • Gateway • Abilitazione SSH • Password SSH	• `install=(nfs,http,ftp,smb)://path_to_instmedia` • `netdevice=some_netdevice` (necessario solo se sono disponibili più dispositivi di rete) • `hostip=some_ip` • `netmask=some_netmask` • `gateway=ip_gateway` • `usessh=1` • `sshpassword=some_password`
Sezione 1.1.5, «Installazione remota semplice tramite SSH - Configurazione di rete dinamica tramite DHCP» (p. 28)	• Posizione del server di installazione • Abilitazione SSH • Password SSH	• `install=(nfs,http,ftp,smb)://path_to_instmedia` • `usessh=1` • `sshpassword=some_password`
Sezione 1.1.6, «Installazione remota tramite SSH - Avvio PXE e Wake on LAN» (p. 29)	• Posizione del server di installazione • Posizione del server TFTP • Abilitazione SSH • Password SSH	Non applicabile. Processo gestito mediante PXE e DHCP

SUGGERIMENTO

Per ulteriori informazioni sulle opzioni di avvio linuxrc utilizzate per l'avvio di un sistema Linux, vedere `/usr/share/doc/packages/linuxrc/linuxrc.html`.

1.5 Monitoraggio del processo di installazione

Vi sono diverse opzioni per eseguire il monitoraggio remoto del processo di installazione. Se sono state specificate le opzioni di avvio corrette,è possibile utilizzare VNC o SSH per controllare l'installazione e la configurazione del sistema da una workstation remota.

1.5.1 Installazione VNC

L'uso di qualsiasi visualizzatore VNC consente di controllare in remoto l'installazione di SUSE Linux virtualmente da ogni sistema operativo. In questa sezione viene illustrata la configurazione eseguita utilizzando un visualizzatore VNC o un browser Web.

Preparazione per l'installazione VNC

Per preparare la destinazione dell'installazione a un'installazione VNC è sufficiente fornire le opzioni di avvio appropriate all'avvio iniziale (vedere la Sezione 1.4.3, «Uso delle opzioni di avvio personalizzate» (p. 53)). Il sistema di destinazione viene avviato avvia in un ambiente basato su testo e attende la connessione di un client VNC al programma di installazione.

Il programma di installazione annuncia l'indirizzo IP e il numero di display necessario alla connessione per l'installazione. Se si dispone dell'accesso fisico al sistema di destinazione, questa informazione viene fornita subito dopo l'avvio del sistema per l'installazione. Immettere questi dati quando il client VNC li richiede e fornire la password VNC in uso.

Poiché la destinazione dell'installazione annuncia se stessa tramite OpenSLP, è possibile recuperare le informazioni relative all'indirizzo della destinazione dell'installazione

mediante un browser SLP senza la necessità di un contatto fisico con l'installazione stessa, a condizione che la configurazione di rete in uso e tutti i computer supportino OpenSLP:

1. Avviare il file KDE e il browser Web Konqueror.

2. Immettere `service://yast.installation.suse` nella barra di posizione.

   Il sistema di destinazione viene quindi visualizzato come icona nella schermata Konqueror. Facendo clic sull'icona, viene avviato il visualizzatore VNC KDE nel quale eseguire l'installazione. In alternativa, eseguire il visualizzatore VNC mediante l'indirizzo IP fornito e aggiungere `:1` al termine dell'indirizzo IP per visualizzare l'installazione in esecuzione.

Connessione al programma di installazione

Vi sono in genere due modi di connettersi al server VNC, in questo caso la destinazione dell'installazione. È possibile avviare un visualizzatore VNC come applicazione indipendente in qualsiasi sistema operativo oppure connettersi utilizzando un browser Web con supporto Java.

L'uso di VNC consente di controllare l'installazione di un sistema Linux da qualsiasi altro sistema operativo, incluse altre varianti Linux, Windows o Mac OS.

In un computer Linux, verificare che il pacchetto `tightvnc` sia installato. In un computer Windows, installare la porta Windows per questa applicazione, che può essere ottenuta dalla home page di TightVNC all'indirizzo `http://www.tightvnc.com/download.html` (in lingua inglese).

Per connettersi al programma di installazione in esecuzione nel computer di destinazione, procedere come indicato di seguito:

1. Avviare il visualizzatore VNC.

2. Immettere l'indirizzo IP e il numero di display della destinazione dell'installazione fornito dal browser SLP o dal programma di installazione stesso:

   ```
   ip_address:display_number
   ```

Sul desktop si apre una finestra in cui vengono visualizzate le schermate YaST come per una normale installazione locale.

L'uso di un browser Web per la connessione al programma di installazione rende l'utente completamente indipendente da qualsiasi software VNC o sistema operativo sottostante. Se l'applicazione browser è abilitata al supporto Java, è possibile utilizzare qualsiasi browser (Firefox, Internet Explorer, Konqueror, Opera e così via) per eseguire l'installazione del sistema Linux.

Per eseguire un'installazione VNC, procedere come indicato di seguito:

1. Avviare il browser Web preferito.
2. Al prompt dell'indirizzo, immettere quanto indicato di seguito:

   ```
   http://ip_address_of_target:5801
   ```

3. Immettere la password VNC quando viene richiesta. Nella finestra del browser vengono ora visualizzate le schermate YaST come per una normale installazione locale.

1.5.2 Installazione SSH

L'uso di SSH consente di controllare in remoto l'installazione del computer Linux utilizzando un client SSH.

Preparazione per l'installazione SSH

Oltre all'installazione del pacchetto software più appropriato (OpenSSH per Linux e PuTTY per Windows), è sufficiente passare le opzioni di avvio appropriate per abilitare SSH all'installazione. Per informazioni, vedere la Sezione 1.4.3, «Uso delle opzioni di avvio personalizzate» (p. 53). Per default OpenSSH viene installato in ogni sistema operativo basato su SUSE Linux.

Connessione al programma di installazione

1. Recuperare l'indirizzo IP della destinazione dell'installazione.

   Se si dispone dell'accesso fisico al computer di destinazione, è sufficiente utilizzare l'indirizzo IP fornito dalle routine di installazione alla console dopo l'avvio iniziale. In alternativa, utilizzare l'indirizzo IP assegnato a quel determinato host nella configurazione del server DHCP.

2. Nella riga di comando immettere il comando seguente:

   ```
   ssh -X root@ip_address_of_target
   ```

   Sostituire *`ip_address_of_target`* con l'indirizzo IP effettivo della destinazione dell'installazione.

3. Alla richiesta di un nome utente, immettere `root`.

4. Alla richiesta della password, immettere la password inviata tramite l'opzione di avvio SSH.

   Al termine dell'autenticazione viene visualizzato un prompt della riga di comando per la destinazione dell'installazione.

5. Immettere `yast` per avviare il programma di installazione.

   Viene aperta una finestra in cui vengono visualizzate le normali schermate YaST, come descritto nel Capitolo *Installazione con YaST* (↑Avvio) .

2 Configurazione avanzata dei dischi

Alcune configurazioni del sistema avanzate richiedono particolari impostazioni dei dischi. Per assegnare nomi permanenti ai dispositivi SCSI, utilizzare uno script di avvio specifico. LVM (Logical Volume Management) è uno schema di partizionamento dei dischi progettato per garantire una flessibilità decisamente maggiore rispetto al partizionamento fisico utilizzato nelle configurazioni standard. La funzionalità di istantanea di LVM semplifica la creazione di copie di backup dei dati. RAID (Redundant Array of Independent Disks) garantisce maggiori livelli di integrità dei dati, prestazioni e tolleranza agli errori.

2.1 Nomi di dispositivo permanenti per i dispositivi SCSI

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

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

/etc/fstab. Se volete dei nomi di dispositivo persistenti, potete definirli nel file /etc/scsi.alias; cfr. man scsidev.

SUGGERIMENTO: Nomi di dispositivo e udev

Benché SUSE Linux supporti boot.scsidev si consiglia comunque, quando intendete creare nomi di dispositivo persistenti, di ricorrere ad udev. udev provvederà alle immissioni da effettuare in /dev/by-id/.

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

2.2 Configurazione dell'LVM

In questa sezione illustriamo i principi alla base di LVM e le sue caratteristiche principali che lo rendono così versatile. Nella Sezione 2.2.2, «Configurazione di LVM tramite YaST» (p. 64) vi mostriamo come impostare LVM servendovi di YaST.

AVVERTIMENTO

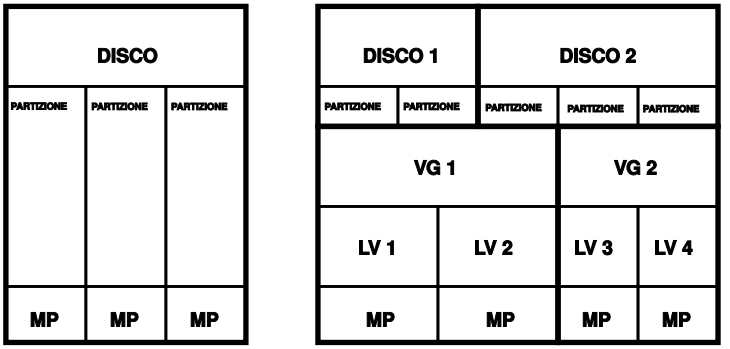
Anche con LVM può verificarsi una perdita di dati, in caso di crollo di una applicazione, mancanza di corrente e comandi errati. Salvate i vostri dati prima di implementare LVM o riconfigurare dei volumi. Una copia di sicurezza è e rimane un accorgimento indispensabile.

2.2.1 Il Logical Volume Manager

LVM (Logical Volume Manager) permette di distribuire lo spazio di dischi rigidi su diversi file system, cosa che si rivela essere utile soprattutto in quei casi in cui si presenta la necessità di dover modificare la segmentazione del disco rigido, dopo aver eseguito il partizionamento in fase di installazione. E visto che è accompagnato da una serie di difficoltà modificare il partizionamento con il sistema in esecuzione è stato ideato LVM che mette a disposizione un pool virtuale (volume group, abbreviato con VG) di memoria per creare dei logical volumes (LV) richiesti. Il sistema operativo indirizza questi LV al posto di partizioni fisiche. I volume group (VG), che chiameremo gruppi di volume possono includere più di un disco rigido, quindi un VG può essere costituito da diversi

dischi o parti di essi. In tal modo LVM si svincola dallo spazio fisico del disco rigido per poter cambiarne segmentazione in modo più semplice e sicuro rispetto alla ripartizionamento fisico. Per maggiori dettagli sul partizionamento fisico si veda la sezione chiamata «Tipi di partizione» (Capitolo 1, *Installazione con YaST*, ↑Avvio) e la Sezione «Partizionamento» (Capitolo 3, *Configurazione di sistema con YaST*, ↑Avvio).

Figura 2.1 *Partizionamento fisico vs. LVM*



La Figura 2.1, «Partizionamento fisico vs. LVM» (p. 63) mette a confronto il partizionamento fisico (sulla sinistra) e la segmentazione LVM (sulla destra). Sulla sinistra, un singolo disco rigido è stato partizionato e presenta tre partizioni fisiche (PART), ognuna con un punto di mount (MP), in modo che il sistema operativo possa accedervi. Sulla destra, due dischi rigidi presentano due e tre partizioni fisiche. Vi sono stati definiti due gruppi di volume LVM (VG 1 e VG 2). VG 1 contiene due partizioni del DISK 1 ed una del DISK 2. VG 2 contiene le rimanenti due partizioni del DISK 2. Sotto LVM, le partizioni fisiche integrate in un gruppo di volume vengono chiamate volumi fisici (PV). All'interno dei gruppi di volume, sono stati definiti quattro logical volumes (LV 1 - LV 4), indirizzabili per il sistema operativo tramite i relativi punti di mount. Non è necessario allineare il limite tra diversi logical volume con il limite di una partizioni qualisasi. Si veda a riguardo LV 1 e LV 2 nel nostro esempio.

Caratteristiche di LVM:

- Più dischi rigidi/partizioni possono essere riuniti in un unica grande logical volume.
- Se un LV si riempie (p.es. `/usr`), potete espanderlo, in presenza della configurazione adeguata.

- Con l'LVM, potrete espandere dischi rigidi o LV addirittura con il sistema in esecuzione, a condizione che disponiate di hardware «hot-swapable», l'unico adatto a questo tipo di operazioni.

- Sussiste di abilitare il modo "striping" che distribuisce il flusso di dati di un logical volume su diversi PV. Se questi PV risiedono su diversi dischi rigidi si hanno migliori prestazioni per quel che riguarda l'acceso in lettura e scrittura, proprio come con RAID 0.

- Il feature «snapshot» consente, soprattutto con server, di ottenere dei backup consistenti con il sistema in esecuzione.

L'impiego dell'LVM si rivelerà vantaggioso anche su un PC domestico usato in modo intensivo e su piccoli server. Se contate di dover amministrare una quantità di dati sempre crescente, ad esempio, banche dati, archivi MP3 o directory di utenti, il Logical Volume Manager potrebbe tornarvi molto utile. Un LVM vi permette, per esempio, di creare file system più grandi del disco fisico. Un altro vantaggio dell'LVM è che si possono creare fino a 256 volumi logici. Tenete comunque presente che lavorare con LVM differisce notevolmente dall'uso delle partizioni convenzionali. Per maggiori informazioni ed un'introduzione alla configurazione del «Logical Volume Manager» (LVM), consultate l'howto LVM ufficiale reperibile all'indirizzo `http://tldp.org/HOWTO/LVM-HOWTO/`.

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

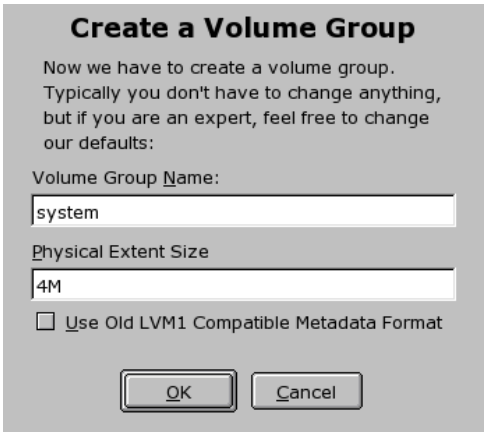
2.2.2 Configurazione di LVM tramite YaST

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

Creare dei gruppi di volume

Se ancora non vi è alcun gruppo di volume sul vostro sistema, createne uno (si veda la Figura 2.2, «Creare un gruppo di volumi» (p. 65)). Potete creare dei gruppi aggiuntivi tramite *Aggiungi gruppo*, comunque basta un solo gruppo di volume; `system` è il nome suggerito per il gruppo di volume che conterrà i file di sistema di SUSE Linux. La dimensione fisica determina la dimensione del blocco fisico del gruppo di volume. In un gruppo di volume lo spazio viene gestito in base questa dimensione. Tale valore verrà normalmente fissato su 4 megabyte, consentendo un'estensione massima di 256 gigabyte per volumi fisici e logici. La dimensione fisica va aumentata (p.es. a 8, 16 o 32 megabyte) solo se avete bisogno di un volume logico più grande di 256 megabyte.

Figura 2.2 *Creare un gruppo di volumi*



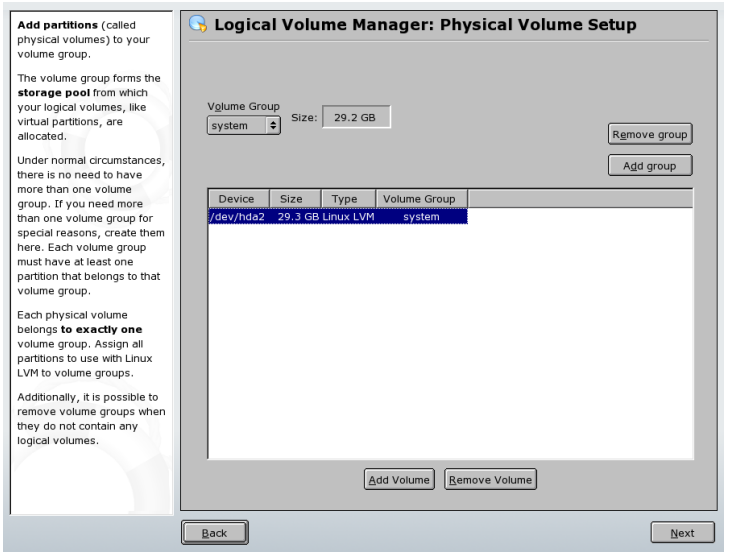
Configurare PV (Physical Volume)

Dopo aver creato il gruppo di volume, nel seguente dialogo verranno elencate tutte le partizioni che presentino l'indicazione «Linux LVM» o «Linux native». Tutte le partizioni swap e DOS non verranno pertanto incluse nella lista. Se una partizione è già stata assegnata ad un gruppo di volume, il nome di quest'ultimo verrà riportato nella lista. Partizioni non allocate saranno contrassegnate con un «--».

Il gruppo di volume da elaborare può essere determinato nel box delle selezioni che si trova in alto a sinistra. Con i bottoni in alto a destra, potrete creare nuovi gruppi di volume e cancellarne dei vecchi. Tuttavia, sarà possibile eliminare solo gruppi di volume

ai quali non è più attribuita alcuna partizione. Una partizione assegnata ad un gruppo di volume anche chiamata Physical Volume (abbr.: PV).

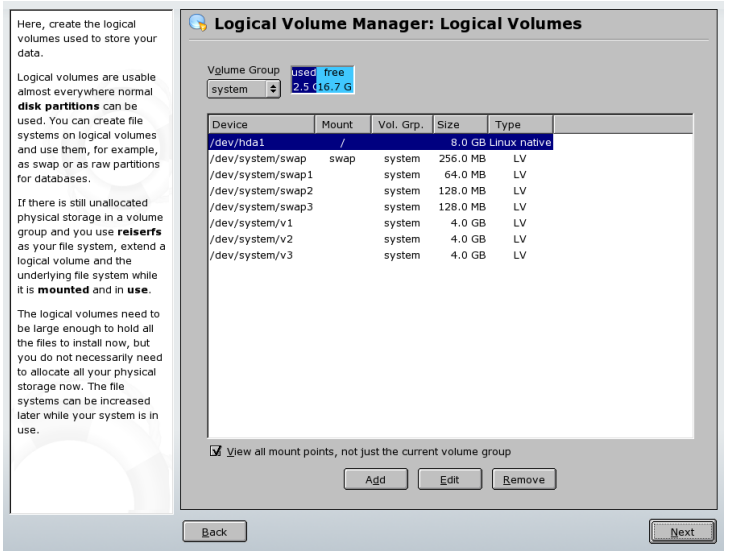
Figura 2.3 *Impostare PV*



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

Configurare i volumi logici

Figura 2.4 *Amministrare i volumi logici*

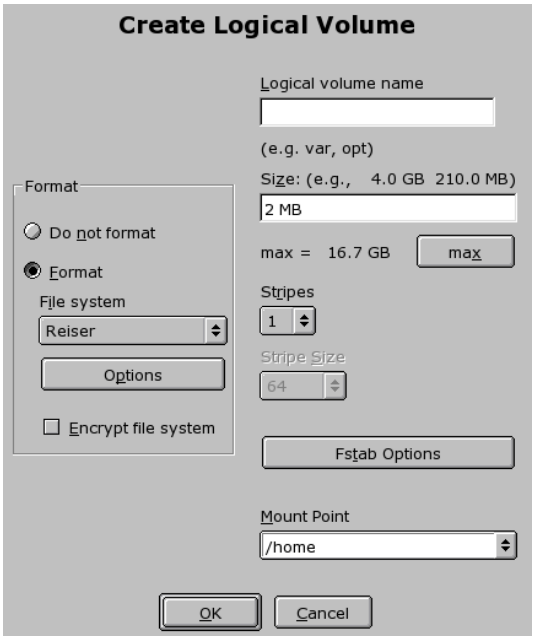


Tramite *Aggiungi* si apre una menu in cui immettere i vostri dati per creare un nuovo volume logico, cioé la dimensione, file system e punto di mount. Di solito viene creato un file system, ad es. reiserfs o ext2, su un volume logico e quindi assegnato un punto di mount. I file archiviati sul volume logico possono essere inidirizzati tramite questo punto di mount. Inoltre, è possibile distribuire il flusso di dati nel volume logico tra diversi volumi fisici (striping). Se i volumi fisici risiedono su diversi dischi rigidi si realizzano dei benefici per quanto riguarda le prestazioni in scrittura e lettura (alla stregua di RAID 0). C'è comunque da tenere presente che lo striping di LV con `n` stripe può essere creato in modo corretto solo se lo spazio di memoria richiesto dall'LV si lascia allocare uniformemente ai `n` volumi fisici. Se chiaramente vi sono solo due PV, non è possibile avere un LV con tre stripe.

AVVERTIMENTO: Striping

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

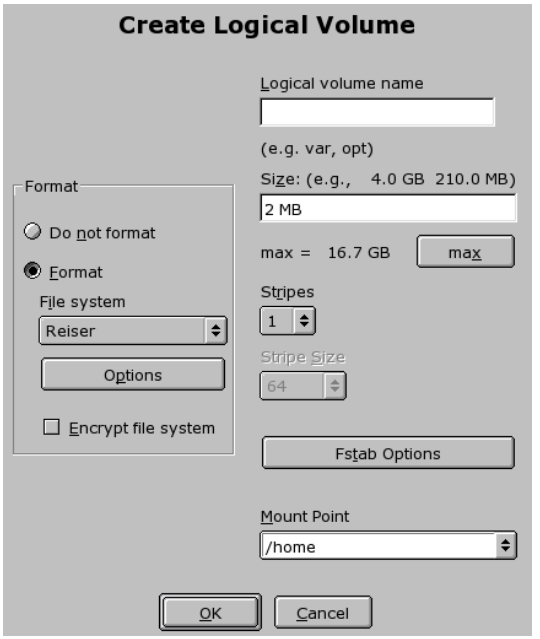
Figura 2.5 *Creare volumi logici*



Normalmente, su un volume logico viene creato un file system (p.es. reiserfs, ext2), al quale viene poi attribuito un punto di mount. Sotto questo punto di mount, nei sistemi installati, si trovano i file memorizzati su questo logical volume. Nella lista, sono riportate tutte le normali partizioni Linux, con un punto di mount, nonché tutte le partizioni swap ed i volumi logici esistenti.

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

Figura 2.6 *Creare volumi logici*



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

Amministrazione diretta di LVM

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

2.3 Configurazione di RAID software

I RAID (Redundant Array of Inexpensive Disks) vengono configurati allo scopo di combinare più partizioni di dischi rigidi in un unico disco rigido *virtuale* di grandi dimensioni per ottimizzare le prestazioni, la sicurezza dei dati o entrambi questi aspetti. Questo metodo, tuttavia, implica la rinuncia a un vantaggio a beneficio di un altro. Nella maggior parte dei controller RAID viene utilizzato il protocollo SCSI poiché è in grado di utilizzare un numero maggiore di dischi rigidi in modo più efficiente rispetto al protocollo IDE ed è più adatto all'elaborazione di comandi in parallelo. Alcuni RAID supportano comunque i dischi rigidi IDE o SATA. Fare riferimento al database dell'hardware all'indirizzo `http://cdb.suse.de` (in lingua tedesca).

2.3.1 RAID software

I RAID software consentono di soddisfare le medesime esigenze dei controller RAID, in genere molto costosi. SUSE Linux consente di combinare più dischi rigidi in un unico sistema RAID software mediante YaST, offrendo un'alternativa particolarmente conveniente ai RAID hardware. Le strategie coinvolte nella configurazione di un sistema RAID che includa diversi dischi rigidi sono numerose e ognuna di queste consente di conseguire particolari obiettivi e vantaggi e si distingue per determinate caratteristiche. Queste varianti sono note in genere come *livelli RAID*.

I livelli RAID più comuni sono:

RAID 0
: Questo livello consente di migliorare le prestazioni di accesso ai dati mediante la suddivisione dei blocchi di ogni file tra più unità disco. Non si tratta, in effetti, di un RAID vero e proprio poiché non prevede il backup dei dati. Tuttavia il nome *RAID 0* è diventato di uso comune per questo tipo di sistema. RAID 0 consente di riunire in pool due o più dischi rigidi. Le prestazioni sono molto buone, ma è sufficiente che si verifichi un problema in uno solo dei dischi rigidi perché il sistema RAID venga distrutto e i dati perduti.

RAID 1
: Questo livello garantisce sicurezza adeguata per i dati poiché ne viene eseguita una copia integrale su un altro disco rigido. Questa tecnica è nota come *copia speculare del disco rigido*. Se un disco viene danneggiato, è sempre disponibile una copia dei rispettivi contenuti in un'altra unità. È sufficiente che un solo disco rimanga integro

affinché non si verifichino perdite di dati. Le prestazioni in scrittura risultano leggermente ridotte durante il processo di copia di circa il 10/20% rispetto all'utilizzo di un unico disco rigido. L'accesso in lettura, tuttavia, è sensibilmente più rapido che in qualsiasi comune disco rigido poiché i dati sono duplicati e ne viene eseguita la scansione in parallelo. In generale, è possibile affermare che il livello 1 offre una velocità circa doppia in lettura e sostanzialmente pari in scrittura rispetto ai dischi rigidi singoli.

RAID 2 e RAID 3

Si tratta di implementazioni RAID atipiche. Se si utilizza il livello 2, i dati vengono suddivisi a livello di bit invece che di blocco. Nel livello 3 la suddivisione dei dati avviene a livello di byte con un disco di parità dedicato e non è possibile gestire più richieste contemporaneamente. Si tratta di livelli poco diffusi.

RAID 4

Se si utilizza il livello 4, i dati vengono suddivisi a livello di blocco, come nel livello 0, con un disco di parità dedicato. In caso di malfunzionamento di uno dei dischi, i dati di parità vengono utilizzati per creare un disco sostitutivo. Il disco di parità può tuttavia causare un collo di bottiglia relativo all'accesso in scrittura. Ciononostante il livello 4 è abbastanza diffuso.

RAID 5

Il RAID 5 è una soluzione di compromesso tra i livelli 0 e 1, ottimizzata in termini di prestazioni e ridondanza. Lo spazio su disco rigido equivale al numero di dischi utilizzati meno uno. I dati vengono distribuiti tra i dischi rigidi come nei RAID 0. Per motivi di sicurezza, i *blocchi di parità* vengono creati in una delle partizioni. Questi sono collegati tra loro tramite XOR che consente di ricostruire i contenuti in base al blocco di parità corrispondente in caso di malfunzionamento del sistema. Nei RAID 5 è consentito il malfunzionamento di un solo disco rigido alla volta il quale, pertanto, deve essere sostituito nel minor tempo possibile per evitare che si verifichino perdite di dati.

Altri livelli RAID

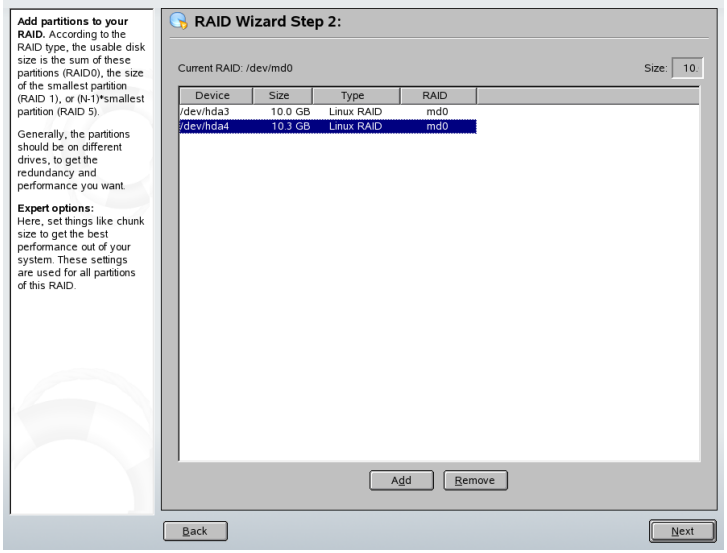
Sono stati sviluppati vari altri livelli RAID, ad esempio RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50 e così via, alcuni dei quali sono implementazioni proprietarie realizzate da fornitori di hardware. Si tratta di livelli poco diffusi, la cui descrizione viene pertanto tralasciata.

2.3.2 Configurazione di RAID software con YaST

Per configurare i RAID software mediante YaST è possibile utilizzare la Modalità di partizionamento per esperti di YaST, descritto nella Sezione «Partizionamento» (Capitolo 3, *Configurazione di sistema con YaST*, ↑Avvio). Questo strumento professionale per il partizionamento consente di modificare e cancellare le partizioni esistenti, nonché di crearne di nuove da utilizzare con i RAID software. Per creare le partizioni RAID, fare innanzitutto clic su *Crea* → *Non formattare* e quindi selezionare *0xFD Linux RAID* come identificatore della partizione. Per i RAID 0 e RAID 1, sono necessarie almeno due partizioni. Per il RAID 1, in genere, solo due. Se si utilizza il RAID 5, sono necessarie almeno tre partizioni. È consigliabile utilizzare soltanto partizioni di dimensioni equivalenti. È consigliabile memorizzare le partizioni RAID in dischi rigidi diversi in modo da ridurre il rischio di perdite dei dati in caso di malfunzionamento (RAID 1 e 5) e per ottimizzare le prestazioni RAID 0. Dopo aver creato tutte le partizioni da utilizzare con il RAID, fare clic su *RAID* → *Crea RAID* per avviare la configurazione RAID.

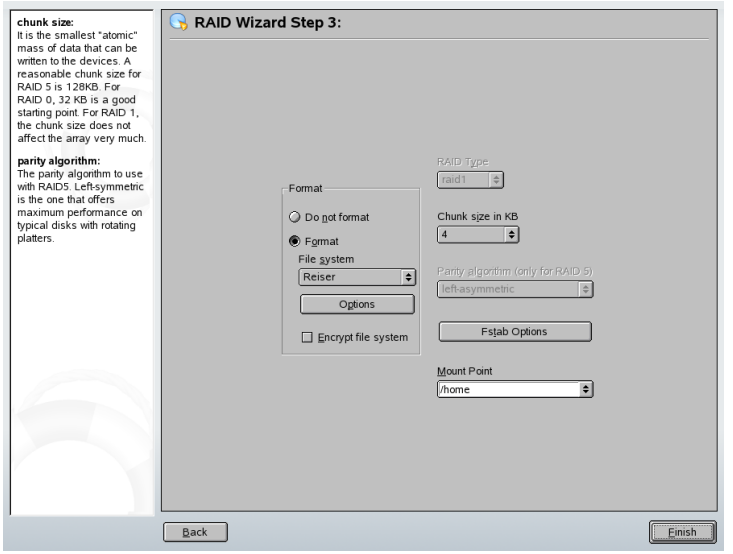
Nella finestra di dialogo successiva, scegliere il livello RAID, ovvero 0, 1 o 5. Per ulteriori informazioni, vedere la Sezione 2.3.1, «RAID software» (p. 70). Fare quindi clic su *Avanti* per visualizzare la finestra di dialogo successiva in cui vengono elencate tutte le partizioni di tipo «Linux RAID» o «Linux native» (vedere la Figura 2.7, «Partizioni RAID» (p. 73)). Non vengono visualizzate partizioni di scambio o DOS. Se una partizione è già assegnata a un volume RAID, nell'elenco viene indicato il nome del dispositivo corrispondente (ad esempio `/dev/md0`). Le partizioni non assegnate sono indicate da «--».

Figura 2.7 *Partizioni RAID*



Per aggiungere una partizione precedentemente non assegnata al volume RAID selezionato, fare clic sulla partizione e quindi su *Aggiungi*. Il nome del dispositivo RAID viene quindi indicato accanto alla partizione selezionata. Assegnare tutte le partizioni riservate al RAID. In caso contrario, lo spazio disponibile nella partizione rimane inutilizzato. Dopo aver assegnato tutte le partizioni, fare clic su *Avanti* per passare alla finestra di dialogo delle impostazioni in cui è possibile ottimizzare le prestazioni (vedere la Figura 2.8, «Impostazioni del file system» (p. 74)).

Figura 2.8 *Impostazioni del file system*



Impostare il file system da utilizzare, la cifratura e il punto di montaggio per il volume RAID come in una partizione tradizionale. Selezionare *Superblock persistente* per fare in modo che le partizioni RAID vengano riconosciute come tali all'avvio del sistema. Fare clic su *Fine* per completare la configurazione e verificare che in Modalità di partizionamento per esperti il dispositivo `/dev/md0` e gli altri siano indicati con il *RAID*.

2.3.3 Risoluzione dei problemi

Esaminare il file `/proc/mdstats` per controllare se una partizione RAID è stata distrutta. In caso di malfunzionamento del sistema, chiudere Linux e sostituire il disco rigido difettoso con una nuova unità partizionata in modo identico. Riavviare quindi il sistema e immettere il comando `mdadm /dev/mdX --add /dev/sdX`. Sostituire "X" con l'identificatore del dispositivo in questione. In questo modo, il disco rigido viene automaticamente integrato nel sistema RAID e ricostruito completamente.

2.3.4 Ulteriori informazioni

Per ulteriori informazioni e istruzioni sulla configurazione di RAID software, vedere la documentazione HOWTO in:

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

Sono disponibili diverse mailing list relative ai RAID Linux, ad esempio `http://www.mail-archive.com/linux-raid@vger.rutgers.edu`.

Parte II. Internet

3 Browser Web Konqueror

Konqueror non è solo un file manager versatile, ma è anche un moderno browser Web. Se si avvia il browser con l'icona del pannello, verrà visualizzato un profilo del browser Web. Come browser, Konqueror offre la navigazione a schede, la possibilità di salvare pagine Web contenenti immagini, parole chiave di Internet, segnalibri e supporto per Java e JavaScript.

Avviare Konqueror dal menu principale o immettendo il comando `konqueror`. Per caricare la pagina Web, immettere il relativo indirizzo nella barra degli indirizzi, ad esempio, `http://www.suse.com`. Konqueror avvia la ricerca dell'indirizzo per visualizzare la pagina. Non è necessariamente richiesta l'immissione del protocollo all'inizio dell'indirizzo (`http://` in questo caso). Il programma è in grado di completare l'indirizzo automaticamente, ma funziona in modo affidabile solo con gli indirizzi Web. Per l'indirizzo FTP, è necessario immettere sempre `ftp://` all'inizio del campo di input.

Figura 3.1 *Finestra del browser di Konqueror*

3.1 Navigazione a schede

Se si utilizza spesso più di una pagina Web contemporaneamente, la navigazione a schede rende più facile il passaggio da una pagina all'altra. Caricare i siti Web in schede separate all'interno di una sola finestra. In tal modo si ha il vantaggio di un maggiore controllo del desktop poiché la finestra principale è una sola. Dopo il logout, la gestione di sessione KDE consente di salvare la sessione Web in Konqueror. Al successivo login, Konqueror carica esattamente gli URL visitati l'ultima volta.

Per aprire una nuova scheda, selezionare *Window (Finestra)* → *New Tab (Nuova scheda)* oppure premere Ctrl + Shift + N. Per modificare il funzionamento delle schede, accedere a *Settings (Impostazioni)* → *Configura Konqueror*. Nella finestra di dialogo che si apre, selezionare *Web Behavior (comportamento Web)* → *Tabbed Browsing (navigazione a schede)*. Per aprire nuove schede invece di finestre, attivare *Open links in new tab instead of in new window (Apri collegamenti nella nuova scheda invece che nella nuova finestra)*. È possibile anche nascondere la scheda con *Hide the tab bar when only one tab is open (Nascondi la barra delle schede solo quando è aperta una sola scheda)*. Per visualizzare opzioni ulteriori, premere *Advanced Options (Opzioni avanzate)*.

È possibile salvare le schede con gli URL e la posizione della finestra in un profilo. Questa procedura è leggermente diversa dalla gestione di sessione sopra indicata. Grazie ai profili, si hanno a disposizione le schede salvate senza perdita di tempo per l'avvio come per la gestione di sessione.

In Konqueror, accedere a *Settings (Impostazioni) → Configure View Profiles (Configura nuovi profili)* e assegnare un nome al profilo. È possibile inoltre salvare le dimensioni della finestra nel profilo utilizzando la relativa opzione. Assicurarsi che sia selezionato *Save URLs in profile (Salva URL nel profilo)*. Confermare con *Save (Salva)*. La volta successiva in cui è necessaria la «raccolta delle schede,» accedere a *Settings (Impostazioni) → Load View Profile (Carica profile della vista)* e visualizzare il nome elencato nel menu. Dopo la selezione del nome, Konqueror ripristina le schede.

3.2 Salvataggio di pagine Web e immagini

Come in altri browser, è possibile salvare le pagine Web. A questo scopo, selezionare *Location (Posizione) → Save as (Salva con nome)* e specificare il nome per il file HTML. Le immagini, tuttavia, non verranno salvate. Per archiviare un'intera pagina Web, incluse le immagini, selezionare *Tools (Strumenti) → Archive Web Page (Archivia pagina Web)*. In Konqueror viene utilizzato un nomefile che in genere è possibile accettare. Il nome file termina con `.war`, ovvero l'estensione per gli archivi Web. Per visualizzare l'archivio Web salvato in un secondo momento, è sufficiente fare clic sul file relativo per visualizzare la pagina Web in Konqueror insieme alle immagini.

3.3 Parole chiave di Internet

Esplorare il Web con Konqueror è estremamente facile. In Konqueror vengono definiti oltre 70 filtri di ricerca, tutti dotati di una scorciatoia specifica. Per cercare un determinato argomento su Internet, è sufficiente immettere la scorciatoia e la parola d'ordine separate da due punti. Verrà visualizzata una pagina contenente i risultati della ricerca.

Per visualizzare le scorciatoie già definite, accedere a *Settings (Impostazioni) → Configure Konqueror (Configura Konqueror)*. Nella finestra di dialogo che si apre, selezionare *Web Shortcuts (Scorciatoie del Web)*. Ora è possibile visualizzare i nomi

dei provider di ricerca e le scorciatoie. Konqueror definisce diversi filtri di ricerca: i motori di ricerca «classici», come Google, Yahoo e Lycos e molti filtri per scopi meno comuni, come le ricerche di un database degli acronimi, di un database dei film di Internet o di applicazioni KDE.

Definire un nuovo motore di ricerca nel caso non si trovi il proprio. Ad esempio, per cercare il nostro database di supporto in relazione ad alcuni articoli interessanti, accedere a `http://portal.suse.com/`, cercare la pagina di ricerca e immettere la propria interrogazione. Questa procedura viene semplificata dalle scorciatoie. Nella finestra di dialogo indicata, selezionare *New (Nuovo)* e assegnare un nome alla scorciatoia in *Search provider name (Cerca nome provider)*. Immettere le proprie abbreviazioni in *URI shortcuts (Scorciatoie URI)*, che possono essere più di una, separate da virgola. Il campo di testo importante è *Search URI (Cerca URI)*. Premere Shift + F1 e fare clic nel campo per aprire una breve guida. L'interrogazione di ricerca è specificata come `\{@}`. A questo punto è fondamentale inserirla nella posizione corretta. In questo caso, le impostazioni per il database di supporto di SUSE saranno: *Search provider name (Cerca nome provider)* è `SUSE Support Database`, *Search URI (Cerca URI)* è (su unica riga) `https://portal.suse.com/PM/page/search.pm?q=\{@}&t=optionSdbKeywords&m=25&l=en&x=true` e *URI shortcuts (Scorciatoie URI)* è `sdb_it`.

Dopo aver confermato due volte con *Ok*, immettere la propria interrogazione nella barra degli indirizzi di Konqueror, ad esempio `sdb_it:kernel`. Il risultato viene visualizzato nella finestra corrente.

3.4 Segnalibri

Invece di ricordare e reimmettere gli indirizzi dei siti visitati spesso, è possibile contrassegnare questi URL utilizzando il menu *Bookmarks (Segnalibri)*. Oltre agli indirizzi delle pagine Web, è possibile anche utilizzare il segnalibro per qualsiasi directory del disco locale.

Per creare un nuovo segnalibro in Konqueror, fare clic su *Bookmarks (Segnalibri)* → *Add Bookmark (Aggiungi segnalibro)*. Ogni segnalibro aggiunto in precedenza viene incluso come voce di menu. Si consiglia di organizzare la raccolta di segnalibri per argomento in una struttura gerarchica in modo da non perdere traccia delle diverse voci. È possibile creare un nuovo sottogruppo per i segnalibri con *New Bookmark Folder (Nuova cartella segnalibri)*. Per aprire l'editor di segnalibri, selezionare *Bookmarks*

(Segnalibri) → Edit Bookmarks (Modifica segnalibri). Utilizzare il programma per organizzare, riordinare, aggiungere ed eliminare i segnalibri.

Se si utilizza Netscape, Mozilla o Firefox come browser aggiuntivo, non è necessario creare di nuovo i segnalibri. Nell'editor di segnalibri, se si seleziona *File → Import Netscape Bookmarks (Importa segnalibri di Netscape)*, è possibile integrare i segnalibri di Netscape e Mozilla nella raccolta più recente. È possibile eseguire anche l'operazione inversa tramite *Export as Netscape Bookmarks (Esporta come segnalibro di Netscape)*.

Per modificare i segnalibri, fare clic con il pulsante destro del mouse sulla voce. Verrà visualizzato un menu a comparsa in cui è possibile selezionare l'azione desiderata (taglia, copia, elimina e così via). Quando si ottiene il risultato desiderato, salvare i segnalibri con *File → Save (Salva)*. Se si desidera modificare soltanto il nome o il collegamento, è sufficiente fare clic con il pulsante destro del mouse sulla voce nella barra degli strumenti del segnalibro e selezionare *Properties (Proprietà)*. Modificare il nome e la posizione, quindi confermare con *Update (Aggiorna)*.

Per salvare l'elenco dei segnalibri e consultarlo in modo rapido, attivare la visualizzazione dei segnalibri in Konqueror. È sufficiente selezionare *Settings (Impostazioni) → Toolbars (Barre strumenti) → Bookmark Toolbar (Konqueror) (Barra degli strumenti dei segnalibri)*. Nella finestra corrente di Konqueror, verrà visualizzato automaticamente un pannello con i segnalibri.

3.5 Java e JavaScript

È opportuno evitare che questi due linguaggi vengano confusi. Java è un linguaggio di programmazione indipendente dalla piattaforma e orientato agli oggetti di Sun Microsystems. È molto utilizzato per piccoli programmi (applet) eseguiti su Internet per servizi bancari in linea, commercio elettronico e chat. JavaScript è un linguaggio di script interpretato che viene utilizzato principalmente per creare la struttura dinamica delle pagine Web (ad esempio per i menu e altri effetti).

Konqueror consente di attivare e disattivare questi due linguaggi anche in base alle specifiche del dominio, consentendo l'accesso ad alcuni host e rifiutandolo ad altri. Per motivi di sicurezza, Java e JavaScript sono spesso disattivati. Tuttavia, per la visualizzazione corretta di alcune pagine Web è richiesta l'attivazione di JavaScript.

3.6 Ulteriori informazioni

Per eventuali domande o problemi che possono derivare dall'utilizzo di Konqueror, fare riferimento al manuale dell'applicazione disponibile nel menu della *Help (Guida)*. È possibile anche visitare la pagina Web di Konqueror all'indirizzo `http://www.konqueror.org`.

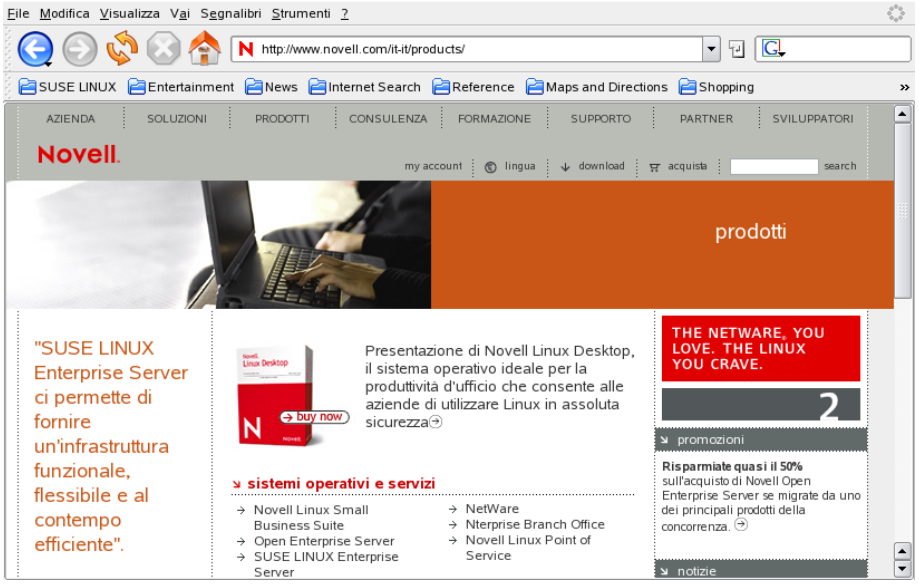
4 Firefox

In SUSE Linux è incluso il browser Web Mozilla Firefox. Con funzioni come la navigazione a schede, il blocco dei popup e la gestione degli scaricamento e delle immagini, Firefox combina le tecnologie Web più avanzate. Visualizzazione di più pagine Web in una singola finestra. Eliminazione di pubblicità fastidiose e disattivazione di immagini che causano rallentamenti. L'accesso a vari motori di ricerca che consentono di trovare le informazioni richieste è facile. Avviare il programma dal menu principale oppure immettendo il comando `firefox`. Le principali funzioni del programma vengono descritte nelle seguenti sezioni.

4.1 Visualizzazione di siti Web

L'aspetto e l'utilizzo di Firefox sono analoghi a quelli di altri browser. Tale strumento viene indicato nella Figura 4.1, «Finestra del browser Firefox» (p. 86). La barra degli strumenti di navigazione include i pulsanti per la navigazione, quali *Avanti* e *Indietro* oltre a una barra degli indirizzi per l'accesso ai siti Web. Per un accesso più rapido alle pagine è possibile utilizzare i segnalibri. Per ulteriori informazioni sulle varie funzioni di Firefox, fare clic su *?* nella barra dei menu.

Figura 4.1 *Finestra del browser Firefox*



4.1.1 Navigazione a schede

Se si utilizzano spesso più pagine Web contemporaneamente, la navigazione a schede renderà più semplice il passaggio da una all'altra. È possibile caricare vari siti Web in schede separate all'interno di una finestra.

Per aprire una nuova scheda, selezionare *File → Nuova scheda*. Verrà aperta una scheda vuota nella finestra di Firefox. In alternativa, fare clic con il pulsante destro su un collegamento e selezionare *Apri in nuova scheda*. Fare clic con il pulsante destro del mouse sulla scheda stessa per accedere ad altri menu e opzioni. È possibile creare una nuova scheda, caricare nuovamente una o tutte le schede presenti o chiuderle.

4.1.2 Utilizzo della barra laterale

Utilizzare il lato sinistro della finestra del browser per visualizzare i segnalibri o la cronologia. Le estensioni possono aggiungere nuove modalità di utilizzo anche alla barra laterale. Per visualizzare la barra laterale, selezionare *Visualizza → Pannelli* e selezionare i contenuti desiderati.

4.2 Ricerca di informazioni

È possibile ricercare le informazioni con Firefox in due modi: la barra dei motori di ricerca e la barra di ricerca. La barra dei motori di ricerca consente di cercare pagine Web, mentre la barra di ricerca consente di trovare elementi sulla pagina corrente.

4.2.1 Utilizzo della barra dei motori di ricerca

Firefox è dotato di una barra di ricerca che consente di accedere a vari motori, quali Google, Yahoo o Amazon. Ad esempio, se si desidera reperire informazioni su SUSE utilizzando il motore corrente, fare clic nella barra dei motori di ricerca, digitare `SUSE` e premere Invio. I risultati verranno visualizzati nella finestra. Per selezionare il motore di ricerca, fare clic sull'icona nella barra. Viene visualizzato un elenco di motori di ricerca disponibili.

4.2.2 Utilizzo della barra di ricerca

Per ricercare all'interno di una pagina Web, fare clic su *Modifica → Trova in questa pagina* o premere Ctrl + F e verrà visualizzata la barra di ricerca. In genere, viene visualizzata nella parte inferiore di una finestra. Digitare la richiesta nel campo di immissione. Firefox evidenzia tutte le occorrenze del gruppo di parole. È possibile attivare o disattivare l'evidenziazione utilizzando *Evidenzia*..

4.3 Gestione dei segnalibri

I segnalibri forniscono una modalità di accesso pratica ai siti Web preferiti. Per aggiungere il sito Web attuale all'elenco dei segnalibri, fare clic su Segnalibri *Segnalibri → Aggiungi pagina nei segnalibri*. Se nel browser sono attualmente visualizzati più siti Web nelle schede, nell'elenco dei segnalibri viene aggiunto solo l'URL della scheda attualmente selezionata.

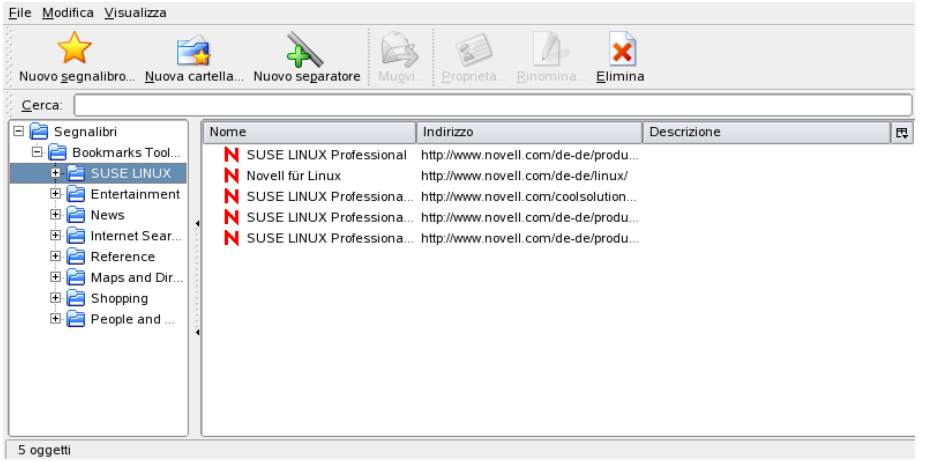
Quando si aggiunge un segnalibro è possibile specificare un nome alternativo per individuarlo e selezionare la cartella in cui memorizzarlo. Per eliminare un sito Web

dall'elenco dei segnalibri, fare clic su *Segnalibri*, individuare il segnalibro nell'elenco, quindi fare clic con il pulsante destro del mouse e selezionare *Elimina*.

4.3.1 Utilizzo di Gestione segnalibri

È possibile utilizzare lo strumento di gestione dei segnalibri per gestire le proprietà (nome e destinazione) di ciascun segnalibro nonché per organizzarli in cartelle e sezioni. Tale strumento ha l'aspetto seguente Figura 4.2, «Utilizzo di Gestione segnalibri di Firefox» (p. 88).

Figura 4.2 *Utilizzo di Gestione segnalibri di Firefox*



Per aprire Gestione segnalibri, fare clic su *Segnalibri* → *Gestione segnalibri*. Verrà visualizzata una finestra contenente i segnalibri. Selezionare *Nuova cartella* per creare una nuova cartella con nome e descrizione. Per creare un nuovo segnalibro, fare clic su *Nuovo segnalibro*. In questo modo sarà possibile inserire nome, indirizzo, parola chiave e descrizione. La parola chiave è un collegamento al segnalibro. Se fosse necessario visualizzare il nuovo segnalibro nella barra laterale, selezionare *Carica questo segnalibro nella barra laterale*.

4.3.2 Migrazione di segnalibri

Se in passato si è utilizzato un altro browser, è probabile che si desideri utilizzare le stesse preferenze e segnalibri anche in Firefox. Al momento è possibile importare da Netscape 4.x, 6, 7, Mozilla 1.x e Opera.

Per importare le impostazioni, fare clic su *File → Importa*. Selezionare il browser dal quale importare le impostazioni. Dopo aver fatto clic su *Avanti*, le impostazioni verranno importate. I segnalibri importati si trovano in una nuova cartella, il cui nome inizia con `Da`.

4.3.3 Segnalibri Live

I segnalibri Live visualizzano i titoli nel menu dei segnalibri e consentono di essere aggiornati con le ultime notizie. In questo modo è possibile risparmiare tempo con un rapido sguardo ai siti preferiti.

Questo formato è supportato da molti siti e blog. Un sito Web indica questa possibilità mostrando nell'angolo inferiore destro un rettangolo arancione con la scritta RSS. Fare clic su di esso e selezionare *Sottoscrivi NOME DEL FEED*. Si apre una finestra di dialogo dove è possibile selezionare il nome e la posizione del segnalibro Live. Confermare con *Aggiungi*.

Alcuni siti non comunicano a Firefox la possibilità di supportare i feed delle notizie, sebbene in effetti lo supportino. Per aggiungere un segnalibro Live manualmente, sarà necessario l'URL del feed. Procedere come segue:

Procedura 4.1 *Aggiunta di un segnalibro Live manualmente*

1. Aprire Gestione segnalibri utilizzando *Segnalibri → Gestione segnalibri*. Viene aperta una nuova finestra.

2. Selezionare *File → Nuovo Nuovo segnalibro Live*. Verrà visualizzata una finestra di dialogo.

3. Inserire un nome per il segnalibro Live e aggiungere l'URL, ad esempio, `http://www.novell.com/newsfeeds/rss/coolsolutions.xml`. Firefox mantiene aggiornati i segnalibri Live.

4 Chiudere Gestione segnalibri.

4.4 Utilizzo di Gestione download

Con l'aiuto di Gestione download è possibile tenere traccia di download correnti e passati. Per aprire Gestione download, fare clic su *Strumenti → Download*. Firefox aprirà una finestra contenente i file scaricati. Durante lo scaricamento di un file, verrà visualizzata una barra di progresso e il nome del file corrente. Se necessario è possibile interrompere lo scaricamento e riprenderlo successivamente. Per aprire un file scaricato, fare clic su *Apri*, per rimuoverlo, fare clic su *Rimuovi*. Per informazioni sul file, fare clic con il pulsante destro del mouse sul nome e scegliere *Proprietà*.

Se è necessario un ulteriore controllo su Gestione download, aprire la finestra di configurazione da *Modifica → Preferenze* e selezionare la scheda *Download*. Qui è possibile determinare la cartella per lo scaricamento, il comportamento del gestore e le configurazioni per alcuni tipi di file.

4.5 Personalizzazione di Firefox

Grazie alla possibilità di installare estensioni, modificare i temi e aggiungere parole chiave intelligenti per le ricerche in linea, è possibile una vasta personalizzazione di Firefox.

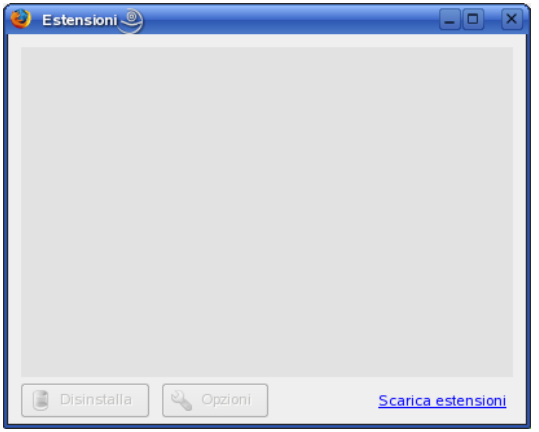
4.5.1 Estensioni

Mozilla Firefox è un'applicazione multifunzionale; è possibile cioè scaricare e installare funzioni aggiuntive, definite estensioni. Ad esempio, è possibile aggiungere un nuovo gestore di download o Mouse Gestures. In questo modo, le dimensioni di Firefox restano contenute.

Per aggiungere un'estensione, fare clic su *Strumenti → Estensioni*. Nell'angolo inferiore destro, fare clic su *Scarica estensioni* per aprire la pagina Web di aggiornamento delle estensioni di Mozilla, dove è possibile scegliere tra una serie di estensioni disponibili. Fare clic sull'estensione da installare, quindi fare clic sul collegamento per scaricarla e installarla. Al successivo riavvio di Firefox, la nuova estensione sarà funzionante. È

anche possibile consultare le varie estensioni all'indirizzo `http://update.mozilla.org/`.

Figura 4.3 *Installazione delle estensioni di Firefox*



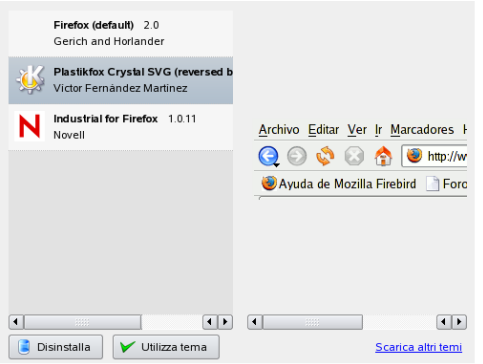
4.5.2 Modifica dei temi

Se si desidera modificare l'aspetto standard di Firefox, installare un nuovo *tema*. I temi non modificano la funzionalità, ma solo l'aspetto del browser. Quando si installa un tema, Firefox chiederà prima conferma. È possibile consentire l'installazione o annullarla. Al termine dell'installazione, sarà possibile abilitare il nuovo tema.

1. Fare clic su *Strumenti* → *Temi*.

2. Verrà visualizzata una nuova finestra di dialogo. Fare clic su *Scarica altri temi*. Se si è già installato un tema, identificarlo nell'elenco, ad esempio Figura 4.4, «Installazione dei temi di Firefox» (p. 92).

Figura 4.4 *Installazione dei temi di Firefox*



3. Verrà visualizzata una nuova finestra con il sito Web `https://update.mozilla.org`.
4. Selezionare un tema e fare clic su *Install Now* (Installa ora).
5. Confermare lo scaricamento e l'installazione.
6. Dopo aver scaricato il tema, verrà visualizzata una finestra di dialogo che elenca i temi. Attivare il nuovo tema mediante l'opzione *Utilizza tema*.
7. Chiudere la finestra e riavviare Firefox.

Se un tema è installato, sarà possibile passare ad un tema differente senza riavviare facendo clic su *Strumenti* → *Temi* quindi su *Utilizza tema*. Se un tema non è più utilizzato, sarà possibile eliminarlo nella stessa finestra di dialogo selezionando *Disinstalla*.

4.5.3 Aggiunta di parole chiave intelligenti alle ricerche in linea

La ricerca su Internet è uno dei compiti principali svolti da un browser. Firefox consente di definire le proprie *parole chiave intelligenti*, abbreviazioni da utilizzare come «comando» per la ricerca sul Web. Ad esempio, se si utilizza spesso Wikipedia, utilizzare una parola chiave intelligente per semplificarne l'utilizzo.

1. Passare a `http://en.wikipedia.org`.

2. Quando Firefox visualizza la pagina Web, identificare il campo per la ricerca testuale. Fare clic con il pulsante destro del mouse su di esso e selezionare *Aggiungi una parola chiave per questa ricerca* nel menu visualizzato.

3. Verrà visualizzata la finestra di dialogo *Aggiungi segnalibro*. Nel campo *Nome*, inserire un nome per questa pagina Web, ad esempio *Wikipedia (en)*.

4. Nel campo *Parola chiave*, immettere un'abbreviazione per questa pagina Web, ad esempio *wiki*.

5. Selezionare la posizione della voce nella sezione segnalibri per mezzo di *Crea in*. È possibile inserirlo in *Ricerche rapide*, ma qualsiasi altro livello è altrettanto valido.

6. Finalizzare con *Aggiungi*.

Si è generata così una nuova parola chiave. Ogni volta sia necessario eseguire una ricerca in Wikipedia, non sarà necessario digitare l'intero URL: sarà sufficiente digitare `wiki Linux` per visualizzare una voce relativa a Linux.

4.6 Stampa da Firefox

Configurare la modalità di stampa del contenuto visualizzato in Firefox dalla finestra di dialogo *Imposta pagina*. Fare clic su *File → Imposta pagina*, quindi selezionare la scheda *Formato e opzioni* per selezionare l'orientamento del lavoro di stampa. È possibile regolare le dimensioni o scegliere l'adattamento automatico della pagina alla larghezza del foglio. Per stampare uno sfondo, selezionare *Stampa lo sfondo (immagini e colori)*. Fare clic sulla scheda *Margini e intestazione/piè di pagina* per regolare i margini e scegliere il contenuto di intestazioni e piè di pagina.

Dopo la configurazione delle impostazioni, stampare una pagina Web selezionando *File → Stampa*. Selezionare la stampante o il file nel quale salvare l'output. Per mezzo di *Proprietà* è possibile impostare le dimensioni del foglio, specificare il comando di stampa, selezionare scala di grigi o colore e determinare i margini. Se si è soddisfatti delle impostazioni, fare clic su *Stampa*.

4.7 Ulteriori informazioni

È possibile ottenere ulteriori informazioni su Firefox per mezzo della home page ufficiale all'indirizzo http://www.mozilla.org/products/firefox/. Per ulteriori informazioni su determinate opzioni o funzioni, consultare la Guida in linea.

5 Linphone - VoIP il desktop Linux

Linphone è una piccola applicazione di telefonia tramite Web ideata per il desktop Linux. La sua funzione è consentire le chiamate tra 2 persone tramite Internet. Non sono necessari speciali componenti hardware, serve solo una postazione fissa standard con una scheda audio correttamente configurata e altoparlanti o cuffie.

5.1 Configurazione di Linphone

Prima di iniziare l'utilizzo di Linphone, è necessario prendere alcune decisioni di base e configurare alcuni parametri. Per iniziare, occorre definire e configurare la modalità di esecuzione di Linphone, definire il tipo di connessione da usare, quindi avviare la configurazione di Linphone (*Go (Passare a)* → *Preferences (Preferenze)*) per effettuare le regolazioni necessarie.

5.1.1 Definizione della modalità di esecuzione di Linphone

Linphone può essere eseguito in 2 diverse modalità a seconda del tipo di desktop usato e della configurazione dello stesso.

Applicazione normale
Dopo l'installazione, il software Linphone può essere avviato tramite i menu delle applicazioni di GNOME e KDE o tramite la riga di comando. Se Linphone non è esecuzione, le chiamate non possono ricevute.

Applet del pannello di GNOME

Linphone può essere aggiunto al pannello di GNOME. Fare clic con il pulsante destro del mouse in una zona vuota del pannello e selezionare *Add to Panel (Aggiungi al pannello)* poi Linphone. Linphone viene in questo modo aggiunto in modo permanente al pannello e automaticamente avviato al login. La sua esecuzione rimane in background fintanto che non vengono ricevute chiamate. L'arrivo di una chiamata apre la finestra principale. Per aprire la finestra principale per chiamare una persona, fare clic sull'icona dell'applet.

5.1.2 Definizione del tipo di connessione

Sono disponibili numerosi metodi per effettuare una chiamata in Linphone. Il modo in cui si effettua una chiamata e in cui si raggiunge l'interlocutore varia a seconda della connessione alla rete o a Internet.

Linphone usa il protocollo SIP (session initiation protocol) per stabilire una connessione a un host remoto. In SIP, ciascun interlocutore è identificato da un URL SIP:

`sip:`*`nomeutente@nomehost`*

`nomeutente` è il login sul computer Linux e *`nomehost`* è il nome del computer che si utilizza. Se si usa un provider SIP, l'URL sarà simile al seguente esempio:

`sip:`*`nomeutente@serversip`*

`nomeutente` è il nome utente scelto durante la registrazione al server SIP. *`serversip`* è l'indirizzo del server SIP o del provider SIP. Per dettagli sulla procedura di registrazione, vedere la Sezione 5.1.5, «Configurazione delle opzioni SIP» (p. 99) e consultare la documentazione sulla registrazione fornita dal provider. Per un elenco dei provider adatti a questo scopo, vedere le pagine Web menzionate in Sezione 5.8, «Ulteriori informazioni» (p. 106).

L'URL da usare varia a seconda del tipo di connessione scelta. Se si chiama direttamente senza ulteriori instradamenti via un provider SIP, digitare l'URL del primo tipo. Se si chiama via un server SIP, digitare l'URL del secondo tipo.

Chiamata nell'ambito della stessa rete

Per chiamare una persona appartenente alla stessa rete, è sufficiente conoscere il nome utente e il nome host per creare un URL SIP valido. Il ragionamento è identico per

essere chiamati da questa stessa persona. Fintanto che non esiste un firewall tra due persone, non è necessaria alcuna ulteriore configurazione.

Chiamata tramite reti o Internet (configurazione IP statico)

Per essere chiamati quando si è connessi a Internet tramite indirizzo IP statico, è sufficiente disporre del nome utente e del nome host o indirizzo IP della postazione per creare un URL SIP valido, come descritto nella sezione chiamata «Chiamata nell'ambito della stessa rete» (p. 96). Se il chiamante o il chiamato si trovano dietro un firewall che filtra il traffico in arrivo e in uscita, aprire la porta SIP (`5060`) e la porta RTP (`7078`) sul computer firewall per abilitare il traffico Linphone attraverso il firewall.

Chiamata tramite reti o Internet (configurazione IP dinamico)

Se l'indirizzo IP non è statico (cioè se viene assegnato un nuovo indirizzo a ogni connessione a Internet), è impossibile creare un URL SIP valido in base a nome utente e indirizzo IP. In questi casi, per accertarsi che un chiamante esterno riesca a connettersi al computer host corretto, usare i servizi offerti da un provider SIP o usare una configurazione DynDNS. Per ulteriori informazioni su DynDNS, vedere `http://en.wikipedia.org/wiki/Dynamic_DNS`.

Chiamata tramite reti e firewall

I computer nascosti dietro un firewall non rivelano il proprio indirizzo IP su Internet. Di conseguenza, non possono essere direttamente rintracciati da coloro che tentano di chiamare l'utente che vi lavora. Linphone supporta le chiamate oltre i confini della rete e del firewall usando un proxy SIP o inoltrando le chiamate a un provider SIP. Per una descrizione dettagliata sulle regolazioni necessarie per l'utilizzo di un server SIP esterno, vedere la Sezione 5.1.5, «Configurazione delle opzioni SIP» (p. 99).

5.1.3 Configurazione dei parametri di rete

La maggior parte delle impostazioni contenute nella scheda *Network (Rete)* non richiede ulteriori regolazioni. In pratica, è possibile effettuare chiamate senza modificare queste impostazioni.

NAT Traversal Options (Opzioni NAT trasversale)
Abilitare questa opzione solo se ci si trova in una rete privata dietro un firewall e se non si usa un provider SIP per inoltrare le chiamate. Selezionare la casella di controllo e immettere l'indirizzo IP del computer firewall con notazione del punto, ad esempio, `192.168.34.166`.

RTP Properties (Proprietà RTP)
Linphone usa il protocollo RTP (real-time transport) per trasmettere i dati audio delle chiamate. La porta per RTP è impostata su `7078` e non deve essere modificata, a meno che questa sia usata da un'altra applicazione. Il parametro di compensazione del jitter è usato per controllare il numero di pacchetti audio che vengono accumulati nel buffer prima della loro riproduzione. Aumentare questo parametro per migliorare la qualità della trasmissione. Maggiore il numero di pacchetti accumulati nel buffer, maggiore sarà la probabilità che i «pacchetti ritardatari» vengano riprodotti. D'alto canto, l'aumento del numero di pacchetti accumulati nel buffer aumenta anche i tempi di latenza - la voce dell'interlocutore giunge con un certo ritardo. Modificare questo parametro tenendo conto di questi due fattori.

Other (Altro)
Se si usa una combinazione di telefonia VoIP e fissa, è possibile usare la tecnologia DTMF (dual tone multiplexed frequency) per innescare determinate azioni, come il controllo a distanza della casella vocale digitando una precisa sequenza di tasti. Linphone supporta 2 protocolli per la trasmissione DTMF, SIP INFO e RTP rfc2833. Per abilitare la funzionalità DTMF in Linphone, scegliere un provider SIP che supporti uno di questi protocolli. Per un elenco completo dei provider VoIP, vedere la Sezione 5.8, «Ulteriori informazioni» (p. 106).

5.1.4 Configurazione della scheda audio

Se la scheda di rete è stata correttamente rilevata da Linux, Linphone la usa automaticamente come scheda audio di default. Lasciare invariato il valore di *Use sound device (Usa scheda audio)*. Usare *Recording source (Fonte di registrazione)* per

determinare la fonte di registrazione da usare. Nella maggior parte dei casi, si tratta del microfono (`micro`). Per selezionare una suoneria personalizzata, usare *Browse (Sfoglia)*, sceglierne una e provarla con *Listen (Ascolta)*. Fare clic su *Apply (Applica)* per accettare le modifiche.

5.1.5 Configurazione delle opzioni SIP

La finestra di dialogo *SIP* contiene tutte le impostazioni per la configurazione del protocollo SIP.

SIP Port (Porta SIP)
Definire la porta se cui eseguire l'agente SIP. La porta di default per SIP è `5060`. Lasciare questo valore invariato salvo se un'altra applicazione o protocollo usano questa porta.

Identity (Identità)
Per essere raggiunti direttamente senza usare un proxy SIP o un provider SIP, è necessario comunicare al chiamante il proprio indirizzo SIP valido. Linphone è in grado di creare un indirizzo SIP valido.

Remote Services (Servizi remoti)
Questo elenco contiene uno o più provider di servizi SIP presso cui è stato creato un conto. Le informazioni relative al server possono essere aggiunte, modificate o cancellate in qualsiasi momento. Per saperne di più sulla procedura di registrazione, vedere Aggiunta di un proxy SIP e registrazione presso un server SIP remoto (p. 100).

Authentication Information (Informazioni di autenticazione)
Per registrare presso un server SIP remoto, è necessario fornire i dati di autenticazione come nome utente e parola d'ordine. Una volta forniti, questi dati vengono memorizzati da Linphone. Per cancellare questi dati per motivi di sicurezza, fare clic su *Clear all stored authentification data (Cancella tutti i dati di autenticazione memorizzati)*.

L'elenco *Remote services (Servizi remoti)* può contenere più indirizzi di proxy o provider di servizi SIP remoti.

Procedura 5.1 *Aggiunta di un proxy SIP e registrazione presso un server SIP remoto*

1. Scegliere un provider SIP adatto e registrarsi per creare un conto utente.
2. Avviare Linphone.
3. Scegliere *Passare a → Preferenze → SIP*.
4. Fare clic su *Add proxy/registrar (Aggiungi proxy/Registra)* per aprire un modulo di registrazione.
5. Valorizzare i campi *Registration Period (Periodo di registrazione)*, *SIP Identity (Identità SIP)*, *SIP Proxy (Proxy SIP)* e *Route (Instradamento)*. Se si è protetti da firewall, selezionare sempre *Send registration (Invia registrazione)* e immettere un valore appropriato per *Registration Period (Periodo di registrazione)*. In questo modo, i dati della registrazione vengono rinviati dopo un dato periodo di tempo per mantenere il firewall aperto a livello delle porte richieste da Linphone. Altrimenti, queste porte verrebbero automaticamente chiuse se il firewall non ricevesse nuovi pacchetti di questo tipo. Il rinvio dei dati della registrazione è necessario anche per mantenere il server SIP informato riguardo lo stato corrente della connessione e l'ubicazione del chiamante. Per il campo *SIP identity (Identità SIP)* digitare l'URL SIP da usare per le chiamate locali. Per usare questo server anche come proxy SIP, digitare gli stessi dati per il campo *SIP Proxy (Proxy SIP)*. Infine se necessario, aggiungere un instradamento e scegliere *OK* per chiudere la finestra.

5.1.6 Configurazione dei codec audio

Linphone supporta numerosi codec per la trasmissione dei dati vocali. Impostare il tipo di connessione e scegliere i codec preferiti dall'elenco. I codec non adatti al tipo di connessione scelto compaiono in rosso e non possono essere selezionati.

5.2 Test di Linphone

Per testare la configurazione di Linphone, usare `sipomatic`, un piccolo programma di test in grado di rispondere alle chiamate effettuate da Linphone.

Procedura 5.2 *Test di una configurazione Linphone*

1. Aprire un terminale.
2. Immettere `sipomatic` nella riga di comando.
3. Avviare Linphone.
4. Immettere `sip:robot@127.0.0.1:5064` come *SIP address (Indirizzo SIP)* e fare clic su *Call or Answer (Chiama o rispondi)*.
5. Se Linphone è configurato correttamente, verrà emessa una suoneria seguita dopo breve tempo da un beve annuncio.

Se la procedura viene completata correttamente, significa che la configurazione audio e di rete sono funzionanti. Se il test fallisce, accertarsi che la scheda audio sia correttamente configurata e che il livello di riproduzione sia impostato a livelli ragionevoli. Se l'audio rimane assente, verificare la configurazione di rete inclusi i numeri di porta per SIP e RTP. Se le porte di default sono usate da un'altra applicazione o protocollo, modificarle e riprovare.

5.3 Composizione di una chiamata

Se Linphone è configurato correttamente, la composizione di una chiamata è un'operazione semplice. La procedura di chiamata varia a seconda del tipo di chiamata (vedere la Sezione 5.1.2, «Definizione del tipo di connessione» (p. 96)).

1. Avviare Linphone tramite il menu o la riga di comando.
2. Immettere l'indirizzo SIP della persona da chiamare in *SIP address (Indirizzo SIP)*. L'indirizzo deve avere il formato `sip:nomeutente@nomedominio` o `nomeutente@nomehost` per le chiamate dirette locali oppure `nomeutente@serversip` o `idutente@serversip` per le chiamate tramite proxy o le chiamate tramite un provider SIP.
3. Se si usa un provider o un proxy SIP, selezionare il proxy o provider appropriato da *Proxy to use (Proxy da usare)* e fornire i dati di autenticazione richiesti da tale proxy.

4. Fare clic su *Call or Answer (Chiama o rispondi)* e attendere che il chiamato risponda.

5. Per terminare una chiamata, fare clic su *Release or Refuse (Termina o rifiuta)* e chiudere Linphone.

Per regolare i parametri audio durante una chiamata, fare clic su *Show more (Altro)* per aprire 4 schede con ulteriori opzioni. La prima *Sound (Suono)* contiene le opzioni per *Playback level (Livello di riproduzione)* e *Recording level (Livello di registrazione)*. Per regolare entrambi i volumi, servirsi dei cursori.

La scheda *Presence (Presenza)* consente di impostare lo stato dell'utente. Queste informazioni vengono comunicate a tutti coloro che tentano di contattare l'utente. Se si è costantemente assenti e si intende informarne i chiamanti, selezionare *Away (Assente)*. Se si è al momento occupati ma disponibili più tardi, selezionare *Busy, I'll be back in ... min (Occupato, torno tra ... min)* e specificare tra quanto tempo si sarà disponibili. Quando si è di nuovo raggiungibili, impostare lo stato al valore di default *Reachable (Raggiungibile)*. La propria visibilità nei riguardi degli altri utenti è definita dai valori di *Subscribe Policy (Politica di sottoscrizione)* impostati nella rubrica, come descritto nella Sezione 5.5, «Utilizzo della rubrica» (p. 103). Lo stato degli utenti presenti in rubrica può essere monitorato tramite la scheda *My online friends (Amici in linea)*.

La scheda *DTMF* può essere usata per immettere codici DTMF per verificare la casella vocale. Per verificare la casella vocale, immettere l'indirizzo SIP appropriato e usare il tastierino della scheda *DTMF* per digitare il codice della casella vocale. Infine, fare clic su *Call or Answer (Chiama o rispondi)* come se fosse una normalissima chiamata.

5.4 Risposta a una chiamata

I metodi di notifica di una chiamata in arrivo variano a seconda della modalità di esecuzione selezionata per Linphone:

Applicazione normale
: Le chiamate in arrivo possono essere ricevute solo se Linphone è già in esecuzione. Verrà emessa una suoneria attraverso le cuffie o gli altoparlanti. Se Linphone non è esecuzione, le chiamate non possono ricevute.

Applet del pannello di GNOME
Di norma, l'applet del pannello per Linphone viene eseguita in modo invisibile senza segnali esterni. Questo stato cambia non appena giunge una chiamata: la finestra principale di Linphone viene visualizzata e viene emesso una suoneria attraverso le cuffie o gli altoparlanti.

Non appena viene notificata una chiamata in arrivo, fare clic su *Call or Answer (Chiama o rispondi)* per "alzare la cornetta" e iniziare a parlare. Per rifiutare la chiamata, fare clic su *Release or Refuse (Termina o rifiuta)*.

5.5 Utilizzo della rubrica

Linphone offre delle funzioni per la gestione dei contatti SIP. Per aprire la rubrica, scegliere *Go (Passare a)* → *Address book (Rubrica)*. Verrà visualizzato un elenco vuoto. Fare clic su *Add (Aggiungi)* per aggiungere un contatto.

Per attivare un contatto, è necessario valorizzare i seguenti campi:

Name (Nome)
Digitare il nome del contatto. Nel campo è possibile digitare il nome completo o un soprannome. Scegliere un nome facile da ricordare. Se si sceglie di monitorare lo stato in linea di questa persona, il nome verrà visualizzato nella scheda *My online friends (Amici in linea)* della finestra principale.

SIP Address (Indirizzo SIP)
Immettere un indirizzo SIP valido per il contatto.

Proxy to Use (Proxy da usare)
Se necessario, immettere il proxy da usare per questa connessione. Nella maggior parte dei casi, si tratta dell'indirizzo SIP del server SIP che si usa.

Subscribe Policy (Politica di sottoscrizione)
La politica di sottoscrizione determina la propria visibilità per gli altri.

Per chiamare un contatto dalla rubrica, selezionarlo con il mouse, fare clic su *Select (Seleziona)* per visualizzare l'indirizzo nell'apposito campo della finestra principale, quindi comporre normalmente la chiamata con *Call or Answer (Chiama o rispondi)*.

5.6 Risoluzione dei problemi

Ho provato a chiamare una persona, ma non sono riuscito a stabilire una connessione.

I motivi che impediscono una chiamata sono molteplici:

La connessione a Internet è interrotta.

Poiché Linphone usa Internet per inoltrare le chiamate, accertarsi che il computer sia correttamente connesso e configurato per Internet. Per verificare se il computer è connesso o meno, aprire una pagina Web nel browser. Se la connessione Internet è attiva, forse il chiamato non è raggiungibile.

La persona chiamata non è raggiungibile.

La persona chiamata può avere rifiutato la chiamata. In quel momento Linphone non è in esecuzione nel computer della persona chiamata. La connessione Internet della persona chiamata è interrotta.

La chiamata giunge a destinazione ma non sento nulla.

Primo, accertarsi che la scheda audio sia correttamente configurata. Per fare ciò, avviare qualsiasi altra applicazione che emette suoni, ad esempio un lettore multimediale. Accertarsi che Linphone abbia sufficienti autorizzazioni per aprire questo dispositivo. Chiudere tutti gli altri programmi che usano la scheda audio per evitare conflitti.

Se i problemi persistono malgrado le verifiche sopra citate, alzare i livelli di registrazione e di riproduzione nella scheda *Sound (Suono)*.

La voce emessa presso entrambi gli interlocutori risulta discontinua.

Tentare di regolare il buffer del jitter tramite *RTP properties (Proprietà RTP)* in *Preferences (Preferenze) → Network (Rete)* per compensare i pacchetti audio ritardatari. Notare che tale operazione prolunga i tempi di latenza.

La funzione DTMF non funziona.

Non è stato possibile stabilire una connessione durante il tentativo di verifica della casella vocale con il tastierino DTMF. Esistono 3 protocolli per la trasmissione dei dati DTMF, ma solo 2 di questi sono supportati da Linphone (SIP INFO e RTP rfc2833). Contattare il provider per verificare quali di questi sono supportati. Il protocollo di default usato da Linphone è rfc2833, ma se questo fallisce impostarlo su SIP INFO in *Preferences (Preferenze) → Network (Rete) → Other (Altro)*. Se

nessuno dei due protocolli funziona, significa che non è possibile usare Linphone per la trasmissione DTMF.

5.7 Glossario

Di seguito vengono date alcune brevi spiegazioni riguardo i termini tecnici e i protocolli più importanti citati nel presente documento:

DTMF
Un codificatore DTMF, come un telefono normale, usa copie di toni per rappresentare i vari tasti. Ciascun tasto è associato a una combinazione univoca costituita da un tono alto e da uno basso. Un decodificatore riconverte poi queste combinazioni di toni in numeri. Linphone supporta i segnali DTMF per innescare azioni remote, come la verifica della casella vocale.

codec
I codec sono algoritmi appositamente ideati per comprimere dati audio e video.

jitter
Jitter è la variabilità della latenza (ritardo) in una connessione. I dispositivi audio o i sistemi di connessione, come ISDN o PSTN, richiedono un continuo flusso di dati. Per compensare questo requisito, i terminali e i gateway VoIP applicano un buffer del jitter che raccoglie i pacchetti prima di inoltrarli verso i dispositivi audio o le linee di connessione, tipo ISDN. Aumentando la dimensione del buffer del jitter, si diminuisce la probabilità di perdita di dati ma si aumenta la latenza della connessione.

RTP
RTP è l'acronimo di *real-time transport protocol (protocollo di trasporto in tempo reale)*. Esso consente il trasporto di flussi multimediali su reti e richiede UDP. I dati vengono trasmessi tramite pacchetti discreti numerati e catalogati con data/ora per consentire una sequenza corretta e identificazione di quelli persi.

SIP
SIP è l'acronimo di *session initiation protocol (protocollo di iniziazione di sessione)*. Questo protocollo serve a stabilire le sessioni multimediali. Nel contesto di Linphone, SIP è il meccanismo che innesca la suoneria presso il computer chiamato, avvia la chiamata e che la termina non appena si "mette giù la cornetta". La trasmissione vera e propria dei dati vocali è gestita da RTP.

VoIP

VoIP è l'acronimo di *voice over Internet protocol (voce tramite protocollo Internet)*. Questa tecnologia consente la trasmissione di chiamate telefoniche normali tramite Internet per mezzo di pacchetti instradati. Le informazioni vocali vengono inviate tramite pacchetti discreti come qualsiasi altro pacchetto di dati trasmesso su Internet via IP.

5.8 Ulteriori informazioni

Per informazioni generali su VoIP, consultare VoIP Wiki all'indirizzo http://voip-info.org/tiki-index.php. Per un elenco completo dei provider che offrono servizi VoIP nel proprio paese, vedere http://voip-info.org/wiki-VOIP+Service+Providers+Residential.

6 Cifratura con KGpg

KGpg è un componente importante dell'infrastruttura di cifratura del sistema. Questo programma consente di generare e gestire tutte le chiavi richieste nonché utilizzare la relativa funzione dell'editor per la creazione e la cifratura rapida dei file o usare l'applet del pannello per eseguire la cifratura o la decifratura mediante trascinamento e rilascio. In altri programmi, ad esempio i programmi di posta (Kontact o Evolution), è possibile accedere ai dati delle chiavi per elaborare il contenuto firmato o cifrato. Nel presente capitolo sono descritte le funzioni di base richieste per la normale gestione dei file cifrati.

6.1 Generazione di una nuova coppia di chiavi

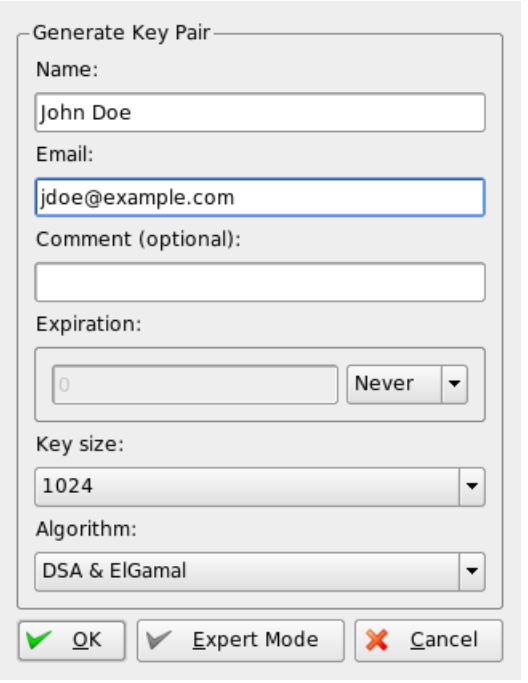
Per poter scambiare messaggi cifrati con altri utenti, è necessario innanzitutto generare una coppia di chiavi personalizzata. Una parte della chiave, ovvero la *chiave pubblica*, viene distribuita ai partner di comunicazione e può essere utilizzata per cifrare i file o i messaggi di e-mail da inviare. L'altra parte della coppia di chiavi, ovvero la *chiave privata*, viene utilizzata per decifrare il contenuto cifrato.

IMPORTANTE: Confronto tra chiave privata e chiave pubblica

La chiave pubblica è destinata al pubblico e deve essere distribuita a tutti i partner di comunicazione. Al contrario, la chiave privata deve essere nota solo all'utente a cui appartiene. È consigliabile evitare che altri utenti abbiano accesso a questi dati.

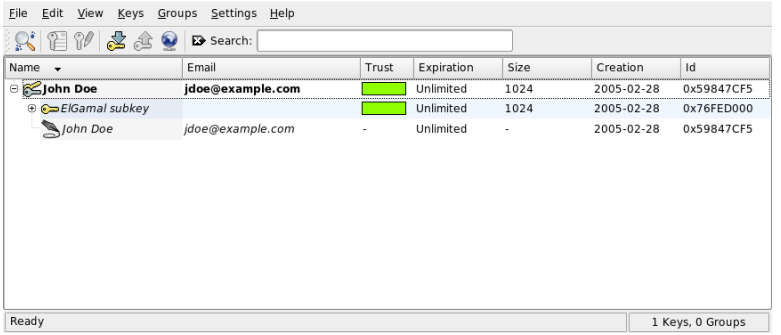
Per avviare KGpg dal menu principale selezionare *Utility* → *KGpg* oppure immettere `kgpg` nella riga di comando. Al primo avvio del programma verrà visualizzato un assistente per facilitare la configurazione. Seguire le istruzioni fino alla fase in cui viene richiesta la creazione di una chiave. Immettere un nome, un indirizzo e-mail e se necessario un commento. Per modificare le impostazioni di default, scegliere l'ora di scadenza della chiave, la sua dimensione e l'algoritmo di cifratura utilizzato. Vedere la Figura 6.1, «KGpg: Creazione di una chiave» (p. 108).

Figura 6.1 *KGpg: Creazione di una chiave*



Confermare le impostazioni premendo *OK*. La finestra di dialogo successiva richiede di immettere due volte una parola d'ordine. Il programma quindi genera la coppia di chiavi e visualizza un riepilogo. Si consiglia di stampare o salvare subito un certificato di revoca. Tale certificato sarà necessario per revocare la chiave privata nel caso in cui si dimentichi la parola d'ordine. Confermare con *OK*; KGpg visualizza la finestra principale. Vedere la Figura 6.2, «Gestione chiavi» (p. 109).

Figura 6.2 *Gestione chiavi*



6.2 Esportazione della chiave pubblica

Dopo aver generato la coppia di chiavi, è necessario rendere disponibile la chiave pubblica ad altri utenti. In questo modo si consente loro di cifrare o firmare i file e i messaggi inviati. Per rendere la chiave pubblica disponibile ad altri utenti, selezionare *Chiavi → Esporta chiavi pubbliche*. Verrà visualizzata una finestra di dialogo in cui sono incluse quattro opzioni:

E-mail
: La chiave pubblica viene inviata tramite e-mail al destinatario scelto. Se si attiva questa opzione e si conferma con *OK*, verrà visualizzata la finestra di dialogo per la creazione di un nuovo messaggio di e-mail con KMail. Immettere il destinatario e fare clic su *Invia*. Il destinatario riceverà la chiave e sarà in grado di inviare contenuto cifrato.

Appunti
: Prima di continuare l'elaborazione della chiave pubblica, è possibile inserirla negli Appunti.

Server chiavi di default
: Per rendere la chiave pubblica disponibile a un numero di utenti maggiore, è sufficiente esportarla in un server delle chiavi su Internet. Per ulteriori informazioni, vedere la Sezione 6.4, «Finestra server delle chiavi» (p. 111).

File

Se si preferisce distribuire la chiave in un file tramite un supporto dati anziché inviarla tramite e-mail, selezionare questa opzione, quindi confermare o modificare il nome e il percorso del file, quindi fare clic su *OK*.

6.3 Importazione delle chiavi

Se si riceve una chiave in un file (ad esempio come allegato di e-mail), è possibile inserire tale chiave nell'apposito contenitore con *Importa chiave* e utilizzarla per stabilire comunicazioni cifrate con il mittente. La procedura è simile a quella utilizzata per l'esportazione delle chiavi riportata in precedenza.

6.3.1 Firma delle chiavi

Le chiavi possono essere firmate come qualsiasi altro file per garantirne autenticità e integrità. Se si è assolutamente certi che la chiave importata appartenga all'utente specificato come proprietario, è possibile apporre la propria firma alla chiave per confermarne l'autenticità.

IMPORTANTE: Consolidamento dell'attendibilità del Web

Le comunicazioni cifrate sono sicure solo per il fatto che è possibile associare senza alcun dubbio le chiavi pubbliche in circolazione all'utente specificato. Mediante il controllo incrociato e la firma delle chiavi, si contribuisce al consolidamento dell'attendibilità del Web.

Selezionare la chiave da firmare nell'elenco delle chiavi. Selezionare *Chiavi → Firma chiavi*. Nella finestra di dialogo visualizzata, indicare la chiave privata da utilizzare per la firma. Prima di apporre la firma, verrà visualizzato un avviso in cui viene indicato di verificare l'autenticità della chiave. Se la verifica è già stata eseguita, fare clic su *Continua* e immettere la parola d'ordine per la chiave privata selezionata nel passaggio successivo. La firma può ora essere verificata da altri utenti mediante l'utilizzo della chiave pubblica.

6.3.2 Affidabilità delle chiavi

Di norma, il programma corrispondente richiede all'utente di confermare l'attendibilità della chiave; in altre parole confermare che la chiave sia effettivamente utilizzata dal legittimo proprietario. Ciò si verifica ogni volta che un messaggio deve essere decifrato o una firma verificata. Per evitare ciò, modificare il livello di attendibilità della nuova chiave importata.

Per accedere a un piccolo menu contestuale per la gestione delle chiavi, fare clic con il pulsante destro del mouse sulla chiave appena importata. Nel menu, selezionare *Modifica chiavi in terminale*. In KGpg verrà aperta una console di testo in cui è possibile impostare il livello di affidabilità mediante pochi comandi.

Al prompt della console di testo (`Comando >`), immettere `trust`. Utilizzando una scala da `1` (non sicuro) a `5` (completamente affidabile) valutare la certezza che i firmatari della chiave importata abbiano verificato la reale identità del proprietario della chiave. Immettere il valore selezionato al prompt (`Decisione dell'utente`). Se si è sicuri riguardo l'affidabilità del firmatario, immettere `5`. Rispondere alla seguente domanda digitando `y`. Infine, immettere `quit` per uscire dalla console e ritornare all'elenco delle chiavi. Il livello di affidabilità impostato per la chiave è `Definitivo`.

Il livello di affidabilità delle chiavi nel contenitore è indicato da una barra colorata accanto al nome della chiave. Minore è il livello di affidabilità, inferiore sarà la certezza che il firmatario della chiave abbia verificato la reale identità delle chiavi firmate. È possibile che l'utente sia completamente certo dell'identità del firmatario, ma che quest'ultimo non verifichi l'identità delle altre persone prima di firmarne le chiavi. Di conseguenza, il firmatario e la sua chiave rimangono affidabili, ma è consigliabile assegnare livelli di affidabilità inferiori alle chiavi di altri che sono state da lui firmate. Il livello di affidabilità è esclusivamente a scopi di promemoria; non attiva alcuna azione automatica di KGpg.

6.4 Finestra server delle chiavi

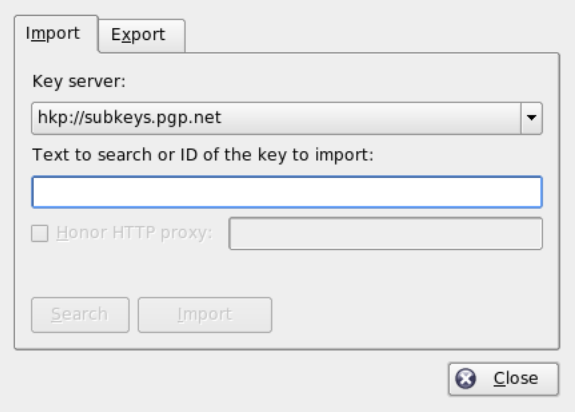
Alcuni server delle chiavi basati su Internet includono le chiavi pubbliche di molti utenti. Per stabilire comunicazioni cifrate con un numero elevato di utenti, è possibile utilizzare i server per distribuire la chiave pubblica. A questo scopo, è necessario esportare la chiave pubblica in uno dei server. Analogamente, KGpg consente la ricerca delle chiavi degli utenti nei server e l'importazione delle relative chiavi pubbliche dal

server. Aprire la finestra di dialogo Server delle chiavi selezionando *File* → *Server delle chiavi*.

6.4.1 Importazione di una chiave da un server delle chiavi

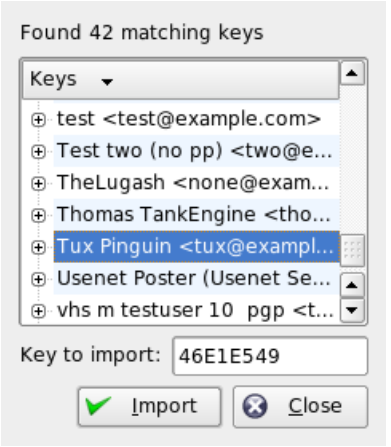
Mediante l'utilizzo della scheda *Importa* nella finestra del server delle chiavi, importare le chiavi pubbliche da uno dei server delle chiavi basati su Internet. Utilizzare il menu a discesa per selezionare uno dei server delle chiavi preconfigurati e immettere una stringa di ricerca (indirizzo di e-mail del partner di comunicazione) o l'ID della chiave da trovare. Quando si fa clic su *Ricerca*, verrà stabilita la connessione a Internet e nel server delle chiavi specificato verrà eseguita la ricerca della chiave che corrisponde alle specifiche. Vedere la Figura 6.3, «Schermata di ricerca per l'importazione di una chiave» (p. 112).

Figura 6.3 *Schermata di ricerca per l'importazione di una chiave*



Se la ricerca nel server delle chiavi ha esito positivo, in una nuova finestra verrà visualizzato un elenco di tutte le voci recuperate dal server. Selezionare la chiave da inserire nel contenitore e fare clic su *Importa*. Vedere la Figura 6.4, «Risultati e importazione» (p. 113). Scegliere *OK* per confermare il messaggio successivo, quindi uscire dalla finestra di dialogo Server delle chiavi con *Chiudi*. La chiave importata, visualizzata nella panoramica principale di gestione chiavi, è pronta per l'uso.

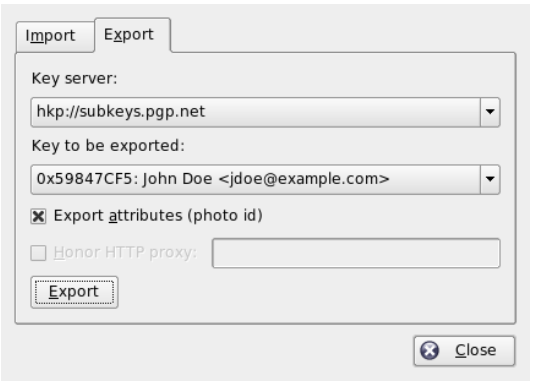
Figura 6.4 *Risultati e importazione*



6.4.2 Esportazione delle chiavi in un server delle chiavi

Per esportare una chiave in uno dei server delle chiavi liberamente accessibili su Internet, selezionare la scheda *Esporta* nella finestra Server delle chiavi. Specificare il server di destinazione e la chiave da esportare mediante l'utilizzo dei due menu a discesa. Quindi avviare l'esportazione con *Esporta*.

Figura 6.5 *Esportazione di una chiave in un server delle chiavi*



6.5 Cifratura di file e testo

KGpg offre anche la possibilità di cifrare il testo o il contenuto degli Appunti. Fare clic sull'icona con il lucchetto per visualizzare le opzioni *Cifra appunti* e *Decifra appunti* nonché l'opzione per l'apertura dell'editor integrato.

6.5.1 Cifratura e decifratura degli Appunti

I file copiati negli Appunti possono essere cifrati in modo semplice e rapido. Fare clic sull'icona di KGpg per visualizzare la panoramica delle funzioni. Selezionare *Cifra appunti* e specificare la chiave da utilizzare. Sul desktop verrà visualizzato un messaggio di stato relativo alla procedura di cifratura. È quindi possibile elaborare il contenuto cifrato degli Appunti in base alle proprie esigenze. La decifratura del contenuto degli Appunti è altrettanto semplice. È sufficiente aprire il menu del pannello, selezionare *Decifra appunti*, quindi immettere la parola d'ordine associata alla chiave privata. La versione decifrata è pronta per essere elaborata negli Appunti e nell'editor di KGpg.

6.5.2 Cifratura e decifratura mediante trascinamento e rilascio

Per cifrare e decifrare i file, è possibile fare clic sulle icone presenti sul desktop o nel file manager, trascinarle in corrispondenza del lucchetto nel pannello e rilasciarle. Se il file non è cifrato, in KGpg verrà chiesto di specificare la chiave da utilizzare. Dopo aver selezionato una chiave, il file viene cifrato e non verranno visualizzati altri messaggi. Nel file manager, i file cifrati vengono indicati dal suffisso `.asc` e dall'icona con il lucchetto. Per decifrare i file, è sufficiente fare clic sull'icona del file, trascinarla in corrispondenza del simbolo di KGpg nel pannello e rilasciarla. È quindi necessario specificare se il file verrà decifrato e salvato o visualizzato nell'editor.

6.5.3 Editor di KGpg

Anziché creare il contenuto da cifrare in un editor esterno e cifrare poi il file con uno dei metodi sopra riportati, è possibile utilizzare l'editor integrato di KGpg per la creazione del file. È sufficiente aprire l'editor (*Apri editor* dal menu contestuale), immettere il testo desiderato e fare clic su *Cifra*. Quindi selezionare la chiave da utilizzare e

completare la procedura di cifratura. Per decifrare i file, utilizzare *Decifra* e immettere la parola d'ordine associata alla chiave.

La procedura di generazione e controllo delle firme è facile quanto la cifratura eseguita direttamente dall'editor. Scegliere *Firma → Genera firma*, quindi selezionare il file da firmare nella finestra di dialogo dei file. Indicare la chiave privata da utilizzare e immettere la parola d'ordine associata. In KGpg verrà indicato se la generazione della firma è stata eseguita in modo corretto. Se si decide di firmare i file nell'editor, è sufficiente fare clic su *Firma/Verifica*. Per verificare un file firmato, scegliere *Firma → Verifica firma* e selezionare il file da controllare nella finestra di dialogo visualizzata. Dopo aver confermato la selezione, in KGpg viene eseguito il controllo della firma e indicato il risultato dell'operazione. In alternativa, è possibile caricare il file firmato nell'editor e fare clic su *Firma/Verifica*.

6.6 Ulteriori informazioni

Per informazioni di base sul metodo di cifratura, consultare l'introduzione disponibile nelle pagine dedicate al progetto GnuPG all'indirizzo `http://www.gnupg.org/documentation/howtos.html.en`. Questo documento fornisce inoltre un elenco di altre fonti di informazioni.

Parte III. Multimedia

7 Suono in Linux

Linux include un'ampia gamma di applicazioni audio e multimediali. Alcune di queste applicazioni fanno parte di uno degli ambienti desktop principali. Le applicazioni descritte in questo capitolo consentono di controllare il volume e il bilanciamento della riproduzione, di riprodurre CD e file musicali, nonché di registrare e comprimere i dati audio.

7.1 Mixer

I mixer forniscono uno strumento per il controllo del volume e il bilanciamento dell'audio in uscita e in entrata nel computer. La differenza principale tra i vari mixer consiste nell'aspetto dell'interfaccia utente. Esistono tuttavia numerosi mixer progettati per componenti hardware specifici. envy24control, ad esempio, è un mixer per il chip audio Envy 24, mentre hdspmixer è progettato per le schede RME Hammerfall. È possibile selezionare il mixer più adatto alle proprie esigenze tra quelli disponibili.

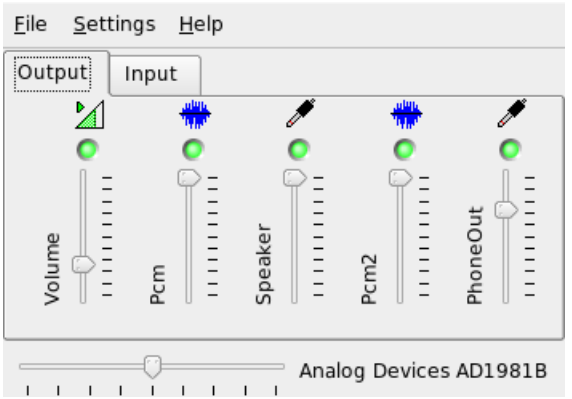
SUGGERIMENTO: Test del mixer

È in genere consigliabile avviare il mixer prima di aprire altre applicazioni audio. Utilizzare il mixer per verificare e regolare le impostazioni di controllo dell'audio in uscita e in entrata nella scheda audio.

7.1.1 Applet del mixer di KDE

KMix è l'applicazione del mixer di KDE. Si tratta di un'applet integrata del pannello di KDE e collocata sulla barra delle applicazioni. Fare clic sull'icona del pannello per controllare il volume degli altoparlanti mediante l'apposito dispositivo di scorrimento. Per visualizzare il menu di scelta rapida di KMix, fare clic con il pulsante destro del mouse sull'icona. Selezionare *Mute (Disattiva audio)* per disattivare l'output audio. L'aspetto dell'icona del pannello viene quindi modificato. Se si fa di nuovo clic su *Mute (Disattiva audio)* il volume viene riattivato. Per ottimizzare le impostazioni dell'audio, selezionare *Show Mixer Window (Mostra finestra del mixer)* e configurare *Output (Output)*, *Input (Input)* e *Switches (Switch)*. Per ognuno dei dispositivi utilizzati è disponibile un menu di scelta rapida diverso a cui è possibile accedere facendo clic con il pulsante destro del mouse sull'icona corrispondente. È possibile disattivare o nascondere ognuno di questi in modo indipendente.

Figura 7.1 *Mixer KMix*

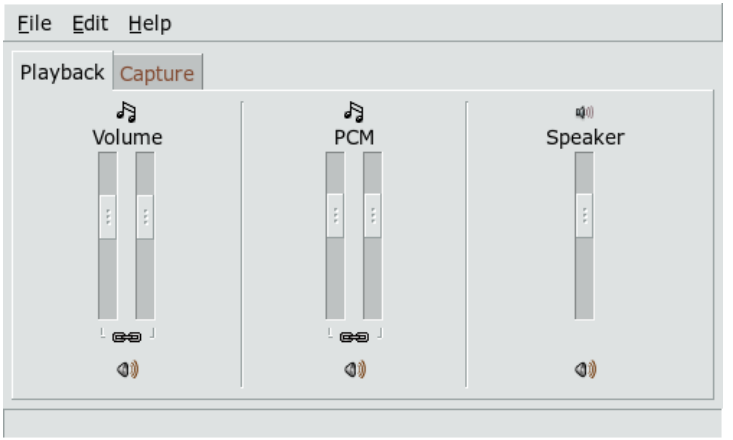


7.1.2 Applet del mixer di GNOME

GMix è l'applet di controllo del volume integrata nel pannello del desktop GNOME. Fare clic sull'icona del pannello per controllare il volume degli altoparlanti mediante l'apposito dispositivo di scorrimento. Per disattivare l'output audio, fare clic con il pulsante destro del mouse sull'icona e scegliere *Mute (Disattiva audio)*. L'aspetto dell'icona di controllo del volume viene quindi modificato. Per riattivare l'output audio, fare di nuovo clic con il pulsante destro del mouse sull'icona e scegliere *Mute (Disattiva*

audio) nel menu. Scegliere *Open Volume Control (Apri Controllo volume)* per accedere alle funzionalità avanzate del mixer, illustrate nella Figura 7.2, «Applet del mixer di GNOME» (p. 121). Ogni dispositivo audio è dotato della propria scheda mixer.

Figura 7.2 *Applet del mixer di GNOME*



7.1.3 alsamixer

È possibile eseguire alsamixer dalla riga di comando senza l'ambiente X. È quindi possibile controllare tutte le funzioni mediante tasti di scelta rapida. La finestra di alsamixer include sempre gli elementi seguenti: una riga superiore contenente informazioni di base sul tipo di chip e scheda, il tipo di visualizzazione selezionato e l'elemento del mixer e quindi, sotto l'area delle informazioni, le barre del volume. Premere ← e → per scorrere a sinistra o a destra se i controlli non vengono visualizzati in un'unica schermata. I nomi dei controlli si trovano sotto i controlli stessi. Il controllo attualmente selezionato viene visualizzato in rosso. È possibile disattivare e riattivare qualsiasi controllo del mixer premendo M. Sotto i controlli disattivati viene visualizzata l'indicazione *MM (MM)*. I controlli dotati di funzionalità di cattura (registrazione) sono contrassegnati da un apposito flag di colore rosso.

Sono disponibili tre diverse modalità di visualizzazione di alsamixer: *Playback (Riproduzione)*, *Capture (Cattura)* e *All (Tutti)*. Per default, alsamixer viene avviato in modalità *Playback (Riproduzione)* in cui vengono visualizzati solo i controlli rilevanti ai fini della riproduzione, ovvero Master Volume (Volume master), PCM (PMC), CD (CD) e così via. In *Capture (Cattura)* vengono visualizzati solo i controlli relativi alla

registrazione. In *All (Tutti)* vengono visualizzati tutti i controlli disponibili. È possibile passare da una modalità di visualizzazione all'altra premendo rispettivamente F3, F4 e F5.

Selezionare i canali con → e ← oppure N e P. Premere ↑ e ↓ oppure + e - per aumentare o ridurre il volume. È possibile controllare i canali stereo in modo indipendente premendo Q, W ed E per aumentare il volume e Z, X e C per ridurlo. È possibile modificare rapidamente il volume assoluto mediate i tasti numerici compresi tra 0 e 9, che corrispondono a valori compresi tra lo zero e il novanta percento del volume massimo.

7.1.4 Aspetto delle applicazioni mixer

L'aspetto delle applicazioni mixer dipende dal tipo di scheda audio utilizzata. Alcuni driver, ad esempio quelli SB Live!, sono dotati di numerosi elementi del mixer regolabili, mentre in quelli delle schede audio professionali ai controlli possono corrispondere nomi completamente diversi.

Chip audio integrato su scheda

La maggior parte dei chip audio integrati su scheda PCI si basa sul codec AC97. *Master (Master)* consente di controllare il volume principale degli altoparlanti anteriori. *Surround (Surround)*, *Center (Centrale)* e *LFE (LFE)* consentono di controllare rispettivamente gli altoparlanti posteriori, quello centrale e il subwoofer. Ognuno di questi elementi può essere disattivato e riattivato in modo indipendente. In alcune schede sono inoltre disponibili controlli indipendenti per il volume delle cuffie e dell'audio mono. Quest'ultimo viene utilizzato per gli altoparlanti integrati di alcuni computer portatili.

PCM (PCM) consente di controllare il livello del volume interno della riproduzione WAVE digitale. PCM è l'acronimo di Pulse Code Modulation, ovvero uno dei formati dei segnali digitali. Anche questo controllo può essere attivato e disattivato in modo indipendente.

Altri volumi, ad esempio quelli di *CD (CD)*, *Line (Linea)*, *Mic (Mic)* e *Aux (Aux)* consentono di controllare il volume di loopback dai rispettivi ingressi all'uscita principale. Questi controlli non hanno effetto sul livello di registrazione, ma solo su quello di riproduzione.

Ai fini della registrazione, attivare lo switch *Capture (Cattura)*. Si tratta dello switch di registrazione principale. Il volume di *Capture (Cattura)* fa riferimento all'ingresso scelto per la registrazione. Per default, questo switch è impostato su zero. È possibile scegliere un'origine di registrazione, ad esempio *Line (Linea)* o *Mic (Mic)*. L'origine di registrazione è esclusiva e non è quindi possibile selezionarne più di una alla volta. *Mix (Mix)* è un'origine di registrazione speciale che consente di registrare il segnale attualmente in riproduzione da tale origine.

La disponibilità di effetti speciali, ad esempio 3D o bassi e alti, dipende dal chip del codec AC97.

Famiglia Audigy e SoundBlaster Live!

SoundBlaster Live! e SB Audigy1 sono dotate di numerosi controlli mixer per i rispettivi chip del codec AC97 e il motore DSP. Oltre ai controllo già descritti, queste schede offrono i volumi *Wave (Wave)*, *Music (Musica)* e *AC97 (AC97)* che consentono di controllore l'instradamento interno del segnale e l'attenuazione del mix AC97, di PCM e della wavetable MIDI. Mantenere il volume al 100% per ascoltarli tutti. SB Audigy2 offre, a seconda del modello, meno controlli rispetto alla SB Live!, ma è comunque dotata dei controlli *Wave (Wave)* e *Music (Musica)*.

La registrazione su SB Live! è analoga a quella dei chip integrati su scheda. È possibile scegliere *Wave (Wave)* e *Music (Musica)* come origini di registrazione aggiuntive per registrare i segnali PCM e wavetable in riproduzione.

Dispositivi audio USB

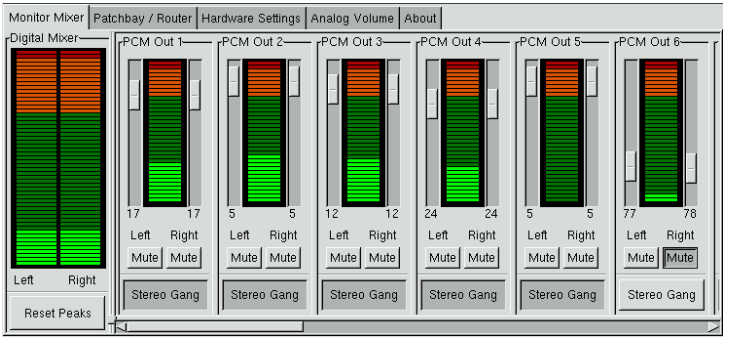
I dispositivi audio USB sono in genere dotati di un numero limitato di controlli mixer. Talvolta addirittura di nessuno. La maggior parte dei dispositivi dispone di uno switch di controllo *Master (Master)* o *PCM (PCM)* che consente di regolare il volume di riproduzione.

7.1.5 Mixer per il chip audio Envy24

envy24control è un'applicazione mixer per schede audio che utilizzano il chip Envy24 (ice1712). La flessibilità del chip Envy24 può determinare una variazione delle funzionalità in schede audio differenti. Le informazioni più aggiornate su questo chip

audio sono disponibili in `/usr/share/doc/packages/alsa/alsa-tools/envy24control`.

Figura 7.3 *Monitor e mixer digitale di envy24control*



Nel *Monitor Mixer (Monitor mixer)* di envy24control vengono visualizzati i livelli dei segnali di cui è possibile eseguire il mix digitale nella scheda audio. I segnali indicati come *PCM Out (PCM Out)* vengono generati da applicazioni che inviano dati PCM alla scheda audio. I segnali degli input analogici vengono visualizzati in *H/W In (H/W In)*. Gli input *S/PDIF* vengono riportati a destra. Impostare i livelli di input e output dei canali analogici in *Analog Volume (Volume analogico)*.

Utilizzare i dispositivi di scorrimento *Mixer monitor* per il mix digitale. I rispettivi livelli vengono visualizzati in *Mixer digitale*. Per ogni canale di output, l'opzione *Patchbay* contiene una fila di pulsanti di scelta per la selezione dell'origine del canale desiderata.

Modificare l'amplificazione per i convertitori analogico-digitale e digitale-analogico sotto *Volume analogico*. Utilizzare i dispositivi di scorrimento *DAC (DAC)* per i canali di output e quelli *ADC (ADC)* per i canali di input.

Le impostazioni dei canali S/PDIF vengono definite in *Impostazioni hardware*. Le modifiche del volume determinano un ritardo da parte del chip Envy24 che può essere configurato con *Modifica volume*.

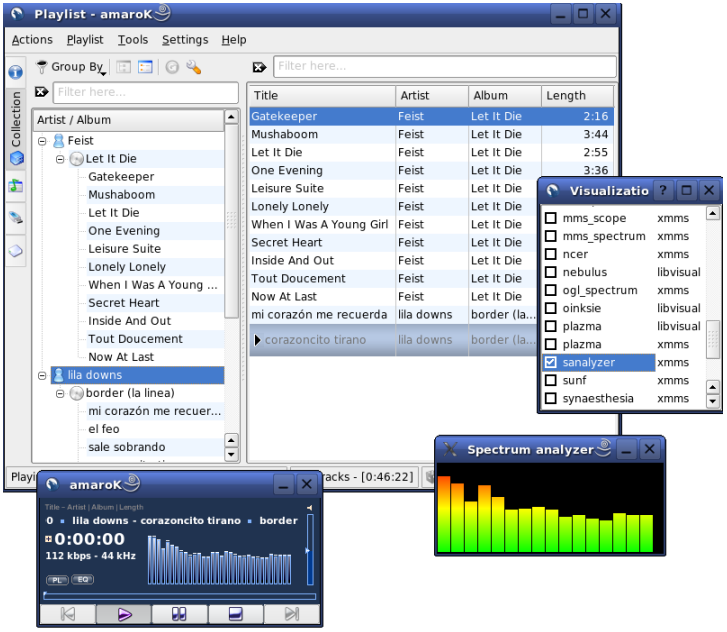
7.2 Lettori multimediali

7.2.1 amaroK

Il lettore multimediale amaroK consente di gestire diversi formati audio e di riprodurre le trasmissioni audio in streaming di stazioni radio su Internet. Il programma è compatibile con tutti i tipi di file supportati dal server audio che svolge il ruolo di back-end, attualmente aRts o GStreamer.

Al primo avvio, viene visualizzata una procedura guidata che consente di configurare amaroK. Nel primo passaggio, scegliere l'aspetto desiderato di amaroK. È possibile decidere di visualizzare il lettore e la playlist in finestre separate (vedere la Figura 7.4, «Lettore multimediale amaroK» (p. 126)) oppure di combinare le funzionalità in un'unica finestra. Nel secondo passaggio, impostare le posizioni in cui amaroK deve eseguire le ricerche di raccolte musicali. Viene eseguita la scansione delle cartelle specificate per individuare i contenuti multimediali riproducibili. Per default, amaroK è configurato per eseguire la ricerca nelle cartelle selezionate in modo ricorsivo per includere tutte le sottodirectory, tenere traccia delle modifiche apportate al contenuto delle directory specificate e importare qualsiasi playlist disponibile. È possibile modificare successivamente le impostazioni avviando di nuovo la procedura guidata mediante *Tools (Strumenti)* → *First-Run Wizard (Avvio guidato)*.

Figura 7.4 *Lettore multimediale amaroK*



Gestione delle playlist

All'avvio, amaroK esegue una ricerca di file multimediali nel file system in base alla impostazioni configurate nella procedura guidata. Nella parte destra della finestra delle playlist vengono visualizzate tutte le playlist individuate. Riprodurre brani i cui titoli sono elencati in essa nell'ordine scelto. Se non viene trovata alcuna playlist, è possibile crearne una. Il metodo migliore per effettuare questa operazione è l'uso della barra laterale a sinistra della finestra. All'estrema sinistra, sono disponibili numerose schede che possono essere utilizzate per aprire viste differenti. Da ciascuna di queste viste, trascinare intere directory o singoli titoli e rilasciarli nella playlist per includerli nell'elenco. Di seguito viene fornita una descrizione della funzione di ciascuna scheda.

Contesto

Questa scheda consente di visualizzare le informazioni sulla raccolta e i dati relativi all'artista attuale. Ad esempio, nella vista vengono visualizzate informazioni sui titoli preferiti, i titoli più recenti aggiunti alla raccolta e ulteriori dettagli. Nella vista *Home (Home)* vengono visualizzate statistiche relative alle proprie abitudini di

ascolto, fra cui elenchi di brani preferiti, nuovi e ascoltati di recente. In *Current Track (Traccia attuale)* vengono visualizzati dati relativi alla traccia in riproduzione, ad esempio la copertina dell'album (vedere la sezione chiamata «Manager di copertine » (p. 128)), le statistiche di ascolto relative al brano e così via. Se si è interessati ai testi dei brani, è possibile visualizzarli nella scheda *Lyrics (Testi)*.

Collection Browser (Browser di raccolte)

Utilizzare questa vista per gestire e visualizzare la raccolta personale di titoli. La vista della raccolta può includere file di diverse ubicazioni. L'icona a forma di chiave inglese sulla barra degli strumenti consente di specificare le posizioni in cui devono essere cercati i file musicali. Una volta selezionate le directory, la ricerca viene avviata automaticamente. Il risultato viene visualizzato come struttura ad albero. Utilizzando *Primary (Primario)* e *Secondary (Secondario)*, organizzare le due diramazioni superiori dell'albero in base ai criteri *Album (Album)*, *Artist (Artista)*, *Genre (Genere)* e *Year (Anno)*. Una volta che la vista dell'albero è pronta, trovare i titoli semplicemente digitandoli nel campo di input. Nella vista dell'albero viene selezionata automaticamente la prima voce corrispondente durante la digitazione. Per aggiornare i dati della raccolta, avviare una nuova scansione del file system mediante *Tools (Strumenti)* → *Rescan Collection (Ripeti scansione raccolta)*.

Playlist Browser (Browser di playlist)

Il browser di playlist è suddiviso in due parti. Nella parte superiore vengono elencate tutte le playlist personalizzate create trascinando i brani nell'apposita finestra e facendo clic su *Save Playlist As (Salva playlist con nome)*. Per visualizzare i contenuti delle playlist, fare clic sul segno + accanto al nome corrispondente. È possibile modificare le playlist tramite operazioni di trascinamento e rilascio. Fare doppio clic su una playlist per caricarla.

IMPORTANTE: Condivisione delle playlist con altri lettori

Se si salvano le playlist in formato `m3u` o `pls`, è possibile condividerle con tutti gli altri lettori che utilizzano questi formati.

---

amaroK offre un'utile funzione di compilazione al volo delle playlist, ovvero«Smart Playlists (Playlist intelligenti)». Utilizzare la parte inferiore del browser di playlist per selezionare una delle playlist intelligenti o fare clic su *Create Smart Playlist (Crea playlist intelligente)* per definirne una personalizzata. Immettere un nome, i criteri di ricerca, l'ordinamento ed eventualmente il limite delle tracce.

Browser di file

Questa scheda consente di aprire un browser di file. Si tratta della finestra di selezione dei file di KDE standard in cui sono disponibili i consueti controlli per l'esplorazione del file system. Immettere l'URL o la directory nel campo di input del testo. Trascinare gli elementi dei contenuti visualizzati nella playlist per includerli. È inoltre possibile eseguire ricerche ricorsive di un file in una directory specificata. Per effettuare questa operazione, immettere una stringa di testo per il titolo e l'ubicazione in cui avviare la ricerca. Successivamente, selezionare *Ricerca* e attendere che i risultati vengano visualizzati nella sezione inferiore della finestra.

Manager di copertine

amaroK include un manager di copertine che consente di associare la musica e le immagini degli album in riproduzione. Avviare il manager di copertine mediante *Tools (Strumenti) → Cover Manager (Manager di copertine)*. Nella parte sinistra della finestra viene visualizzato un albero che include tutti gli album della raccolta. Le copertine recuperate da Amazon vengono visualizzate nella parte destra della finestra. Fare clic su *View (Visualizza)* per scegliere la copertina da visualizzare fra quelle incluse nell'apposita vista. *All albums (Tutti gli album)* consente di visualizzare un elenco di tutti gli album della raccolta indipendentemente dal fatto che sia loro associata un'immagine di copertina. *Albums with cover (Album con copertina)* consente di elencare solo gli album a cui è associata una copertina, mentre *Albums without cover (Album senza copertina)* consente di visualizzare quelli che ne sono sprovvisti. Per recuperare i dati di copertina, scegliere *Amazon Locale (Impostazioni internazionali Amazon)* e quindi fare clic su *Fetch Missing Covers (Recupera copertine mancanti)*. amaroK tenterà di recuperare le copertine degli album inclusi nella raccolta.

Effetti

Selezionare il pulsante *FX (FX)* nella finestra del lettore oppure utilizzare il menu dell'applicazione amaroK per aprire una finestra di dialogo in cui abilitare e configurare diversi effetti sonori, quali un equalizzatore, la regolazione dello stereo e l'effetto Hall. Selezionare gli effetti desiderati e regolare per ciascuno le impostazioni, se disponibili.

Visualizzazioni

In amaroK sono disponibili numerose visualizzazioni che forniscono un effetto grafico per la musica riprodotta. Le visualizzazioni amaroK native vengono visualizzate nella

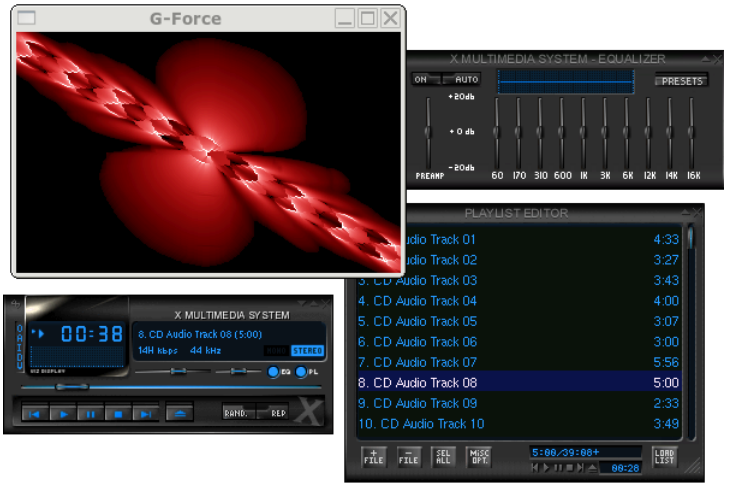
finestra del lettore. Scorrere le diverse modalità di visualizzazione disponibili facendo clic sull'animazione.

amaroK supporta inoltre i plug-in di visualizzazione del lettore multimediale XMMS. Per utilizzarli, installare il pacchetto `xmms-plugins`, quindi selezionare *Visualizations (Visualizzazioni)* dal menu amaroK. Viene aperta una finestra in cui vengono elencati i plugin disponibili. I plug-in di XMMS vengono sempre visualizzati in una finestra separata. In alcuni casi, è possibile visualizzali in modalità a tutto schermo. Per alcuni plugin, si potrebbe non ottenere un effetto visivo uniforme a meno che non si utilizzi un scheda grafica con accelerazione 3D.

7.2.2 XMMS

XMMS è un altro lettore multimediale dotato di numerose funzioni con un supporto audio efficace che consente di evitare disturbi fastidiosi o interruzioni durante la riproduzione. L'applicazione è facile da utilizzare. Il pulsante per la visualizzazione del menu si trova nell'angolo superiore sinistro della finestra del programma. Per gli utenti che preferiscono un aspetto simile a GNOME, è disponibile la versione GTK2 di XMMS, ovvero Beep Media Player. È sufficiente installare il pacchetto `bmp`. Non tutti i plug-in di XMMS, tuttavia, sono supportati da questa versione.

Figura 7.5 *Plug-in XMMS con equalizzatore, analizzatore di spettro OpenGL e Infinity*



Selezionare il modulo del plug-in di output mediante *Options (Opzioni) → Preferences (Preferenze) → Audio I/O Plugins (Plug-in I/O audio)*. Se è installato il pacchetto `xmms-kde`, è possibile configurare qui il server audio aRts.

IMPORTANTE: Utilizzo del plug-in Disk Writer

XMMS reindirizza automaticamente l'output a *Disk Writer Plugin (Plug-in masterizzazione disco)* se non è possibile individuare una scheda audio configurata. In questo caso, i file in riproduzione vengono scritti sul disco rigido come file WAV. La visualizzazione del tempo viene quindi eseguita più rapidamente rispetto a quando viene riprodotto l'output mediante una scheda audio.

È possibile avviare i vari plug-in di visualizzazione mediante *Options (Opzioni) → Preferences (Preferenze) → Visualization Plugins (Plug-in di visualizzazione)*. Se si dispone di una scheda grafica con accelerazione 3D, selezionare un'applicazione quale l'analizzatore a spettro OpenGL. Se è installato il pacchetto `xmms-plugins`, provare a utilizzare il plug-in Infinity.

A sinistra sotto il pulsante di menu, sono disponibili cinque pulsanti con differenti lettere. Questi pulsanti consentono di accedere rapidamente a configurazioni, finestre di dialogo e menu aggiuntivi. Aprire la playlist mediante *PL (PL)* e l'equalizzatore mediante *EQ (EQ)*.

7.3 CD - Riproduzione e copia

Sono disponibili varie modalità di ascolto dei brani musicali desiderati. È possibile riprodurre un CD oppure una versione digitalizzata di quest'ultimo. Nella sezione seguente vengono descritte alcune applicazioni per la riproduzione dei CD, nonché quelle che è possibile utilizzare per copiarne e codificarne i contenuti.

IMPORTANTE: CDDA e riproduzione analogica di CD

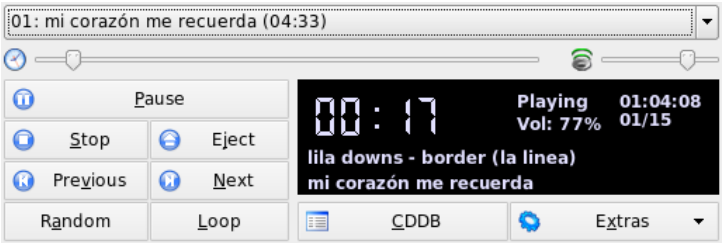
È possibile riprodurre i CD audio in due modi. Le unità CD e DVD che consentono la riproduzione analogica dei CD leggono i dati audio e li inviano all'apposito dispositivo di output. Alcune unità esterne collegate tramite PCMCIA, FireWire o USB devono utilizzare CDDA (Compact Disk Digital Audio) per estrarre i dati audio prima di riprodurli in formato PCM digitale. I lettori

inclusi nelle sezioni seguenti non supportano la modalità CDDA. Utilizzare XMMS se è necessario il supporto CDDA.

7.3.1 KsCD - Lettore di CD audio

KsCD è un lettore di CD audio facile da utilizzare. È integrato nella barra delle applicazioni di KDE ed è possibile configurarlo per l'avvio automatico della riproduzione all'inserimento di un CD. Per accedere al menu di configurazione, selezionare *Extras (Extra)* → *Configure KsCD (Configura KsCD)*. Se KsCD è opportunamente configurato, è possibile recuperare informazioni relative al brano e all'album da un server CDDB (Compact Disc DataBase) su Internet. È inoltre possibile caricare informazioni CDDB da condividere con altri utenti. Utilizzare la finestra di dialogo *CDDB (CDDB)* per informazioni sul recupero e il caricamento.

Figura 7.6 *Interfaccia utente di KsCD*



7.3.2 Applet del lettore CD di GNOME

Si tratta di una semplice applet integrata nel pannello di GNOME. Utilizzare l'icona degli strumenti per configurarne il funzionamento e selezionare un tema. È possibile controllare la riproduzione mediante i pulsanti nella parte inferiore della finestra del lettore o tramite il menu di scelta rapida che viene visualizzato facendo clic sull'icona del pannello o nella finestra del lettore.

7.3.3 Compressione di dati audio

Sono disponibili vari strumenti che consentono di gestire la compressione dell'audio. Nelle sezioni seguenti vengono descritte le procedure per codificare e riprodurre dati

audio mediante la riga di comando, nonché alcune applicazioni grafiche in grado di eseguire la compressione dell'audio.

Strumenti della riga di comando per la codifica e la riproduzione di dati audio

Ogg Vorbis (pacchetto `vorbis-tools`) è un formato di compressione audio gratuito supportato ormai dalla maggior parte dei lettori audio, nonché dai lettori MP3 portatili. È possibile visitare la pagina Web del progetto all'indirizzo `http://www.xiph.org/ogg/` (in lingua inglese).

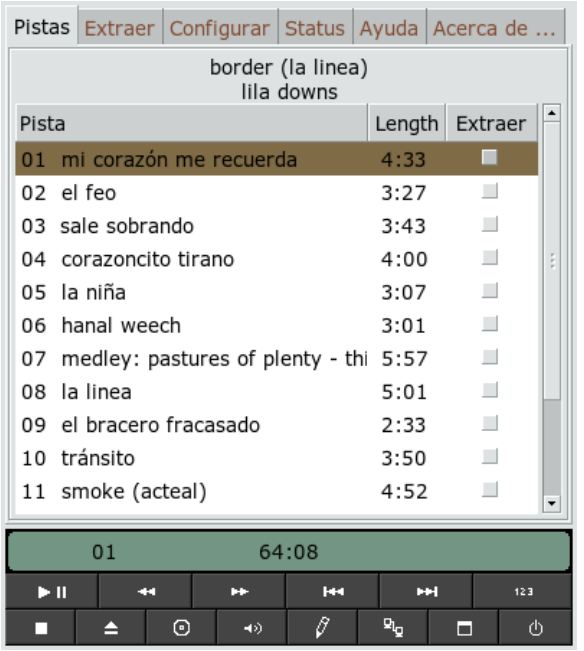
SUSE Linux include diversi strumenti che supportano Ogg Vorbis. `oggenc` è uno strumento della riga di comando utilizzato per codificare i file WAV in Ogg. È sufficiente eseguire `oggenc` *`myfile.wav`* per trasformare un file `.wav` in file Ogg Vorbis. L'opzione `-h` consente di visualizzare una panoramica degli altri parametri. Oggenc supporta la codifica con bit rate variabile. In questo modo è possibile ottenere un livello più elevato di compressione. Invece del bit rate, è possibile specificare la qualità desiderata mediante il parametro `-q`. `-b` consente di determinare il bit rate medio, mentre `-m` e `-M` di specificare rispettivamente il bit rate minimo e quello massimo.

ogg123 è un lettore Ogg della riga di comando. Avviarlo mediante un comando del tipo `ogg123` *`mysong.ogg`* .

Compressione di dati audio mediante Grip

Grip è il lettore di CD con funzioni di copia di GNOME (vedere la Figura 7.7, «Copia di CD audio con Grip» (p. 133)). La funzionalità di riproduzione dei CD viene interamente controllata tramite i pulsanti nella parte inferiore della finestra. È possibile controllare le funzionalità di copia e codifica mediante le schede nella parte superiore della finestra. Per visualizzare e modificare le informazioni relative a tracce e album o per selezionare le tracce da copiare, aprire la scheda *Tracks (Tracce)*. Selezionare la casella di controllo accanto al titolo della traccia per selezionarla. Per modificare le relative informazioni, fare clic su *Toggle disc editor (Attiva/Disattiva editor di dischi)* e apportare le modifiche. Nella scheda *Rip (Copia)* è possibile selezionare la modalità di copia desiderata e controllarne l'esecuzione. È possibile accedere a tutte le impostazioni di configurazione di Grip nella scheda *Config (Configura)*. Utilizzare *Status (Stato)* per controllare lo stato dell'applicazione.

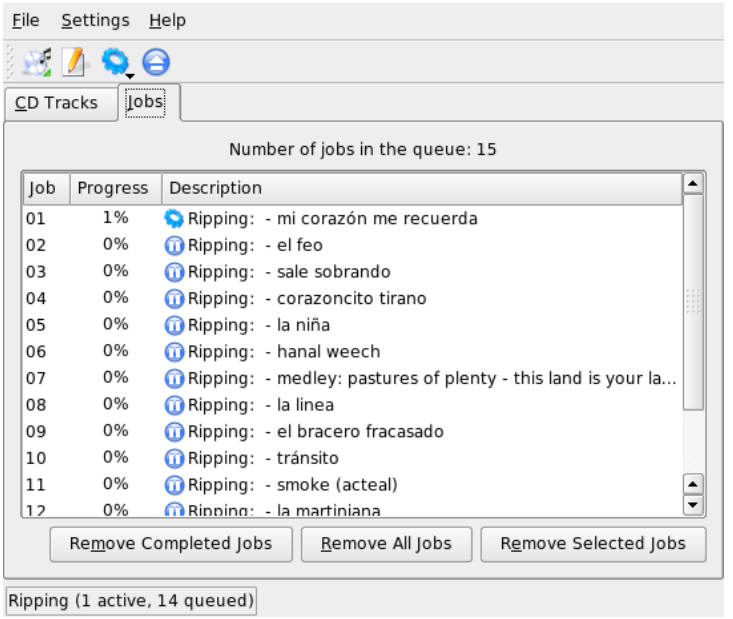
Figura 7.7 *Copia di CD audio con Grip*



Compressione di dati audio mediante KAudioCreator

KAudioCreator è una semplice applicazione per la copia di CD (vedere la Figura 7.8, «Copia di CD audio con KAudioCreator» (p. 134)). Una volta avviato, viene visualizzato l'elenco di tutte le tracce del CD nella scheda *CD Tracks (Tracce del CD)*. Selezionare le tracce da copiare e codificare. Per modificare le informazioni relative alla traccia, utilizzare *Album Editor (Editor di album)* in *File (File)* → *Edit Album (Modifica album)*. In alternativa, avviare il processo di copia e codifica tramite *File (File)* → *Rip Selection (Copia selezione)*. È possibile osservare l'avanzamento delle operazioni nella scheda *Jobs (Lavori)*. Se opportunamente configurato, KAudioCreator consente inoltre di generare file di playlist a partire dalla selezione. È possibile utilizzare tali playlist con altri lettori, ad esempio amaroK e XMMS.

Figura 7.8 *Copia di CD audio con KAudioCreator*



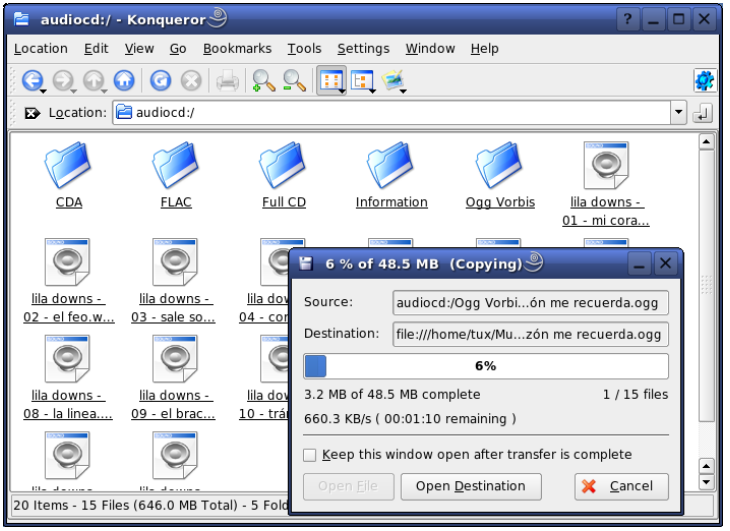
Compressione di CD audio mediante Konqueror

Prima di avviare il processo di copia vero e proprio di Konqueror, configurare la gestione dei CD audio e il codificatore Ogg Vorbis nel centro controllo di KDE. Selezionare *Sound & Multimedia (Audio e multimedia)* → *Audio CDs (CD audio)*. Il modulo di configurazione è suddiviso in tre schede: *General (Generale)*, *Names (Nomi)* e *Ogg Vorbis Encoder (Codificatore Ogg Vorbis)*. L'unità CD appropriata viene in genere rilevata automaticamente. Non modificare questa impostazione di default a meno che il rilevamento automatico abbia esito negativo e risulti necessario impostare l'unità CD manualmente. È inoltre possibile impostare qui la correzione degli errori e la priorità dei codificatori. Nella scheda *Ogg Vorbis Encoder (Codificatore Ogg Vorbis)* determinare la qualità della codifica. Per configurare la ricerca in linea di informazioni relative ad album, brani e artisti per i dati audio copiati, selezionare *Add Track Information (Aggiungi informazioni tracce)*.

Inserire il CD nell'apposita unità e immettere `audiocd:/` nella barra *Location (Posizione)* per avviare il processo di copia. In Konqueror viene quindi visualizzato

l'elenco delle tracce del CD e di alcune cartelle (vedere la Figura 7.9, «Copia di dati audio con Konqueror» (p. 135)).

Figura 7.9 *Copia di dati audio con Konqueror*

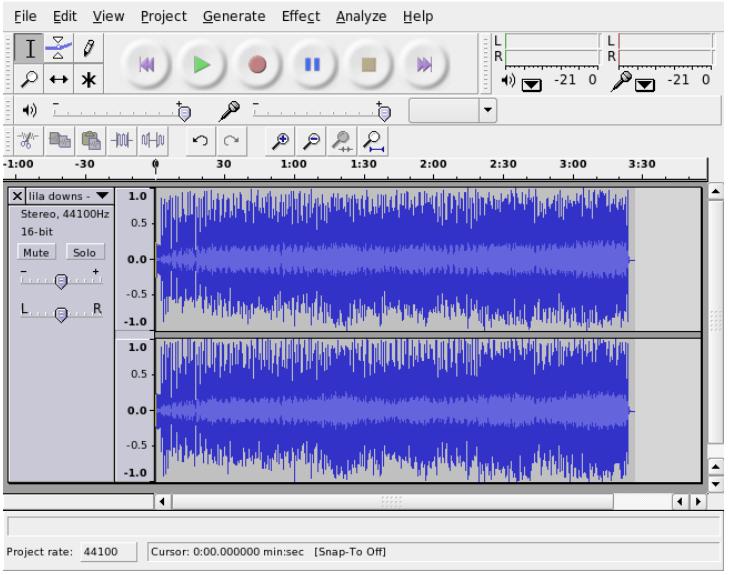


Per non comprimere i dati audio nel disco, è sufficiente selezionare i file `.wav` e trascinarli in un'altra finestra di Konqueror per copiarli nella rispettiva destinazione. Per avviare la codifica Ogg Vorbis, trascinare la cartella `Ogg Vorbis` in un'altra finestra di Konqueror. La codifica viene avviata non appena la cartella Ogg Vorbis viene rilasciata nella relativa destinazione.

7.4 Registrazione su disco rigido con Audacity

Audacity (pacchetto `audacity`) consente di registrare e modificare i file audio. Si tratta della registrazione su disco rigido. Al primo avvio del programma, selezionare una lingua. È possibile modificare successivamente l'impostazione della lingua in *File (File) → Preferences (Preferenze) → Interface (Interfaccia)*. La modifica della lingua viene applicata al successivo avvio del programma.

Figura 7.10 *Vista dello spettro dei dati audio*



7.4.1 Registrazione di file WAV e importazione di file

Fare clic sul pulsante rosso di registrazione per creare una traccia stereo vuota e avviare la registrazione. Per modificare i parametri standard, configurare le impostazioni desiderate in *File (File)* → *Preferences (Preferenze)*. *Audio I/O (I/O audio)* e *Quality (Qualità)* sono importanti ai fini della registrazione. È possibile fare clic sul pulsante di registrazione per creare nuove tracce anche ne sono già presenti altre. Ciò può generare confusione all'inizio poiché non è possibile visualizzare tali tracce nella finestra del programma nelle dimensioni standard.

Per importare file audio, selezionare *Project (Progetto)* → *Import Audio (Importa audio)*. Il programma supporta il formato WAV e il formato compresso Ogg Vorbis. Per ulteriori informazioni su questo formato, vedere la Sezione 7.3.3, «Compressione di dati audio» (p. 131).

7.4.2 Modifica di file audio

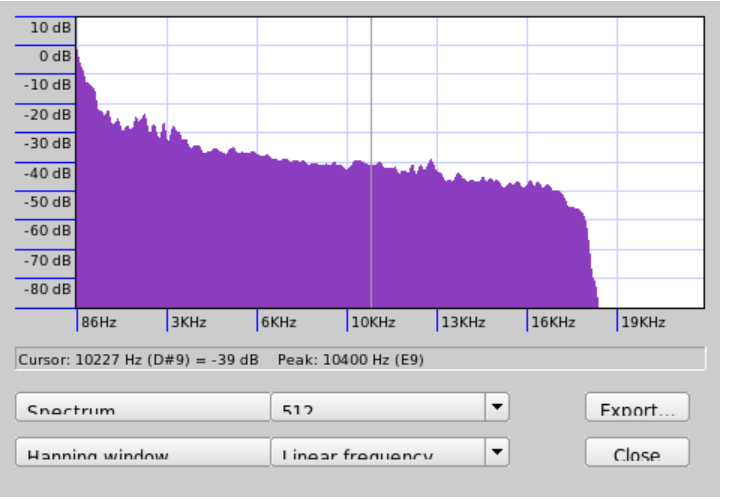
Aprire il menu *AudioTrack (Traccia audio)* a sinistra della traccia. In questo menu sono disponibili varie opzioni per le diverse viste e le operazioni di modifica di base. Per rinominare la traccia, selezionare *Name (Nome)* e immettere un nuovo nome. Le diverse modalità di visualizzazione offerte da Audacity includono *Waveform (Forma d'onda)*, *Waveform (dB) (Forma d'onda)*, *Spectrum (Spettro)* e *Pitch (Tonalità)*. Scegliere quella più adatta alle proprie esigenze. Se si desidera modificare i singoli canali di una traccia stereo in modo indipendente, selezionare *Split Track (Suddividi traccia)*. È possibile trattare ogni canale come traccia indipendente. Impostare i parametri *Sample Format (Formato di campionamento)* (in bit) e *Sample Rate (Frequenza di campionamento)* (in Hz) per ogni traccia.

Per poter utilizzare la maggior parte degli strumenti disponibili nel menu *Edit (Modifica)*, è necessario innanzitutto selezionare il canale e il segmento della traccia da modificare. Dopo aver eseguito la selezione, è possibile applicarvi qualsiasi modifica ed effetto.

A seconda del tipo di file scelto, nel menu *View (Visualizza)* → *Set Selection Format (Imposta formato selezione)* vengono resi disponibili diversi formati di visualizzazione per i segmenti selezionati. *Set Snap-To Mode (Imposta modalità Aggancia a)* consente di adattare gli estremi del segmento al formato di visualizzazione selezionato. Ad esempio, se si seleziona *PAL frames (Frame PAL)* come formato di visualizzazione e si attiva *Snap-To (Aggancia a)*, gli estremi del segmento vengono sempre selezionati in multipli di frame.

Tutti gli strumenti di modifica dispongono di descrizioni comando che ne facilitano l'uso. La funzione *Undo History (Cronologia modifiche)*, a cui è possibile accedere mediante *View (Visualizza)* → *History (Cronologia)*, è una funzionalità utile per visualizzare le operazioni di modifica eseguite di recente e annullarle facendo clic sulle voci corrispondenti nell'elenco. Utilizzare *Discard (Elimina modifiche)* con attenzione poiché determina la cancellazione delle operazioni di modifica dall'elenco. Una volta eliminate, tali operazioni non possono più essere annullate.

Figura 7.11 *Spettro*



L'analizzatore di spettro integrato consente di individuare e analizzare rapidamente qualsiasi disturbo. È possibile visualizzare lo spettro del segmento selezionato mediante *View (Visualizza)* → *Plot Spectrum (Traccia spettro)*. Selezionare una scala logaritmica di frequenze in ottave mediante *Log frequency (Registra frequenza)*. Se si sposta il cursore del mouse all'interno dello spettro, le frequenze di picco vengono visualizzate automaticamente con le rispettive note.

Rimuovere le frequenze indesiderate mediante *Effect (Effetto)* → *FFT Filter (Filtro FFT)*. In seguito al processo di applicazione del filtro, potrebbe essere necessario regolare nuovamente l'ampiezza del segnale mediante *Amplify (Amplifica)*. È inoltre possibile utilizzare *Amplify (Amplifica)* per verificare l'ampiezza. Per default, *New Peak Amplitude (Nuova ampiezza picco)* è impostato su 0.0 dB. Questo valore rappresenta l'ampiezza massima possibile nel formato audio selezionato. *Amplification (Amplificazione)* consente di visualizzare i valori necessari per amplificare il segmento selezionato fino all'ampiezza di picco desiderata. Un valore negativo indica la sovra-amplificazione.

7.4.3 Salvataggio ed esportazione

Per salvare l'intero progetto, selezionare *File (File)* → *Save Project (Salva progetto)* o *Save Project As (Salva progetto con nome)*. Questa operazione consente di generare

un file XML con estensione `.aup` nel quale è descritto il progetto. I dati audio effettivi vengono salvati in una directory denominata in base al nome del progetto con l'aggiunta del suffisso `_data`.

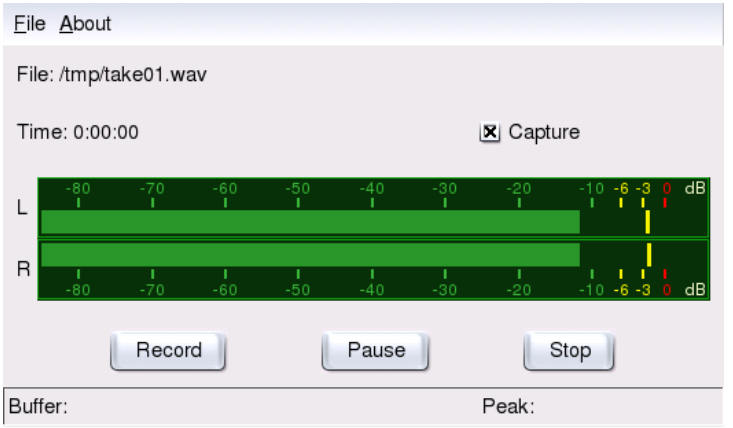
È inoltre possibile esportare l'intero progetto o il segmento selezionato come file WAV stereo. Per informazioni sull'esportazione del progetto in formato Vorbis, vedere la Sezione 7.3.3, «Compressione di dati audio» (p. 131).

7.5 Riproduzione e registrazione diretta di file WAV

`arecord` e `aplay` del pacchetto `alsa` offrono un'interfaccia semplice e flessibile per i dispositivi PCM. È possibile utilizzare `arecord` e `aplay` per registrare e riprodurre dati audio in formato WAV e altri formati. Il comando `arecord -d 10 -f cd -t wav mysong.wav` consente di registrare un file WAV di 10 secondi con qualità CD (16 bit, 44,1 kHz). È possibile visualizzare un elenco di tutte le opzioni di `arecord` e `aplay` eseguendoli con il parametro `--help`.

qaRecord (pacchetto `kalsatools`) è un semplice programma di registrazione dotato di interfaccia grafica e visualizzazione dei livelli. Poiché il programma utilizza un buffer interno di circa 1 MB (configurabile mediante `--buffersize`), consente di registrare ininterrottamente anche in presenza di hardware lento, in particolare se viene eseguito con priorità real-time (tempo reale). Durante la registrazione, le dimensioni del buffer in uso vengono visualizzate nella riga di stato in *Buffer (Buffer)* mentre le dimensioni massime del buffer finora necessarie per la registrazione vengono indicate in *Peak (Picco)*.

Figura 7.12 *QARecord - Semplice applicazione per la registrazione su disco rigido*



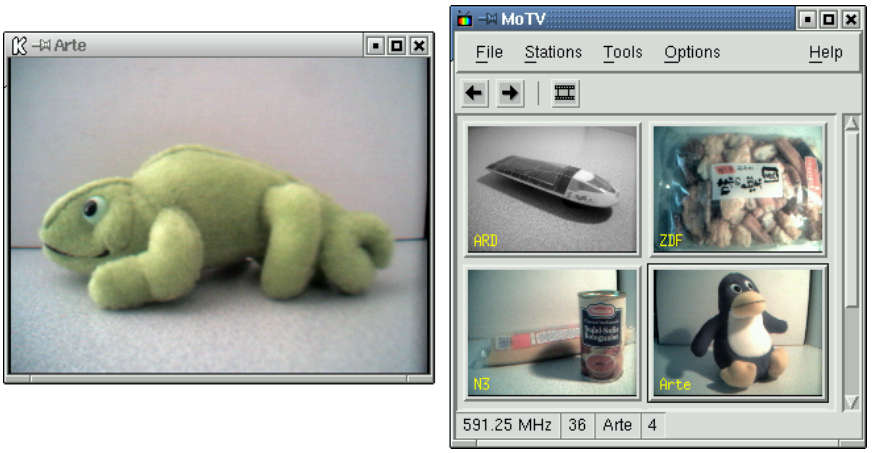
8 TV, video, radio e webcam

In questo capitolo vengono presentate alcune semplici applicazioni Linux per video, radio e webcam. Verranno illustrate le procedure per configurare e utilizzare motv per guardare programmi televisivi analogici, utilizzare una webcam e consultare il teletext. È possibile utilizzare xawtv4 per la diffusione di video digitali, ed eseguire gqcam per controllare le webcam. È possibile accedere ai dati EPG tramite nxtvepg o xawtv4.

8.1 TV con motv

motv è una versione migliorata di xawtv. Incorpora tutte le funzioni essenziali nell'interfaccia utente. Per avviare l'applicazione, scegliere *Multimedia (Multimedia)* → *Video (Video)* → *motv (motv)*. Avviarlo dalla riga di comando con `motv`. All'inizio viene visualizzata solo una finestra relativa alla TV dopo l'avvio dell'applicazione. Per aprire una finestra di menu, fare clic con il pulsante destro del mouse.

Figura 8.1 *Applicazione TV motv*



8.1.1 Origine video e ricerca di rete

Scegliere l'origine video in *Settings (Impostazioni)* → *Input (Input)*. Se si seleziona *Televisione*, configurare la rete di diffusione prima dell'avvio dell'applicazione. Questa operazione viene eseguita automaticamente con la ricerca di rete, ma è possibile trovare la rete anche nel menu *Impostazioni*. Se si fa clic su *Save settings (Salva impostazioni)*, la rete trovata viene immessa nel file `.xawtv` nella home directory e sarà disponibile al successivo avvio dell'applicazione.

SUGGERIMENTO: Selezione dei canali

Se non si desidera cercare tutti i canali disponibili, trovare il canale successivo con Ctrl + ↑. Se necessario, regolare quindi la frequenza di diffusione mediante ← o →.

8.1.2 Recupero di dati audio

L'output audio della scheda TV è collegata all'input della linea della scheda audio, agli altoparlanti o a un amplificatore. Alcune schede TV possono modificare il volume dell'output audio. Il volume può essere impostato mediante i dispositivi di scorrimento che vengono visualizzati dopo aver selezionato *Settings (Impostazioni)* → *Slider*

(Dispositivo di scorrimento). Anche in questa finestra sono disponibili i dispositivi di scorrimento per la luminosità, il contrasto e il colore.

Per utilizzare la scheda audio ai fini della riproduzione, controllare le impostazioni del mixer mediante gamix, descritto nella Sezione 7.1, «Mixer» (p. 119). Per le schede audio che soddisfano le specifiche AC97, impostare *Input-MUX (MUX input)* su *Line (Linea)*. Il volume può essere regolato mediante i dispositivi *Master (Master)* e *Line (Linea)*.

8.1.3 Proporzioni dello schermo e modalità a tutto schermo

Per la maggior parte delle immagini televisive il rapporto tra altezza e larghezza è 4:3. Queste proporzioni possono essere impostate mediante *Tools (Strumenti)* → *Screen Dimensions (Dimensioni schermo)*. Se si seleziona *4:3* (questa è l'impostazione di default), le dimensioni dello schermo vengono conservate automaticamente, anche quando le dimensioni della visualizzazione vengono modificate.

È possibile passare alla modalità a schermo interno mediante F o *Tools (Strumenti)* → *Fullscreen (Schermo intero)*. Se l'immagine televisiva in modalità a tutto schermo non è ridotta in scala in base alla dimensione del monitor completa, è necessario eseguire un'ottimizzazione. Molte schede grafiche possono ridurre in scala l'immagine televisiva in modalità a tutto schermo in base alla dimensione del monitor completa senza modificare la modalità grafica. Se la scheda non supporta questa funzione, la modalità grafica deve essere modificata in 640x480 per la modalità a tutto schermo. Definire la relativa configurazione in *Settings (Impostazioni)* → *Configuration (Configurazione)*. Dopo il riavvio di motv, viene modificata anche la modalità del monitor se si è passati alla modalità a tutto schermo.

SUGGERIMENTO: Memorizzazione della configurazione in .xawtv

Il file `.xawtv` viene creato automaticamente e aggiornato facendo clic su *Settings (Impostazioni)* → *Save settings (Salva impostazioni)*. I broadcaster vengono salvati insieme alla configurazione. Ulteriori informazioni sul file di configurazione sono disponibili nella documentazione relativa a `xawtvrc`.

8.1.4 Menu di avvio

Utilizzare il menu di avvio per avviare altre applicazioni da utilizzare con motv. Avviare il mixer audio gamix e l'applicazione per teletext alevt, ad esempio, mediante un tasto di scelta rapida. È necessario immettere le applicazioni da avviare tramite motv nel file `.xawtv`. Le voci devono avere il seguente formato:

```
[launch] Gamix = Ctrl+G, gamix AleVT = Ctrl+A, alevt
```

La scorciatoia e successivamente il comando utilizzato per avviare l'applicazione devono seguire il nome stesso dell'applicazione. Avviare le applicazioni immesse sotto [launch] tramite il menu *Strumenti*.

8.2 Supporto teletext

Utilizzare alevt per sfogliare le pagine del teletext. Avviare l'applicazione mediante *Multimedia (Multimedia) → Video (Video) → alevt (alevt)* oppure dalla riga di comando con `alevt`.

L'applicazione consente di salvare tutte le pagine della stazione selezionata appena attivata con motv. Sfogliare le pagine immettendo il numero di pagina desiderato oppure facendo clic su un numero di pagina. Spostarsi in avanti o indietro tra le pagine facendo clic su << o >>, che si trovano nel margine inferiore della finestra.

Le versioni recenti di motv e xawtv4 includono applicazioni proprie per la visualizzazione del teletext: mtt (motv) e mtt4 (xawtv4). mtt4 supporta anche le schede DVB.

8.3 Webcam e motv

Se la webcam in uso è già supportata da Linux, accedervi mediante motv. Per un elenco dei dispositivi USB supportati, visitare il sito all'indirizzo `http://www.linux-usb.org` (in lingua inglese). Se si è già utilizzato motv per accedere alla scheda TV prima di avviare la webcam, verrà caricato il driver bttv. Il driver della webcam viene caricato automaticamente quando la webcam è collegata al dispositivo USB. Per accedere alla webcam, avviare motv dalla riga di comando

mediante il parametro `-c /dev/video1`. Accedere alla scheda TV con `motv -c /dev/video0`.

Quando si collega la webcam alla porta USB prima del caricamento automatico del driver bttv, ad esempio se si avvia un'applicazione TV, `/dev/video0` è riservato alla webcam. In questo caso, se si avvia motv mediante il parametro `-c /dev/video1` per accedere alla scheda TV, potrebbe essere visualizzato un messaggio di errore poiché il driver bttv non viene caricato automaticamente. Per risolvere il problema, caricare il driver separatamente mediante `modprobe bttv` come utente `root`. È possibile visualizzare una panoramica dei dispositivi video configurabili nel sistema con `motv -hwscan`.

8.4 nxtvepg - Guida TV per il PC

Da alcuni broadcaster, viene trasmesso un segnale EPG (Electronic Program Guide) insieme con il segnale del testo su video. È possibile visualizzare facilmente la guida elettronica mediante il programma nxtvepg. Per effettuare questa operazione, è tuttavia necessario disporre di una scheda TV supportata dal driver bttv ed essere in grado di ricevere uno dei canali diffusi con EPG.

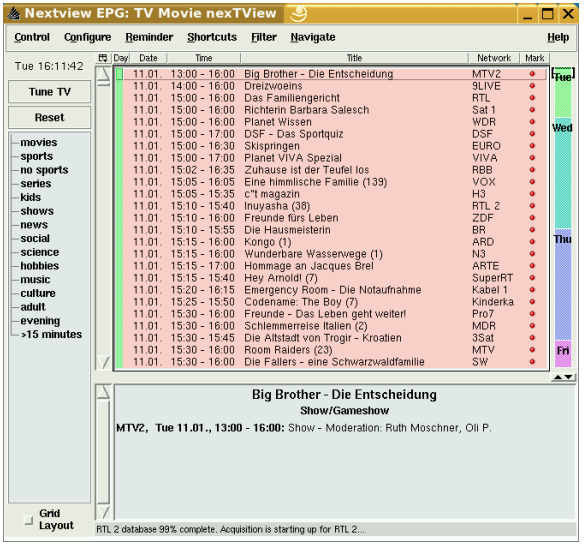
In nxtvepg, le trasmissioni vengono ordinate in base al canale e all'argomento, ad esempio *film* e *sport* e filtrate in base a criteri quali *Live (In diretta)*, *Stereo (Stereo)* o *Subtitle (Sottotitolato)*. Avviare l'applicazione mediante *Multimedia (Multimedia)* → *Video (Video)* → *nxtvepg (nxtvepg)* oppure dalla riga di comando mediante `nxtvepg`.

8.4.1 Importazione del database EPG

Per configurare e aggiornare il database dei programmi tramite il segnale EPG, impostare il sintonizzatore della scheda TV su una stazione che diffonde EPG. È possibile eseguire questa operazione mediante un'applicazione TV, ad esempio motv o nxtvepg. Il sintonizzatore può accedere a una sola applicazione alla volta.

Se si imposta un broadcaster EPG in motv, nxtvepg avvia immediatamente l'importazione dell'elenco attuale di programmi televisivi e viene visualizzato l'avanzamento dell'operazione.

Figura 8.2 *Guida TV elettronica nxtvepg*



Se non è stata avviata un'applicazione TV, è possibile utilizzare nxtvepg per ricercare broadcaster EPG. Per eseguire questa operazione, utilizzare *Configure (Configura)* → *Provider scan (Scansione provider)*. L'opzione *Usa .xatv* è attivata per default. Ciò indica che nxtvepg sta eseguendo l'accesso ai broadcaster salvati nel file.

SUGGERIMENTO: Risoluzione dei problemi

Se si verificano dei problemi, controllare che sia stata scelta l'origine video corretta sotto *Input scheda TV*.

Selezionare un provider EPG tra quelli trovati in *Configure (Configura)* → *Select Provider (Selezione provider)*. L'opzione *Configure (Configura)* → *Merge Providers (Unisci provider)* consente inoltre di creare associazioni flessibili tra database di provider diversi.

8.4.2 Ordinamento dei programmi

nxtvepg offre una comoda funzione di filtro che consente di gestire una quantità elevata di programmi televisivi. Attivare un elenco di selezione della rete mediante *Configure (Configura)* → *Show networks (Mostra reti)*. Il menu *Filtro* offre numerose funzioni

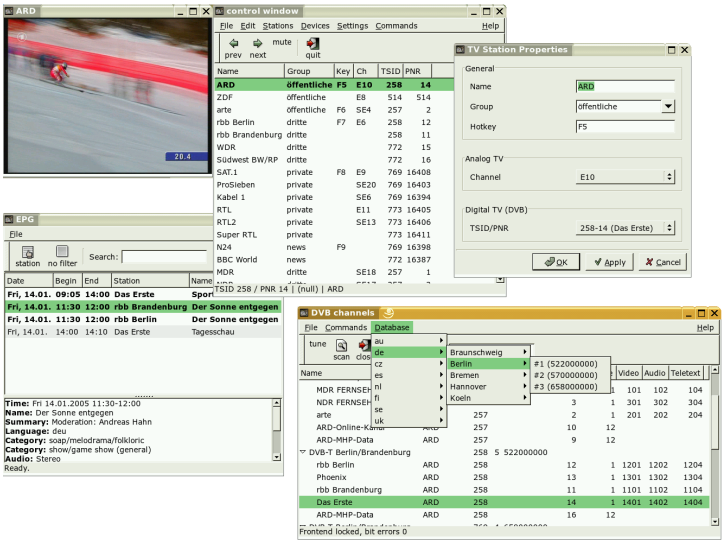
di filtro. Fare clic con il pulsante destro del mouse sull'elenco di programmi per aprire un menu di filtro particolare in cui attivare funzioni di filtro contestuali.

Particolarmente importante è il menu *Spostamento*. Si basa direttamente sui dati EPG. Viene visualizzato nella lingua della rete.

8.5 Trasmissioni video digitali con xawtv4

Dopo aver correttamente configurato l'hardware con YaST, avviare xawtv4 dal menu principale, ovvero mediante *Multimedia (Multimedia)* → *Video (Video)* → *xawtv4 (xawtv4)*. Per poter guardare le trasmissioni desiderate, è innanzitutto necessario creare un database di stazioni DVB.

Figura 8.3 *Esecuzione di xawtv4*



Fare clic con il pulsante destro del mouse sulla finestra di avvio per aprire la finestra di controllo (vedere la Figura 8.3, «Esecuzione di xawtv4» (p. 147)). Avviare una scansione delle stazioni DVB disponibili mediante *Edit (Modifica)* → *Scan DVB (Scansione DVB)*. Vengono visualizzati un rilevatore di canali e una finestra del browser. Selezionare un bouquet per preparare la scansione. È possibile eseguire questa operazione

manualmente mediante *Commands (Comandi)* → *Tune manually (Sintonizzazione manuale)* se si conoscono già i parametri di sintonizzazione del bouquet oppure recuperandoli da un database incorporato di xawtv4 tramite *Database* → *_country_* → *_channel number_* (sostituire `_country_` e `_channel_number_` con i valori effettivi della zona desiderata).

Non appena lo scanner è sintonizzato, i primi dati vengono visualizzati nella finestra del browser. Avviare una scansione completa di tutte le stazioni disponibili mediante *Commands (Comandi)* → *Full Scan (Scansione completa)*. Durante la scansione, è possibile selezionare le stazioni desiderate e aggiungerle all'apposito elenco trascinandole nella finestra di controllo. Terminare la scansione dei canali e selezionarne uno per iniziare a guardare la diffusione.

SUGGERIMENTO: Modifica dell'elenco delle stazioni

È possibile controllare la selezione dei canali tramite tasti di scelta rapida. Per impostare un tasto di scelta rapida per qualsiasi stazione inclusa nell'elenco, selezionare la stazione, fare clic su *Edit (Modifica)* → *Edit Station (Modifica stazione)*. Viene visualizzata la finestra di dialogo *TV Station Properties (Proprietà stazione TV)*. Immettere il tasto di scelta rapida e quindi fare clic su *OK* per chiudere la finestra di dialogo. Questa finestra di dialogo consente inoltre di definire i sottomenu contenenti i gruppi di stazioni, ad esempio «notizie» o «private».

Il pacchetto software xawtv4 include numerose altre applicazioni multimediali autonome:

pia4
: Un lettore di film della riga di comando che può essere utilizzato per riprodurre qualsiasi flusso video registrato da xawtv4.

mtt4
: Un browser di teletext (vedere la Figura 8.4, «Browser di teletext mtt4» (p. 149)).

Figura 8.4 *Browser di teletext mtt4*

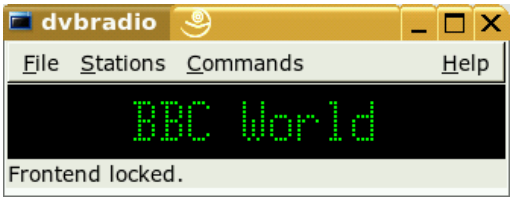
alexplore

Un'applicazione autonoma per la scansione dei canali DVB. Le funzionalità di questo prodotto sono integrate in xawtv4.

dvbradio

Un sintonizzatore radio DVB. Utilizzare questo programma per ascoltare i flussi radio DVB-S dopo aver completato la scansione iniziale delle stazioni (vedere la Figura 8.5, «Radio DVB» (p. 149)).

Figura 8.5 *Radio DVB*



dvbrowse

Un browser EPG. Utilizzare questo programma per recuperare dati EPG dopo aver completato la scansione iniziale delle stazioni.

K3b: un programma per la masterizzazione di CD o DVD

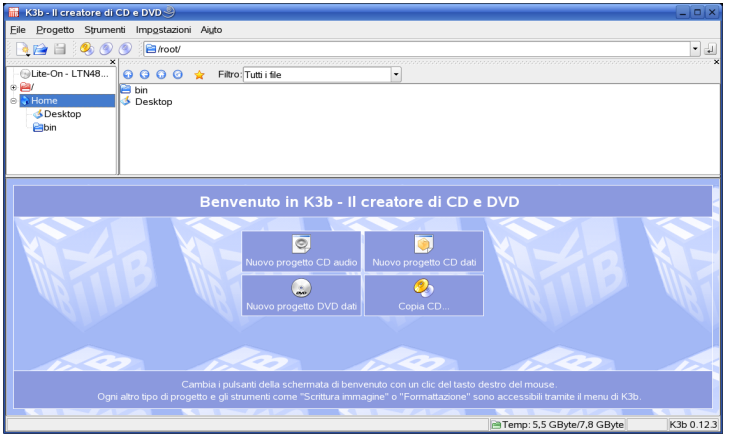
9

K3b è un programma completo per la masterizzazione di CD e DVD dati e audio. Avviare il programma dal menu principale oppure immettendo il comando `k3b`. Nelle sezioni seguenti viene brevemente descritto come avviare un processo di masterizzazione di base per creare un primo CD o DVD con Linux.

9.1 Creazione di un CD di dati

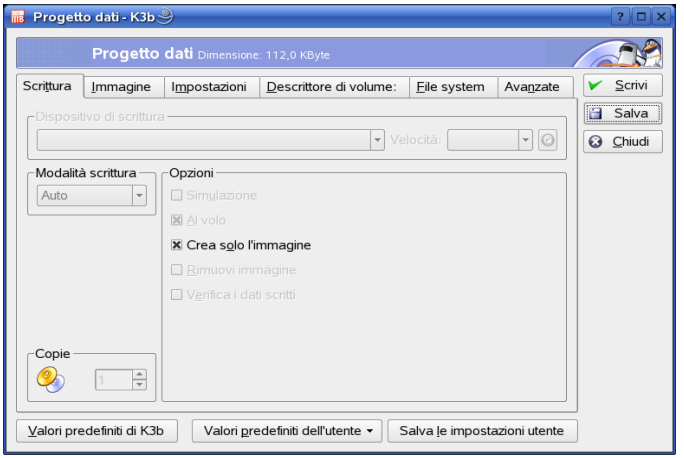
Per creare un CD dati, selezionare *File → New Project (Nuovo progetto) → New Data Project (Nuovo progetto dati)*. La vista del progetto viene visualizzata nella parte inferiore della finestra, come illustrato nella Figura 9.1, «Creazione di un nuovo CD di dati» (p. 152). Trascinare i singoli file o le directory desiderate dalla home directory alla cartella del progetto e rilasciare tali elementi. Salvare il progetto con un nome desiderato selezionando *File → Save as (Salva con nome)*.

Figura 9.1 *Creazione di un nuovo CD di dati*



Selezionare quindi *Burn (Masterizza)* sulla barra degli strumenti oppure premere Ctrl + B. Viene visualizzata una finestra di dialogo con sei schede contenenti varie opzioni per la masterizzazione di CD. Vedere la Figura 9.2, «Personalizzazione del processo di masterizzazione» (p. 152).

Figura 9.2 *Personalizzazione del processo di masterizzazione*



La scheda *Writing (Scrittura)* contiene varie impostazioni per il dispositivo, la velocità e le opzioni di masterizzazione. Sono disponibili le seguenti opzioni:

Burning Device (Dispositivo di masterizzazione)

Il dispositivo rilevato viene visualizzato in questo menu popup. In questo riquadro è inoltre possibile selezionare la velocità.

AVVERTIMENTO: prestare attenzione durante la selezione della velocità di scrittura

In genere, è consigliabile selezionare l'opzione *Auto (Automatica)* per impostare la massima velocità di scrittura possibile. Tuttavia, se si aumenta questo valore e il sistema non è in grado di inviare i dati abbastanza velocemente, le probabilità di sottocarico del buffer aumenteranno.

Writing Mode (Modalità di scrittura)

Questa opzione determina la modalità di scrittura del laser su un CD. Nella modalità DAO (disk at once), il laser non viene disattivato durante la scrittura del CD. Questa modalità è consigliata per la creazione di CD audio. Tuttavia, non è supportata da tutti i masterizzatori CD. Nella modalità TAO (track at once) viene utilizzato un processo di scrittura separato per ogni singola traccia. La modalità RAW non viene utilizzata molto spesso, poiché il masterizzatore non esegue alcuna correzione di dati. L'impostazione ottimale è *Auto (Automatica)* perché consente a K3b di utilizzare le impostazioni più adeguate.

Simula

Questa funzione può essere utilizzata per controllare se il sistema supporta la velocità di scrittura selezionata. La scrittura viene eseguita con il laser disattivato per eseguire un test del sistema.

On the Fly (Al volo)

Consente di scrivere i dati desiderati senza creare un file di immagine (non utilizzare questa funzione in computer a prestazioni ridotte). Un file di immagine, anche definito immagine ISO, è un file contenente tutti i dati del CD che viene successivamente scritto sul CD esattamente com'è.

Only Create Image (Crea solo immagine)

Questa opzione consente di creare un file di immagine. Impostare il percorso di questo file in *File temporaneo*. Il file di immagine può essere scritto su CD in un secondo momento. Per eseguire questa operazione, selezionare *Tools (Strumenti) → CD → Burn CD Image (Masterizza immagine CD)*. Se si utilizza questa opzione, tutte le altre opzioni presenti in questa sezione vengono disattivate.

Remove Image (Rimuovi immagine)
Questa opzione consente di rimuovere il file di immagine temporaneo dal disco rigido al termine del processo.

Verify Written Data (Verifica dati scritti)
Questa opzione consente di controllare l'integrità dei dati scritti confrontando le checksum MD5 dei dati originali e di quelli scritti.

La scheda *Image (Immagine)* è accessibile solo se nella scheda precedente è stata selezionata l'opzione *Only create image (Crea solo immagine)*, nel qual caso è possibile specificare il file in cui viene scritta l'immagine ISO.

La scheda *Settings (Impostazioni)* contiene due opzioni: *Datatrack Mode (Modalità traccia dati)* e *Multisession Mode (Modalità multisessione)*. L'opzione *Datatrack Mode (Modalità traccia dati)* consente di configurare la modalità di scrittura delle tracce di dati. In genere, *auto (automatica)* è la modalità più indicata. L'opzione *Multisession Mode (Modalità multisessione)* viene utilizzata per aggiungere dati a un CD già masterizzato ma non ancora finalizzato.

Nella scheda *Volume Desc (Descrizione volume)* è possibile immettere alcune informazioni generali per l'identificazione di un particolare progetto dati, ovvero il produttore, l'autore e l'applicazione e il sistema operativo utilizzati per la creazione del progetto.

In *File system*, specificare le impostazioni per il file system nel CD (RockRidge, Joliet, UDF). Inoltre, determinare il modo in cui i collegamenti simbolici, le autorizzazioni dei file e gli spazi vengono trattati. Nella scheda *Advanced (Avanzate)* gli utenti esperti possono specificare ulteriori impostazioni.

Dopo avere regolato tutte le impostazioni in base alle proprie esigenze, avviare il processo effettivo di masterizzazione scegliendo *Burn (Masterizza)*. In alternativa, salvare le impostazioni per usi e regolazioni futuri scegliendo *Save (Salva)*.

9.2 Creazione di un CD audio

Non esistono differenze significative tra la creazione di un CD audio e un CD dati. Selezionare *File → Nuovo progetto audio*. Trascinare e rilasciare le singole tracce audio nella cartella del progetto. I dati audio devono essere in formato WAV o Ogg

Vorbis. Determinare la sequenza delle tracce spostandole verso l'alto o verso il basso nella cartella del progetto.

CD Text consente di aggiungere alcune informazioni in formato testo a un CD, ad esempio il titolo, il nome dell'artista e il nome delle tracce. I lettori CD che supportano questa funzionalità sono in grado di leggere e visualizzare queste informazioni. Per aggiungere le informazioni di CD Text alle tracce audio, selezionare prima di tutto la traccia. Fare clic con il pulsante destro del mouse e selezionare *Properties (Proprietà)*. Viene visualizzata una nuova finestra in cui è possibile immettere le informazioni desiderate.

La finestra di dialogo per la scrittura di un CD audio non è molto differente da quella per la scrittura di un CD dati. Tuttavia, le modalità *Disc at once (Aggiorna disco)* e *Track at once (Aggiorna traccia)* hanno una maggiore rilevanza. La modalità *Aggiorna traccia* consente di inserire una intermissione di due secondi dopo ogni traccia.

SUGGERIMENTO: salvaguardia dell'integrità dei dati

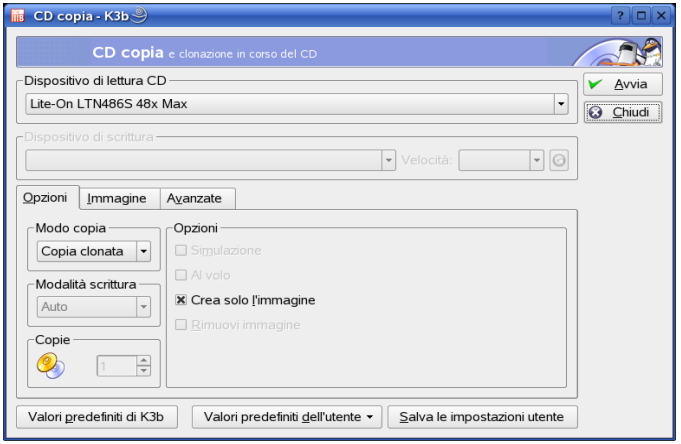
Quando si masterizzano CD audio, è consigliabile scegliere una velocità ridotta per limitare i rischi di errore durante la masterizzazione.

Dopo avere regolato tutte le impostazioni in base alle proprie esigenze, avviare il processo effettivo di masterizzazione scegliendo *Burn (Masterizza)*. In alternativa, salvare le impostazioni per usi e regolazioni futuri scegliendo *Save (Salva)*.

9.3 Copia di un CD o un DVD

Selezionare *Tools (Strumenti)* → *Copy CD (Copia CD)* oppure *Tools (Strumenti)* → *Copy DVD (Copia DVD)* in base al tipo di supporto. Nella finestra di dialogo visualizzata configurare le impostazioni per il dispositivo di lettura e scrittura, come illustrato nella Figura 9.3, «Copia di un CD» (p. 156). In questa finestra sono disponibili anche le opzioni di scrittura illustrate in precedenza. Una funzionalità aggiuntiva consente di creare diverse copie del CD o del DVD.

Figura 9.3 *Copia di un CD*



Selezionare *On the fly (Al volo)* per masterizzare il CD non appena viene letto oppure selezionare *Only create image (Crea solo immagine)* per creare un'immagine nel percorso specificato in *Temp Directory (Directory temporanea)* → *Write image file to (Scrivi file immagine in)* e masterizzare l'immagine in seguito.

9.4 Scrittura di immagini ISO

Se si dispone già di un'immagine ISO, selezionare *Tools (Strumenti)* → *CD* → *Burn CD image (Masterizza immagine CD)*. Viene aperta una finestra di dialogo in cui immettere l'ubicazione di *Immagine da scrivere*. K3b calcola una checksum e la visualizza in *MD5 Sum (Checksum MD5)*. Se il file ISO è stato scaricato da Internet, questa somma mostra se lo scaricamento è stato eseguito.

Utilizzare le schede *Opzioni* e *Avanzate* per impostare le preferenze desiderate. Per masterizzare il CD, fare clic su *Start (Avvia)*.

9.5 Creazione di un CD o un DVD multisessione

I dischi multisessione possono essere utilizzati per scrivere dati durante più sessioni di masterizzazione e risultano utili, ad esempio, per creare file di backup di dimensioni inferiori rispetto al supporto. In ogni sessione è possibile aggiungere un altro file di backup. L'aspetto interessante è che non si è limitati a utilizzare CD o DVD dati. In un disco multisessione è anche possibile aggiungere sessioni audio.

Per avviare un nuovo disco multisessione, procedere come indicato di seguito:

1. Creare innanzitutto il disco dati e aggiungere tutti i file. Non è possibile iniziare con una sessione CD audio. Prestare attenzione a non esaurire lo spazio del disco perché altrimenti non sarà possibile aggiungere una nuova sessione.

2. Masterizzare i dati selezionando *Project (Progetto)* → *Burn (Masterizza)*. Viene visualizzata una finestra di dialogo.

3. Visualizzare la scheda *Settings (Impostazioni)* e selezionare *Start Multisession (Avvia multisessione)*.

4. Se necessario, configurare altre opzioni. Vedere anche la Sezione 9.1, «Creazione di un CD di dati» (p. 151).

5. Avviare la sessione di masterizzazione scegliendo *Burn (Masterizza)*.

Se il processo di masterizzazione ha esito positivo, viene creato un disco multisessione. Se nel supporto è disponibile spazio sufficiente, è possibile aggiungere altre sessioni. Finalizzare i dischi solo se si è certi di non dover salvare altre sessioni oppure se lo spazio è esaurito.

NOTA: Informazioni sullo spazio di memorizzazione disponibile nei dischi multisessione

Si tenga presente che i dischi multisessione richiedono spazio per registrare tutte le voci delle sessioni. Di conseguenza, nel disco sarà disponibile una quantità di spazio minore, che dipende dal numero di sessioni salvate.

9.6 Ulteriori informazioni

K3b offre altre funzioni, oltre alle due principali descritte sopra, che consentono ad esempio di creare copie di DVD, leggere dati audio in formato WAV, riscrivere CD e riprodurre musica con il lettore audio integrato. Una descrizione dettagliata di tutte le funzionalità del programma è disponibile all'indirizzo http://k3b.sourceforge.net.

Parte IV. Ufficio

10 Suite per l'ufficio OpenOffice.org

OpenOffice.org è una potente suite Linux che offre strumenti per tutti i tipi di compiti d'ufficio, come scrittura di testi, utilizzo di fogli di calcolo o creazione di illustrazioni e presentazioni. OpenOffice.org consente di utilizzare gli stessi dati su più piattaforme di elaborazione. È anche possibile aprire e modificare file in formati Microsoft Office e salvarli nello stesso formato, se necessario. In questo capitolo sono illustrate solo le operazioni di base necessarie per iniziare a lavorare con OpenOffice.org. Avviare l'applicazione dal menu di SUSE oppure mediante il comando `ooffice`.

In OpenOffice.org sono inclusi alcuni moduli di applicazioni (sottoprogrammi), progettati per interagire reciprocamente. Tali moduli sono elencati nella Tabella 10.1, «Moduli delle applicazioni di OpenOffice.org» (p. 161). In questo capitolo vengono descritte le funzioni di Writer. Una descrizione esaustiva di ciascun modulo è disponibile nella guida in linea come descritto nella Sezione 10.6, «Ulteriori informazioni» (p. 168).

Tabella 10.1 *Moduli delle applicazioni di OpenOffice.org*

Writer	Potente applicazione di elaborazione di testi
Calc	Foglio di lavoro che include un'utility per la creazione di grafici
Draw	Applicazione di disegno per la creazione di grafica vettoriale
Math	Applicazione per la generazione di formule matematiche
Impress	Applicazione per la creazione di presentazioni

L'aspetto dell'applicazione varia in relazione al tipo di desktop o di gestore delle finestre in uso. Vengono inoltre utilizzati i formati delle finestre di dialogo di apertura e salvataggio per il desktop. Indipendentemente dall'aspetto, il layout e le funzioni di base sono le stesse.

10.1 Compatibilità con altre applicazioni per l'ufficio

OpenOffice.org è in grado di utilizzare documenti, fogli di calcolo, presentazioni e database di Microsoft Office. Questi tipi di documenti possono essere aperti normalmente come gli altri file e salvati nel formato originale. Poiché i formati Microsoft sono chiusi e le specifiche non sono disponibili per altre applicazioni, in qualche caso possono verificarsi problemi di formattazione. Se si riscontrano problemi nei documenti, può essere opportuno aprirli nell'applicazione originale e salvarli nuovamente in un formato aperto, quale RTF per i documenti di testo o CSV per i fogli di calcolo.

Per convertire un certo numero di documenti, ad esempio durante il passaggio iniziale all'applicazione, selezionare *File (File) → Wizard (Procedura guidata) → Document Converter (Convertitore documenti)*. Selezionare il formato di file da convertire. Sono disponibili diversi formati StarOffice e Microsoft Office. Dopo aver selezionato un formato, fare clic su *Next (Avanti)* e specificare dove OpenOffice.org dovrà cercare i modelli e documenti da convertire e in quale directory dovranno essere posizionati i file convertiti. Prima di continuare, verificare che tutte le altre impostazioni siano corrette. Fare clic su *Avanti* per visualizzare un riepilogo delle azioni da eseguire che consente di controllare che tutte le impostazioni siano corrette. Iniziare quindi la conversione selezionando *Converti*.

IMPORTANTE: Individuazione dei file di Windows

I documenti di una partizione Windows sono in genere posizionati in una sottodirectory di `/windows`.

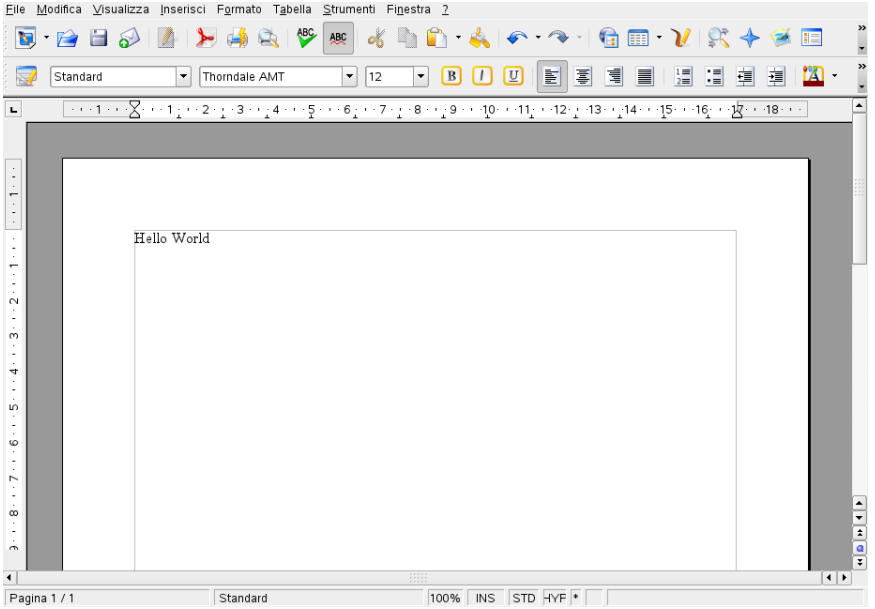
Quando si condividono documenti con altri utenti, è possibile scegliere tra varie opzioni. Se il destinatario deve soltanto leggere il documento, esportarlo in un file PDF mediante

File (File) → Export as PDF (Esporta come PDF). I file PDF possono essere letti su qualsiasi piattaforma che disponga di un visualizzatore quale Adobe Acrobat Reader. Per condividere un documento per la modifica, utilizzare uno dei normali formati di documento. I formati di default sono conformi al formato XML standard OASIS e pertanto sono compatibili con diverse applicazioni. I formati TXT e RTF, sebbene presentino una formattazione limitata, possono rappresentare una valida opzione per i documenti di testo. Il formato CSV è adatto ai fogli di calcolo. In OpenOffice.org può anche essere disponibile il formato preferito del destinatario, in particolare i formati Microsoft.

OpenOffice.org è disponibile per numerosi sistemi operativi e rappresenta quindi un ottimo strumento nel caso di gruppi di utenti che devono condividere frequentemente i file e non dispongono dello stesso sistema nei computer in uso.

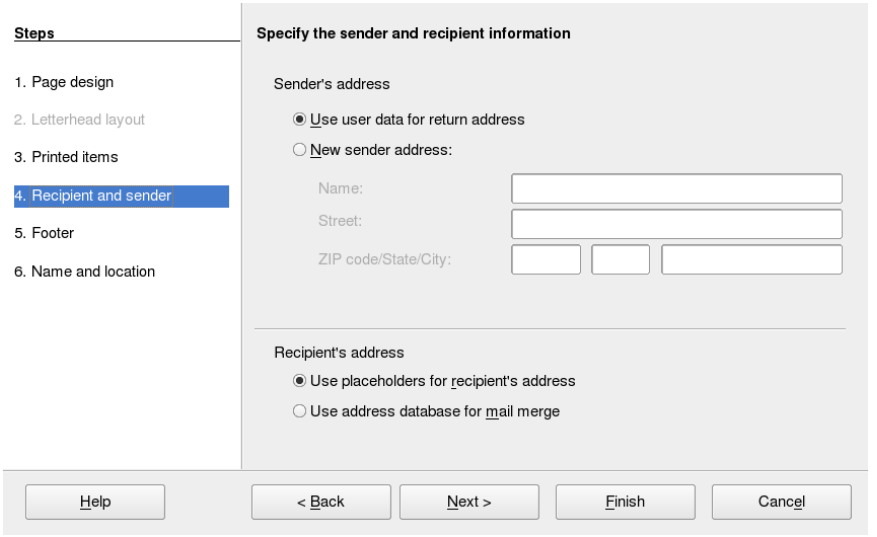
10.2 Elaborazione di testi con Writer

Figura 10.1 *Writer di OpenOffice.org*



È possibile creare un nuovo documento in due modi. Per creare un documento da zero, utilizzare *File (File)* → *New (Nuovo)* → *Text Document (Documento di testo)*. Per utilizzare un formato standard ed elementi predefiniti per i documenti, scegliere una procedura guidata. Le procedure guidate sono piccole utility che consentono di effettuare alcune scelte di base e di produrre un documento direttamente da un modello. Per creare una lettera commerciale, ad esempio, selezionare *File (File)* → *Wizards (Procedure guidate)* → *Letter (Lettera)*. Utilizzando le finestre di dialogo della procedura guidata, è possibile creare facilmente un documento base mediante un formato standard. Una finestra di dialogo di esempio della procedura guidata è illustrata nella Figura 10.2, «Procedura guidata di OpenOffice.org» (p. 164).

Figura 10.2 *Procedura guidata di OpenOffice.org*



Immettere il testo nella finestra del documento in base alle esigenze. Utilizzare la barra degli strumenti *Formatting (Formattazione)* o il menu *Format (Formato)* per modificare l'aspetto del documento. Utilizzare le opzioni del menu *File (File)* o i pulsanti appropriati nella barra degli strumenti per stampare o salvare il documento. Le opzioni del menu *Insert (Inserisci)* consentono di aggiungere ulteriori elementi al documento, ad esempio una tabella, un'immagine o un grafico.

10.2.1 Selezione di testo

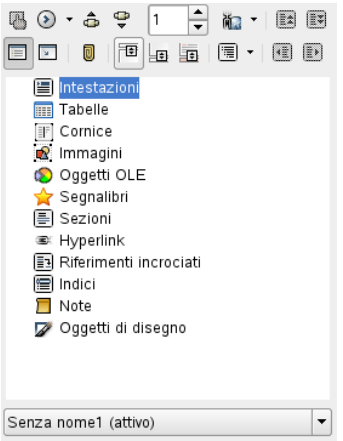
Per selezionare il testo, fare clic nel punto desiderato di inizio della selezione e, tenendo premuto il pulsante del mouse, spostare il cursore alla fine dell'intervallo (che può essere costituito da caratteri, righe o da interi paragrafi). Rilasciare il pulsante del mouse quando tutto il testo desiderato è stato selezionato. A questo punto, il testo è visualizzato con i colori invertiti. Aprire il menu contestuale facendo clic con il pulsante destro del mouse sulla selezione. Utilizzare il menu contestuale per modificare font, stile del font e altre proprietà del testo.

Il testo selezionato può essere tagliato o copiato negli Appunti e successivamente incollato in un altro punto del documento. Utilizzare il menu contestuale *Edit (Modifica)* o le icone della barra degli strumenti appropriate per accedere a queste funzioni.

10.2.2 Navigazione in documenti estesi

Nel riquadro di navigazione sono visualizzate informazioni sul contenuto di un documento. È inoltre possibile passare rapidamente ai diversi elementi inclusi. Ad esempio, utilizzare il riquadro di navigazione per ottenere una rapida panoramica di tutti i capitoli o per visualizzare un elenco delle immagini incluse nel documento. Per aprirlo, selezionare *Edit (Modifica)* → *Navigator (Navigatore)*. Nella Figura 10.3, «Riquadro di navigazione di Writer» (p. 166) è illustrato il riquadro di navigazione attivo. Gli elementi riportati nel riquadro di navigazione variano in base al documento caricato in Writer.

Figura 10.3 *Riquadro di navigazione di Writer*



10.2.3 Formattazione con gli stili

La finestra di dialogo visualizzata selezionando *Format (Formato)* → *Styles and Formatting (Stili e formattazione)* consente di formattare il testo in vari modi. Se si seleziona *Automatic (Automatico)* dall'elenco a discesa che si trova nella parte inferiore della finestra di dialogo, in OpenOffice.org verrà presentata una selezione di stili adattati all'attività in corso. Se si seleziona *All Styles (Tutti gli stili)*, saranno disponibili tutti gli stili del gruppo attualmente attivo. Selezionare i gruppi mediante i pulsanti posti nella parte superiore.

Formattando il testo mediante questa procedura, definita *formattazione parziale*, la formattazione non viene applicata direttamente al testo, bensì uno stile viene applicato al testo. Lo stile può essere facilmente modificato e le modifiche vengono applicate alla formattazione di tutto il testo a cui tale stile è assegnato.

Per assegnare uno stile a un paragrafo, selezionare lo stile da utilizzare e fare clic sulla tavolozza dei colori in *Styles and Formatting (Stili e formattazione)*. Fare clic sui paragrafi ai quali assegnare lo stile. Per terminare l'assegnazione dello stile, premere Esc (Esc) o fare nuovamente clic sulla tavolozza dei colori.

È possibile creare facilmente i propri stili formattando un paragrafo o un carattere mediante il menu *Format (Formato)* o la barra degli strumenti. Selezionare l'elemento formattato da cui copiare lo stile, fare clic a destra della tavolozza in *Styles and*

Formatting (Stili e formattazione) e tenere premuto il pulsante, quindi scegliere *New Style from Selection (Nuovo stile da selezione)* dal menu visualizzato. Immettere un nome per lo stile e fare clic su *OK*. Questo stile può essere applicato ad altre parti di testo.

Per modificare le proprietà di uno stile, selezionarlo dall'elenco, quindi fare clic con il pulsante destro del mouse e scegliere *Modify (Modifica)* dal menu. Viene aperta una finestra di dialogo in cui è possibile selezionare e modificare tutte le proprietà di formattazione.

10.3 Introduzione a Calc

Calc è l'applicazione per fogli di calcolo di OpenOffice.org. Creare un nuovo foglio di calcolo selezionando *File (File) → New (Nuovo) → Spreadsheet (Foglio di calcolo)* o aprirne uno mediante *File (File) → Open (Apri)*. In Calc è possibile leggere e salvare file nel formato Microsoft Excel.

Nelle celle del foglio di calcolo immettere dati o formule fissi. Una formula consente di utilizzare dati di altre celle per generare un valore nella cella in cui è stata immessa. È inoltre possibile creare grafici sulla base dei valori delle celle.

10.4 Introduzione a Impress

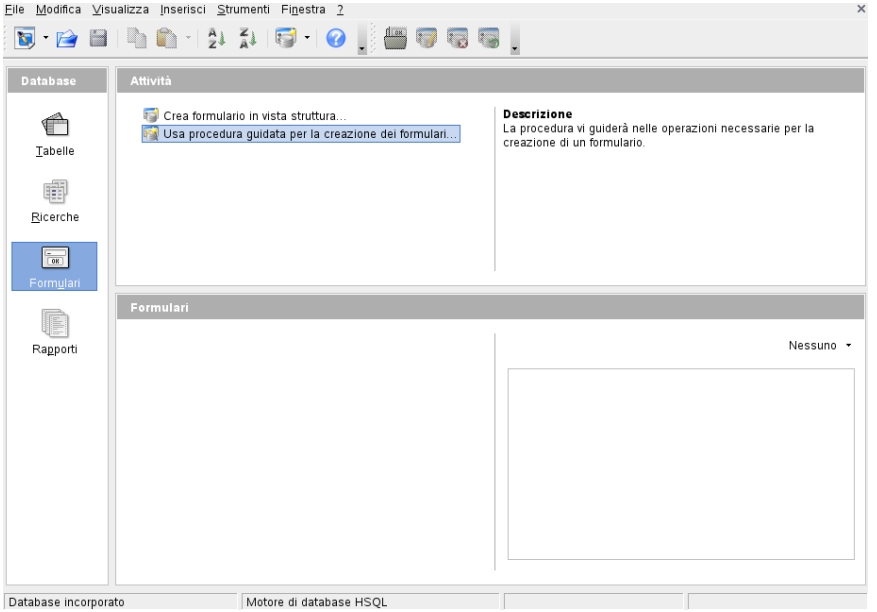
Impress è progettato per la creazione di presentazioni destinate alla visualizzazione su schermo o alla stampa, ad esempio i lucidi. Creare una presentazione da zero mediante *File (File) → New (Nuovo) → Presentation (Presentazione)*. Per creare una presentazione con il supporto di una procedura guidata, utilizzare *File (File) → Wizards (Procedure guidate) → Presentation (Presentazione)*. Aprire una presentazione esistente con *File (File) → Open (Apri)*. In Impress è possibile aprire e salvare presentazioni Microsoft PowerPoint.

10.5 Introduzione a Base

In OpenOffice 2.0 è stato introdotto un nuovo modulo di database. Creare un database mediante *File (File) → New (Nuovo) → Database (Database)*. Viene visualizzata una

procedura guidata per agevolare la creazione del database. In Base possono inoltre essere utilizzati database di Microsoft Access.

Figura 10.4 *Base—database in OpenOffice.org*



Le tabelle, i moduli, le query e i rapporti possono essere creati manualmente o tramite utili procedure guidate. La procedura guidata per la creazione di tabelle, ad esempio, contiene numerosi campi per uso personale o aziendale. I database creati in Base possono essere utilizzati come origini dati, ad esempio nella creazione di lettere tipo.

10.6 Ulteriori informazioni

In OpenOffice.org sono incluse numerose opzioni che forniscono vari livelli di informazioni. Per ottenere informazioni complete su un argomento, selezionare *Help (Guida) → OpenOffice.org Help (Guida di OpenOffice.org)*. Il sistema di guida fornisce informazioni approfondite su ciascuno dei moduli di OpenOffice.org (Writer, Calc, Impress e così via).

Al primo avvio dell'applicazione vengono visualizzate le informazioni *Tips (Suggerimenti)*, descrizioni sintetiche dei pulsanti visualizzate al passaggio del mouse,

e *Help Agent (Agente Guida)*, argomenti basati sulle azioni eseguite. Per ottenere informazioni più complete sui pulsanti rispetto a quelle fornite in *Tips (Suggerimenti)*, selezionare *Help (Guida)* → *What's This (Guida rapida)*, quindi posizionare il mouse sui pulsanti desiderati. Per interrompere la modalità *What's This (Guida rapida)*, fare clic in un punto qualsiasi. Se questa funzione è utilizzata frequentemente, è possibile abilitare *Extended Tips (Suggerimenti estesi)* in *Tools (Strumenti)* → *Options (Opzioni)* → *OpenOffice.org (OpenOffice.org)* → *General (Generale)*. In questa finestra è possibile abilitare anche *Help Agent (Agente Guida)* e *Tips (Suggerimenti)*.

Nel sito Web di OpenOffice.org, `http://www.openoffice.org` (in lingua inglese), è possibile trovare mailing list, articoli e informazioni sui bug. In questo sito sono disponibili le versioni per il download di numerosi sistemi operativi.

Evolution, programma per la gestione della posta e del calendario

11

Evolution è una suite groupware che dispone delle comuni funzionalità e-mail e di funzionalità estese, quali l'elenco delle attività e il calendario. L'applicazione fornisce inoltre una rubrica completa che consente di inviare le informazioni sui contatti in formato vCard.

Avviare Evolution dal menu principale o con il comando `evolution`. La prima volta che si avvia Evolution, è disponibile un assistente di configurazione, descritto nella Sezione 11.3.1, «Configurazione degli account» (p. 174).

IMPORTANTE: account di Microsoft Exchange

Per utilizzare Evolution con Microsoft Exchange, è necessario installare il pacchetto `ximian-connector`. Eseguire l'installazione mediante YaST.

11.1 Importazione di messaggi e-mail da altri programmi di posta

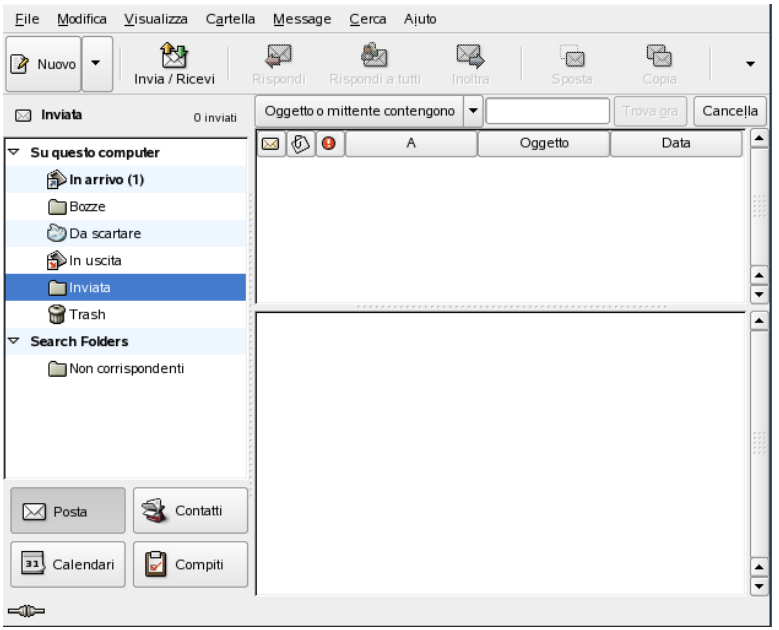
Per importare messaggi e-mail da altri programmi di posta, ad esempio Netscape, selezionare *File (File)* → *Import (Importa)*. Per i formati mbox, selezionare *Import a single file (Importa un file singolo)*. Per Netscape, selezionare *Import data and settings*

from older programs (Importa dati e impostazioni da programmi precedenti). Per utilizzare dati provenienti da programmi che utilizzano il formato maildir, ad esempio KMail, configurare un account per l'accesso alla directory della posta.

11.2 Panoramica di Evolution

La Figura 11.1, «Finestra di Evolution con messaggi e-mail» (p. 172) illustra la vista della finestra di default. I menu, le voci di menu e le icone nella barra degli strumenti variano in base al componente aperto. Utilizzare il riquadro a sinistra per selezionare le informazioni da visualizzare nel riquadro di destra. Modificare le dimensioni dei riquadri trascinando le barre di divisione.

Figura 11.1 *Finestra di Evolution con messaggi e-mail*



11.2.1 Messaggi e-mail

In questa vista, la metà superiore della finestra visualizza il contenuto della cartella corrente. La metà inferiore è un riquadro di anteprima utilizzato per visualizzare il

messaggio e-mail selezionato. Per visualizzare una diversa cartella, selezionarne una dall'elenco delle cartelle nel riquadro a sinistra.

Utilizzare la barra di ricerca per eseguire la ricerca di messaggi all'interno di una cartella. Per ordinare i messaggi in base all'intestazione di una tabella, fare clic sull'intestazione desiderata. La freccia a destra indica se la colonna è ordinata in modo crescente o decrescente. Fare clic sull'intestazione della colonna finché i messaggi sono ordinati nel modo desiderato.

11.2.2 Contatti

Questa vista visualizza gli indirizzi della rubrica dell'utente. Per individuare un indirizzo specifico, utilizzare la barra di ricerca o fare clic sul pulsante a destra che visualizza l'iniziale del cognome del contatto. Aggiungere contatti o elenchi mediante la barra degli strumenti.

11.2.3 Calendario

La visualizzazione iniziale contiene una vista del giorno corrente, con il mese e l'elenco delle attività mostrati in un riquadro aggiuntivo a destra. Dalla barra degli strumenti o dal menu *View (Visualizza)* è inoltre possibile accedere alle viste relative alla settimana, alla settimana lavorativa e al mese. Utilizzare la barra di ricerca per trovare un appuntamento immesso nel calendario. Utilizzare i pulsanti della barra degli strumenti per aggiungere appuntamenti e attività. È inoltre possibile utilizzare la barra degli strumenti per sfogliare le pagine del calendario o passare a una data specifica.

11.2.4 Attività

Task (Attività) fornisce un elenco delle attività. I dettagli relativi all'attività selezionata vengono visualizzati nella parte inferiore della finestra. Utilizzare*File (File) → New (Nuovo) → Task (Attività)* per aggiungere una nuova attività. Eseguire la ricerca delle attività con la barra di ricerca. Fare clic con il pulsante destro del mouse sull'attività e selezionare *Assign Task (Assegna attività)*. Selezionare *Open (Apri)* per aggiungere all'attività ulteriori dettagli, ad esempio la data prevista e lo stato di completamento.

11.3 Posta

Il componente per la gestione della posta presente in Evolution può essere utilizzato con numerosi account in diversi formati. Questo componente offre utili funzionalità, ad esempio le cartelle virtuali per visualizzare i risultati della ricerca e il filtro per la posta indesiderata. Configurare l'applicazione da *Edit (Modifica)* → *Preferences (Preferenze)*.

11.3.1 Configurazione degli account

Con Evolution è possibile richiamare messaggi e-mail da più account di posta. È possibile selezionare l'account dal quale si desidera inviare messaggi e-mail quando si compone un messaggio. Configurare gli account di posta da *Edit (Modifica)* → *Preferences (Preferenze)* → *Mail Accounts (Account di posta)*. Per modificare una configurazione esistente, selezionarla e fare clic su *Edit (Modifica)*. Per cancellare un account, selezionarlo e fare clic su *Delete (Cancella)*.

Per aggiungere un nuovo account, fare clic su *Add (Aggiungi)*. In questo modo viene aperto l'assistente di configurazione. Per utilizzarlo fare clic su *Forward (Avanti)*. Immettere il nome e l'indirizzo di e-mail nei campi corrispondenti. Se lo si desidera, è possibile immettere informazioni facoltative. Selezionare *Make this my default account (Imposta questo account come default)* per utilizzare questo account come default quando si scrivono messaggi. Fare clic su *Forward (Avanti)*.

Selezionare il formato di messaggi e-mail in entrata appropriato per questo indirizzo in *Server Type (Tipo di server)*. Il formato più comune per scaricare la posta da un server remoto è *POP (POP)*. Il formato *IMAP (IMAP)* viene utilizzato per le cartelle di posta su server speciali. Richiedere questa informazione all'ISP o all'amministratore del server. Completare gli altri campi rilevanti dopo aver selezionato il tipo di server. Al termine, fare clic su *Forward (Avanti)*. Se disponibili, selezionare le *Receiving Options (Opzioni di ricezione)*. Fare clic su *Forward (Avanti)*.

Configurare quindi le opzioni di consegna della posta. Per inviare messaggi e-mail al sistema locale, selezionare *Sendmail (Invia e-mail)*. Per un server remoto, selezionare *SMTP (SMTP)*. Richiedere informazioni all'ISP o all'amministratore del server. Per l'opzione SMTP, completare gli altri campi visualizzati dopo la selezione. Al termine, fare clic su *Forward (Avanti)*.

Per default, l'indirizzo di e-mail viene utilizzato come nome per l'identificazione dell'account. Se lo si desidera, è possibile immettere un nome diverso. Fare clic su *Forward (Avanti)*. Fare clic su *Apply (Applica)* per salvare la configurazione dell'account.

Per impostare un account come account di default per l'invio di messaggi e-mail, selezionare l'account desiderato, quindi fare clic su *Default (Default)*. Per disabilitare la funzione di richiamo di messaggi e-mail da un account, selezionare l'account e quindi fare clic su *Disable (Disabilita)*. L'account disabilitato può essere utilizzato come indirizzo per l'invio, ma non viene più controllato per quando riguarda i messaggi e-mail in entrata. Se necessario, riattivare l'account con *Enable (Abilita)*.

11.3.2 Creazione di messaggi

Per comporre un nuovo messaggio, fare clic su *Nuovo → Mail Message (Messaggio)*. La risposta a un messaggio o il suo inoltro determina l'apertura dello stesso editor di messaggi. Passare a *From (Da)* e selezionare l'account dal quale si desidera inviare il messaggio. Nei campi relativi al destinatario, immettere un indirizzo e-mail o parte del nome o dell'indirizzo presenti nella rubrica. Se viene individuata una corrispondenza tra quanto immesso e i dati contenuti nella rubrica, viene visualizzato un elenco per la selezione. Fare clic sul contatto desiderato o completare l'immissione se non esistono corrispondenze. Per selezionare un destinatario dalla rubrica, fare clic su *To (A)* oppure *CC (CC)*.

Evolution consente di inviare messaggi e-mail in formato testo o HTML. Per formattare messaggi in formato HTML , selezionare *Format (Formato)* nella barra degli strumenti. Per inviare allegati, selezionare *Attach (Allega)* oppure *Insert (Inserisci) → Attachment (Allegato)*.

Per inviare il messaggio, fare clic su *Send (Invia)*. Se non si desidera inviare immediatamente il messaggio, scegliere un comando dal menu *File (File)*. Ad esempio, salvare il messaggio come bozza e inviarlo successivamente.

11.3.3 Messaggi e-mail cifrati e firme

In Evolution è supportata la cifratura dei messaggi e-mail tramite PGP. che include la firma e la verifica dei messaggi e-mail firmati. Per utilizzare queste funzionalità, generare e gestire chiavi con un'applicazione esterna, ad esempio gpg o KGpg.

Per firmare un messaggio e-mail prima di inviarlo, selezionare *Security (Sicurezza) → PGP sign (Firma PGP)*. Quando si fa clic su *Send (Invia)*, una finestra di dialogo richiede l'immissione della password della chiave segreta. Immettere la password e chiudere la finestra di dialogo facendo clic su *OK* per inviare il messaggio e-mail firmato. Per inviare altri messaggi e-mail nel corso della sessione corrente senza la necessità di «sbloccare» ripetutamente la chiave segreta, selezionare *Remember this password for the remainder of this session (Ricorda questa password)*.

Quando si ricevono messaggi e-mail firmati da altri utenti, alla fine del messaggio viene visualizzata un'icona che raffigura un lucchetto. Se si fa clic sull'icona, viene avviato un programma esterno (gpg) per il controllo della firma. Se la firma è valida, viene visualizzato un segno di spunta verde accanto al simbolo del lucchetto. Se la firma non è valida, viene visualizzato un lucchetto spezzato.

La operazioni di cifratura e decifratura dei messaggi e-mail sono estremamente semplici. Dopo aver composto il messaggio e-mail, passare a *Security (Sicurezza) → PGP encrypt (Cifratura PGP)* e inviare il messaggio. Quando si ricevono messaggi cifrati, una finestra di dialogo chiede la password della chiave segreta. Immettere la password per decifrare il messaggio e-mail.

11.3.4 Cartelle

È spesso consigliabile ordinare i messaggi e-mail in diverse cartelle. L'albero delle cartelle è visualizzato nel riquadro a sinistra. Se si accede alla posta tramite IMAP, le cartelle IMAP vengono visualizzate anche in questa barra delle cartelle. Per il formato POP e la maggior parte degli altri formati, le cartelle sono memorizzate localmente, ordinate in *Local Folders (Cartelle locali)*.

Per default, sono incluse diverse cartelle. Nella cartella *Inbox (Posta in arrivo)* vengono inizialmente inseriti i nuovi messaggi recuperati da un server. La cartella *Sent (Posta inviata)* viene utilizzata per salvare le copie dei messaggi e-mail inviati. La cartella *Outbox (Posta in uscita)* consente la memorizzazione temporanea dei messaggi e-mail non ancora inviati. È utile se non si lavora in linea o se il server della posta in uscita non è momentaneamente raggiungibile. La cartella *Drafts (Bozze)* viene utilizzata per il salvataggio dei messaggi e-mail non completati. La cartella *Trash (Cestino)* è progettata per la memorizzazione temporanea degli elementi cancellati. La cartella *Junk (Posta indesiderata)* è utilizzata per la funzionalità di filtro della posta indesiderata di Evolution.

È possibile creare nuove cartelle in *On This Computer (Risorse locali)* oppure creare sottocartelle di cartelle esistenti. È possibile creare una gerarchia di cartelle complessa. Per creare una nuova cartella, selezionare *File (File)* → *New (Nuovo)* → *Mail Folder (Cartella posta)*. Nella finestra di dialogo Mail Folder (Cartella posta), immettere un nome per la nuova cartella. Utilizzare il mouse per determinare in quale cartella superiore inserire la nuova cartella. Fare clic su *OK* per chiudere la finestra di dialogo.

Per spostare un messaggio in una determinata cartella, selezionare il messaggio da spostare. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida. Selezionare *Move to Folder (Sposta nella cartella)* quindi selezionare la cartella di destinazione nella finestra di dialogo che viene visualizzata. Fare clic su *OK* per spostare il messaggio. Sull'intestazione del messaggio nella cartella originale viene tracciata una linea, per indicare che il messaggio è contrassegnato per essere cancellato dalla cartella in questione. Il messaggio viene memorizzato nella nuova cartella. Per copiare i messaggi, la procedura è simile.

Spostare manualmente un certo numero di messaggi in diverse cartelle può richiedere tempo. Per automatizzare questa procedura, è possibile utilizzare i filtri.

11.3.5 Filtri

In Evolution sono presenti diverse opzioni per filtrare i messaggi e-mail. È possibile utilizzare i filtri per spostare un messaggio in una specifica cartella oppure per cancellare un messaggio. È inoltre possibile spostare i messaggi direttamente nel cestino tramite un filtro. Esistono due opzioni per la creazione di un nuovo filtro: la creazione di un filtro completamente nuovo o la creazione di un filtro sulla base del messaggio da filtrare. Questa seconda opzione è estremamente utile per filtrare i messaggi inviati a una mailing list.

Impostazione di un filtro

Selezionare *Tools (Strumenti)* → *Filters (Filtri)*. Questa finestra di dialogo elenca i filtri esistenti, che possono essere modificati o cancellati. Fare clic su *Add (Aggiungi)* per creare un nuovo filtro. In alternativa, creare un filtro basato su un messaggio, selezionare il messaggio, quindi *Tools (Strumenti)* → *Create Filter from Message (Crea filtro da messaggio)*.

Immettere un nome per il nuovo filtro in *Rule Name (Nome regola)*. Selezionare i criteri per l'utilizzo del filtro. Le opzioni includono il mittente, i destinatari, l'account di origine,

l'oggetto, la data e lo stato. La casella di riepilogo a discesa in cui è visualizzata la voce *Contains (Contiene)* fornisce numerose opzioni, ad esempio *contiene*, *uguale a* , e *diverso da.* Selezionare la condizione appropriata. Immettere il testo per la ricerca. Fare clic su *Add (Aggiungi)* per aggiungere ulteriori criteri di filtro. Utilizzare *Execute actions (Esegui azioni)* per determinare se per l'applicazione del filtro è necessario rispettare tutti i criteri solo alcuni.

Nella parte inferiore della finestra, determinare l'azione da intraprendere quando i criteri del filtro sono rispettati. È ad esempio possibile spostare o copiare i messaggi in una cartella o assegnare loro un colore particolare. Quando si esegue uno spostamento o una copia, fare clic per selezionare la cartella di destinazione. Nell'elenco di cartelle visualizzato, selezionare la cartella desiderata. Per creare una nuova cartella, fare clic su *New (Nuova)*. Fare clic su *OK* dopo aver selezionato la cartella desiderata. Dopo aver creato il filtro, fare clic su *OK*.

Applicazione dei filtri

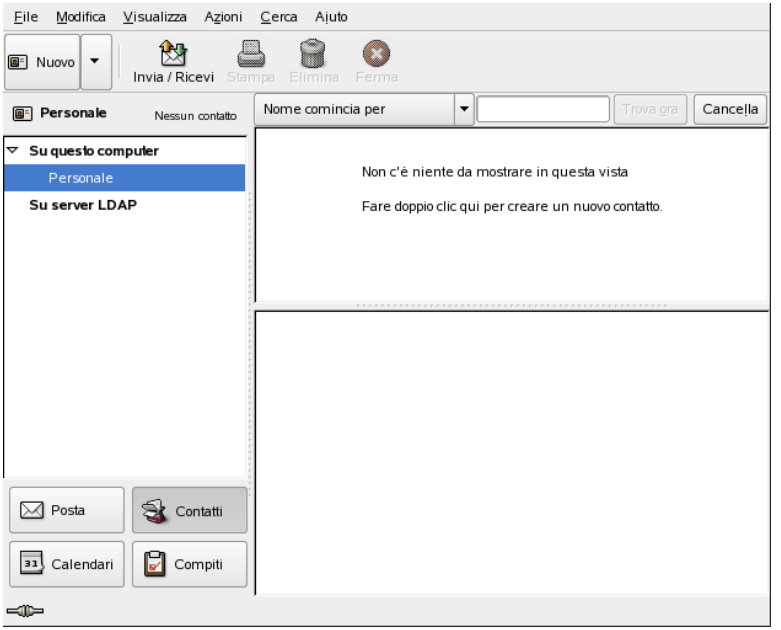
I filtri vengono applicati nell'ordine elencato nella finestra di dialogo visualizzata facendo clic su *Tools (Strumenti) → Filters (Filtri)*. Per modificare l'ordine, evidenziare un filtro e fare clic su *Up (Su)* o *Down (Giù)*. Al termine, fare clic su *OK* per chiudere la finestra di dialogo del filtro.

I filtri vengono applicati a tutti i nuovi messaggi. Non vengono tuttavia applicati ai messaggi già presenti nelle cartelle. Per applicare i filtri ai messaggi già ricevuti, selezionare i messaggi desiderati, quindi selezionare *Actions (Azioni) → Apply Filters (Applica filtri)*.

11.4 Contatti

In Evolution è possibile utilizzare diverse rubriche. Le rubriche disponibili vengono elencate nel riquadro a sinistra. Cercare il contatto desiderato utilizzando la barra di ricerca. È possibile aggiungere i contatti alla rubrica di Evolution in diversi formati, utilizzando *File (File) → Import (Importa)*. Fare clic con il pulsante destro del mouse su un contatto per aprire un menu dal quale selezionare diverse opzioni, ad esempio l'inoltro del contatto o il salvataggio come vCard. Fare doppio clic su un contatto se si desidera modificarlo.

Figura 11.2 *Rubrica di Evolution*



11.4.1 Aggiunta di contatti

Oltre al nome e all'indirizzo di e-mail, in Evolution è possibile memorizzare altre informazioni personali relative all'indirizzo o ai contatti. Per aggiungere velocemente l'indirizzo di e-mail di un mittente, fare clic con il pulsante destro del mouse sull'indirizzo contrassegnato nell'anteprima del messaggio. Per immettere un contatto completamente nuovo, fare clic su *New Contact (Nuovo contatto)* dalla vista *Contacts (Contatti)*. Entrambi i metodi consentono di aprire una finestra di dialogo in cui immettere le informazioni relative ai contatti.

Nella scheda *Contact (Contatto)*, immettere il nome del contatto, gli indirizzi di e-mail, i numeri di telefono e le identità per la messaggistica in tempo reale. La scheda *Personal Information (Informazioni personali)* è destinata agli indirizzi Web e ad altre informazioni personali. Immettere le altre informazioni relative all'indirizzo del contatto in *Mailing Address (Indirizzo)*. Dopo aver immesso tutti i dettagli relativi al contatto, fare clic su *OK* per aggiungerlo alla rubrica.

11.4.2 Creazione di un elenco

Se si inviano frequentemente messaggi e-mail a un gruppo di persone, è possibile semplificare il processo creando un elenco che contiene tali indirizzi. Fare clic su *File (File) → New (Nuovo) → Contact List (Elenco contatti)*. Verrà visualizzato l'editor dell'elenco dei contatti. Immettere un nome per l'elenco. Aggiungere gli indirizzi digitandoli nella casella e facendo clic su *Add (Aggiungi)* oppure trascinando i contatti dalla vista *Contacts (Contatti)* e rilasciandoli nella casella. Attivare/Disattivare *Hide addresses (Nascondi indirizzi)* per determinare se i destinatari possono vedere gli altri destinatari del messaggio e-mail. Al termine, fare clic su *OK*. L'elenco è ora uno dei contatti dell'utente e viene visualizzato nella finestra di composizione dopo aver digitato le prime lettere.

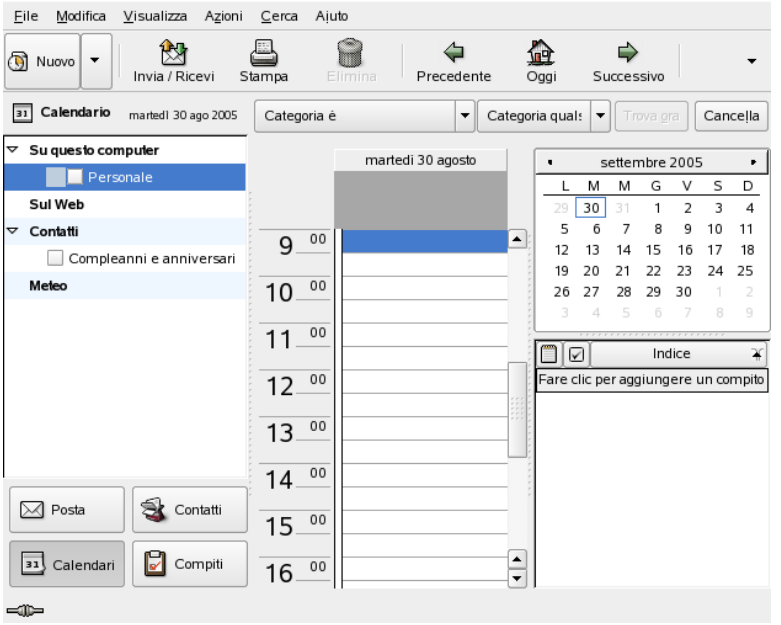
11.4.3 Aggiunta di rubriche

Configurare rubriche aggiuntive di GroupWise ed Exchange nella configurazione di uno specifico account. Per aggiungere altre rubriche locali o LDAP, selezionare *File (File) → New (Nuovo) → Address Book (Rubrica)*. Nelle finestra di dialogo visualizzata, selezionare il tipo di rubrica e immettere le informazioni necessarie.

11.5 Calendari

Con Evolution è possibile utilizzare più calendari. Per importare i calendari in formato iCalendar, scegliere *File (File) → Import (Importa)*. Utilizzare il calendario per immettere appuntamenti e pianificare riunioni con altre persone. Se lo si desidera, impostare una nota per sapere quando stanno per iniziare gli appuntamenti pianificati.

Figura 11.3 *Calendario di Evolution*



11.5.1 Aggiunta di appuntamenti

Per aggiungere nuovi appuntamenti al calendario, fare clic su *File (File)* → *New (Nuovo)* → *Appointment (Appuntamento)*. Nella scheda *Appointment (Appuntamento)*, immettere i dettagli relativi all'appuntamento. Se lo si desidera, selezionare una categoria per semplificare la ricerca e l'ordinamento successivi. È inoltre possibile utilizzare *Alarm (Avviso)* per impostare un allarme in modo che Evolution avvisi l'utente prima dell'inizio dell'appuntamento. Se l'appuntamento si verifica regolarmente, impostare le date ricorrenti in *Recurrence (Ricorrenza)*. Fare clic su *OK* al termine di tutte le impostazioni. Il nuovo appuntamento viene quindi visualizzato nel calendario.

11.5.2 Pianificazione di una riunione

Per pianificare una riunione con altre persone, selezionare *File (File)* → *New (Nuovo)* → *Meeting (Riunione)*. Immettere le informazioni seguendo la procedura utilizzata per l'immissione di un appuntamento. Aggiungere i partecipanti in *Invitations (Inviti)* o

Scheduling (Pianificazione). Per immettere i partecipanti dalla rubrica, utilizzare *Contacts (Contatti)* per aprire un elenco di contatti della rubrica. È possibile utilizzare *Scheduling (Pianificazione)* anche per pianificare un orario che sia accettabile per tutti i partecipanti. Dopo aver scelto i partecipanti, premere *Autopick (Scelta automatica)* per individuare automaticamente l'ora.

11.5.3 Aggiunta di calendari

È consigliabile configurare i calendari di GroupWise e di Exchange nella configurazione dell'account. Per aggiungere calendari locali o calendari Web, selezionare *File (File)* → *New (Nuovo)* → *Calendar (Calendario)*. Selezionare il tipo desiderato e immettere le informazioni necessarie.

11.6 Sincronizzazione dei dati con un palmare

Evolution è progettato in modo che i dati possano essere sincronizzati con dispositivi palmari, quali Palm. Per la sincronizzazione viene utilizzato GNOME Pilot. Selezionare *Tools (Strumenti)* → *Pilot Settings (Impostazioni Pilot)* per aprire la procedura guidata di configurazione. Per ulteriori informazioni consultare la Guida.

11.7 Evolution per gli utenti di GroupWise

Gli utenti di GroupWise non dovrebbero incontrare difficoltà nell'utilizzo di Evolution per accedere agli account di GroupWise. Evolution e GroupWise infatti utilizzano una terminologia molto simile. Gli utenti che hanno familiarità con uno dei due sistemi dovrebbero essere in grado di apprendere l'altro con uno sforzo minimo.

11.7.1 Configurazione di Evolution per l'accesso al sistema GroupWise

Utilizzare Evolution Mail Configuration Assistant (Assistente di configurazione posta di Evolution) per configurare Evolution per l'accesso al sistema GroupWise. Per avviare Evolution Mail Configuration Assistant (Assistente di configurazione posta di Evolution), fare clic su *Preferences (Preferenze)* → *Mail Accounts (Account posta)* → *Add (Aggiungi)* e quindi fare clic su *Forward (Avanti)*.

Nella pagina Identity (Identità), fornire il proprio indirizzo di e-mail nel sistema GroupWise (ad esempio, mario@esempio.com), quindi fare clic su *Forward (Avanti)*.

Nella pagina Receiving Email (Ricezione messaggio e-mail in corso), selezionare *IMAP (IMAP)* nell'elenco Server Type (Tipo di server), specificare il nome host del server GroupWise utilizzato nel campo Host (Host), impostare le altre opzioni nella pagina Receiving Options (Opzioni di ricezione) nel modo più appropriato per il sistema utilizzato, quindi fare clic su *Forward (Avanti)*.

Nella pagina Sending Email (Invio di messaggi e-mail in corso), selezionare *SMTP (SMTP)* nell'elenco Server Type (Tipo di server), specificare il nome host del server GroupWise utilizzato nel campo Host (Host), impostare le altre opzioni di invio di e-mail nel modo più appropriato per il sistema utilizzato, quindi fare clic su *Forward (Avanti)*.

Nella pagina Account Management (Gestione account), specificare il nome che si desidera utilizzare per identificare questo account nella pagina Evolution Settings (Impostazioni di Evolution), quindi fare clic su *Forward (Avanti)*.

Fare clic su *Apply (Applica)* per creare un account di GroupWise. La casella postale di GroupWise viene ora visualizzata nell'elenco degli account e-mail disponibili.

11.8 Ulteriori informazioni

Evolution dispone di una Guida interna completa. Utilizzare il menu *Help (Guida)* per accedere a queste informazioni. Per ulteriori informazioni su Evolution, visitare il sito Web del progetto all'indirizzo `http://www.gnome.org/projects/evolution/` (in lingua inglese).

Kontact: programma per e-mail e calendario

12

Kontact offre un'unica pratica interfaccia per la gestione di informazioni personali nella quale vengono riunite le funzionalità di varie applicazioni KDE, tra cui KMail per i messaggi e-mail, KOrganizer per il calendario, KAddressbook per i contatti e KNotes per le annotazioni. È inoltre possibile sincronizzare dati con dispositivi esterni, quali PalmPilot o altri palmari. Kontact si integra facilmente con il resto del desktop KDE e si connette a numerosi server groupware. Sono disponibili funzionalità supplementari, ad esempio il filtraggio di posta indesiderata e virus e un lettore RSS.

Per avviare Kontact, utilizzare il menu principale e selezionare *Office (Ufficio)* → *Kontact (Personal Information Manager)*. In alternativa, immettere `kontact` nella riga di comando. Se è necessario utilizzare solo alcune funzionalità, è anche possibile aprire i singoli componenti anziché l'applicazione combinata.

12.1 Importazione di messaggi e-mail da altri programmi di posta

Per importare messaggi e-mail da altre applicazioni, selezionare *Tools (Strumenti)* → *Import Messages (Importa messaggi)* dalla vista della posta in Kontact. Attualmente sono disponibili filtri di importazione per Outlook Express, il formato mbox, il formato di testo dei messaggi e-mail, Pegasus Mail, Opera, Evolution e altri ancora. L'utility di importazione può essere avviata anche separatamente con il comando `kmailcvt`.

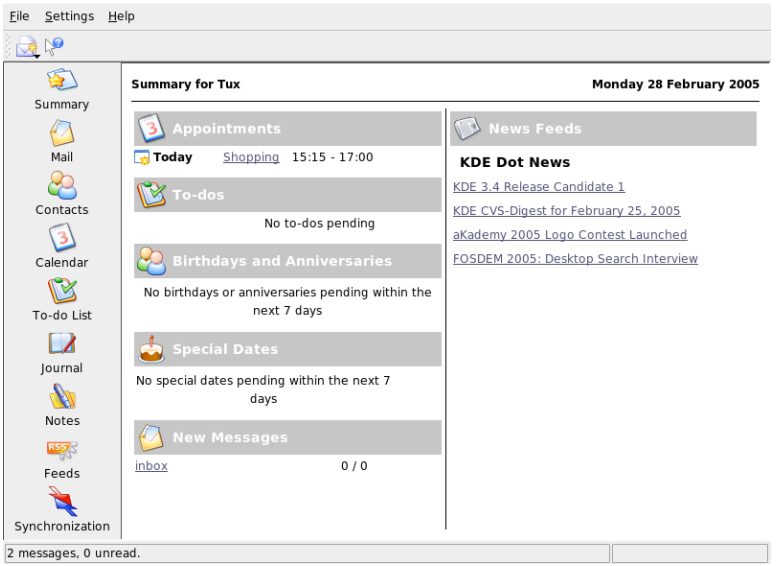
Selezionare l'applicazione corrispondente e confermare facendo clic su *Continue (Continua)*. In base al tipo selezionato, è necessario specificare un file o una cartella. Il processo verrà completato automaticamente da Kontact.

12.2 Panoramica di Kontact

La vista di default della finestra, *Summary (Riepilogo)*, è illustrata nella Figura 12.1, «Finestra di Kontact contenente il riepilogo» (p. 186). Utilizzare i pulsanti nella sezione di sinistra per accedere ai vari componenti.

Nella finestra *Summary (Riepilogo)* sono disponibili informazioni di base, tra cui i compleanni che ricorreranno nei giorni immediatamente successivi, le attività da completare, le condizioni meteorologiche e lo stato di KPilot. La sezione delle news consente di accedere a feed RSS per ottenere notizie aggiornate su argomenti di proprio interesse. Utilizzare *Settings (Impostazioni)* → *Configure Summary View (Configura vista riepilogo)* per configurare le informazioni da visualizzare.

Figura 12.1 *Finestra di Kontact contenente il riepilogo*



12.2.1 Posta

L'area cartelle visualizzata a sinistra contiene un elenco delle cartelle principali (caselle postali) in cui è indicato il numero totale di messaggi e il numero di messaggi ancora non letti. Per selezionare una cartella, è sufficiente fare clic su di essa. I messaggi contenuti in tale cartella vengono visualizzati nel riquadro in alto a destra. Sulla barra di stato nella parte inferiore della finestra dell'applicazione è inoltre indicato il numero di messaggi presenti nella cartella.

Nell'area di intestazione visualizzata a destra vengono indicati l'oggetto, il mittente e l'ora di ricezione. È sufficiente fare clic sui messaggi per selezionarli e visualizzarli nell'apposita finestra. Per ordinare i messaggi, è possibile fare clic su una delle colonne (oggetto, mittente, data e così via). Il contenuto del messaggio selezionato viene visualizzato nell'apposito riquadro della finestra. Gli allegati sono rappresentati da icone riportate alla fine del messaggio, che variano in base al tipo MIME dell'allegato, oppure possono essere visualizzati in linea.

I messaggi possono essere contrassegnati con diversi flag di stato. Per modificare lo stato, selezionare *Message (Messaggio)* → *Mark Message (Contrassegna messaggio)*. È possibile utilizzare questa funzionalità per assegnare uno stato a un messaggio, ad esempio per contrassegnare un messaggio importante da non dimenticare oppure un messaggio che può essere ignorato. Per visualizzare solo i messaggi con un determinato stato, utilizzare *Status (Stato)* sulla barra di ricerca.

12.2.2 Contatti

Nel riquadro in alto a sinistra di questo componente sono riportati tutti gli indirizzi presenti nella rubrica attivata. Nel riquadro in basso a sinistra sono elencate le rubriche disponibili ed è indicato se sono attivate. Nel riquadro a destra è visualizzato il contatto selezionato. Per trovare un particolare contatto, utilizzare la barra di ricerca nella parte superiore.

12.2.3 Elenco delle attività

In *To-do List (Elenco attività)* è riportato l'elenco delle attività. Fare clic sul campo nella parte superiore per aggiungere un nuovo elemento all'elenco. Fare clic con il pulsante destro del mouse in una colonna di un elemento esistente per apportare

modifiche al valore di tale colonna. Un elemento può essere suddiviso in più elementi secondari. Fare clic con il pulsante destro del mouse e selezionare *New Sub-to-do (Nuova attività secondaria)* per creare un elemento secondario. È inoltre possibile assegnare attività ad altri.

12.2.4 Calendario

La vista del calendario è suddivisa in vari riquadri. Per default, vengono visualizzati un piccolo calendario del mese corrente e una vista della settimana corrente. Sono inoltre disponibili un elenco delle attività, una vista dettagliata dell'evento o dell'attività corrente e un elenco dei calendari con il relativo stato. Per selezionare una vista diversa, utilizzare la barra degli strumenti oppure il menu *View (Visualizza)*.

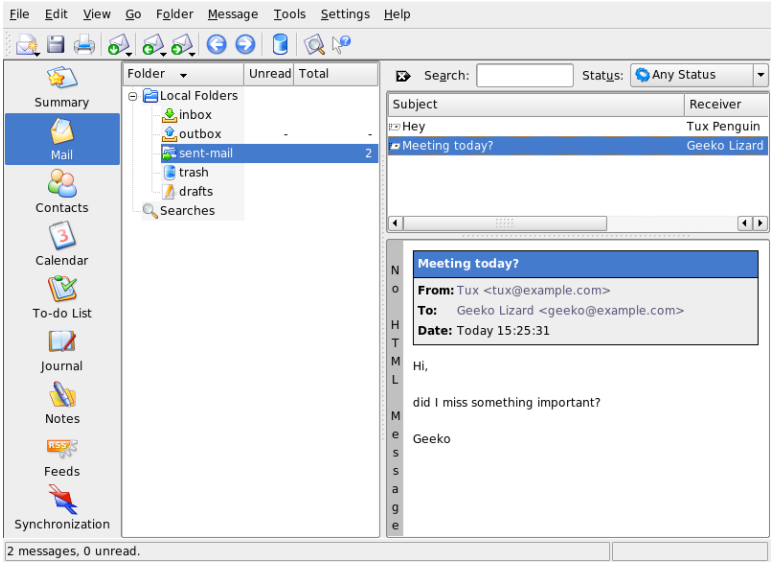
12.2.5 Annotazioni

Utilizzare il componente per le annotazioni per creare annotazioni personali. Se si utilizza KDE, scegliere l'icona KNote sulla barra delle applicazioni per visualizzare le annotazioni sul desktop.

12.3 Posta

Kontact utilizza KMail come componente per i messaggi e-mail. Per configurarlo, aprire il componente per la posta, quindi selezionare *Settings (Impostazioni) → Configure KMail (Configura KMail)*. KMail è un client completo per i messaggi e-mail che supporta vari protocolli. Nel menu *Tools (Strumenti)* sono disponibili vari strumenti che consentono di gestire i messaggi e-mail indesiderati. Utilizzare *Find (Trova)* per eseguire una ricerca dettagliata dei messaggi. *Anti-Spam Wizard (Configurazione guidata posta indesiderata)* consente di configurare in modo semplificato gli strumenti per filtrare i messaggi e-mail commerciali indesiderati. *Anti-Virus Wizard (Configurazione guidata strumenti anti-virus)* consente di configurare in modo semplificato gli strumenti anti-virus per i messaggi e-mail. Queste due procedure guidate possono essere utilizzate con prodotti software anti-virus e per la posta indesiderata esterni. Se queste opzioni sono disabilitate, installare pacchetti aggiuntivi per garantire una protezione contro posta indesiderata e virus.

Figura 12.2 *Componente di Kontact per la posta*



12.3.1 Configurazione degli account

Kontact è in grado di gestire più account e-mail, ad esempio l'indirizzo e-mail privato e quello dell'ufficio. Quando si scrive un messaggio e-mail, selezionare una delle identità definite in precedenza facendo clic su *View (Visualizza)* → *Identity (Identità)*. Per creare un nuovo profilo di identità, selezionare *Settings (Impostazioni)* → *Configure KMail (Configura KMail)*, quindi *Identities (Identità)* → *New (Nuova)*. Nella finestra di dialogo visualizzata assegnare un nome alla nuova identità, ad esempio «privata» o «ufficio». Fare clic su *OK* per visualizzare una finestra di dialogo in cui è possibile immettere informazioni aggiuntive. È inoltre possibile assegnare un'identità a una cartella affinché, quando si risponde a un messaggio in tale cartella, venga selezionata l'identità assegnata.

Nella scheda *General (Generale)* immettere il proprio nome, l'organizzazione e l'indirizzo e-mail. In *Cryptography (Cifratura)* selezionare le chiavi per l'invio di messaggi cifrati o con firma digitale. Per poter utilizzare le funzionalità di cifratura, è prima necessario creare una chiave con KGpg, come descritto nel Capitolo 6, *Cifratura con KGpg* (p. 107).

In *Advanced (Avanzate)* è possibile immettere un indirizzo di risposta e un indirizzo ccn (copia per conoscenza nascosta), scegliere un dizionario, selezionare le cartelle per le bozze e i messaggi inviati e definire la modalità di invio dei messaggi. In *Signature (Firma)* specificare se e come si desidera firmare ogni messaggio aggiungendo un blocco di testo supplementare alla fine. Ad esempio, si potrebbe firmare ogni messaggio e-mail specificando le proprie informazioni di contatto. Per attivare questa opzione, selezionare *Enable Signature (Abilita firma)* e scegliere se si desidera ottenere la firma da un file, da un campo di input oppure dall'output di un comando. Dopo avere configurato tutte le impostazioni dell'identità desiderate, confermarle facendo clic su *OK*.

Le impostazioni in *Network (Rete)* stabiliscono la modalità di invio e ricezione dei messaggi e-mail in Kontact. Sono disponibili due schede, una per l'invio e l'altra per la ricezione della posta. Molte delle impostazioni variano in base al sistema e alla rete in cui si trova il server della posta. Se non si è sicuri delle impostazioni o degli elementi da selezionare, consultare il proprio ISP (Provider di servizi Internet) o l'amministratore di sistema.

Per creare caselle postali per la posta in uscita, nella scheda *Sending (Invio)* fare clic su *Add (Aggiungi)*. Scegliere tra i tipi di trasporto SMTP e sendmail. Nella maggior parte dei casi la scelta corretta è SMTP. Al termine di questa selezione, viene visualizzata una finestra in cui è possibile immettere i dati del server SMTP. Specificare un nome e immettere l'indirizzo del server (ricevuto dall'ISP). Se il server richiede l'autenticazione dell'utente, selezionare *Server requires authentication (Il server richiede l'autenticazione)*. Le impostazioni di sicurezza sono incluse nella scheda *Sicurezza*. In questa scheda, è possibile specificare il metodo di cifratura preferito.

Nella scheda *Ricezione*, è possibile definire le impostazioni per la ricezione dei messaggi di e-mail. Si può utilizzare *Aggiungi* per creare un nuovo account. Scegliere tra i diversi metodi di recupero della posta, ad esempio i formati Mbox e Maildir locali oppure POP3 o IMAP. Configurare le impostazioni appropriate in base al server in uso.

12.3.2 Creazione di messaggi

Per creare nuovi messaggi, selezionare *Message (Messaggio)* → *New Message (Nuovo messaggio)* oppure fare clic sull'icona corrispondente sulla barra degli strumenti. Per inviare i messaggi utilizzando account e-mail diversi, selezionare un'identità come descritto nella Sezione 12.3.1, «Configurazione degli account» (p. 189). In *To (A)* immettere un indirizzo e-mail oppure parte di un nome o un indirizzo presente nella

rubrica. Se Kontact è in grado di associare le informazioni specificate alle informazioni presenti nella rubrica, viene visualizzato un elenco di selezione. Fare clic sul contatto desiderato oppure completare l'input se non viene rilevata alcuna corrispondenza. Per selezionare direttamente il destinatario dalla rubrica, fare clic sul pulsante ... accanto al campo Address (Indirizzo).

Per allegare file al messaggio, fare clic sull'icona a forma di graffetta e selezionare il file da allegare. In alternativa, trascinare un file dal desktop o da un'altra cartella nella finestra *Nuovo messaggio* o selezionare una delle opzioni nel menu *Allega*. In genere, il formato di un file viene riconosciuto correttamente. In caso contrario, fare clic con il pulsante destro del mouse sull'icona. Selezionare *Properties (Proprietà)* dal menu visualizzato. Impostare il formato e il nome di file nella finestra di dialogo successiva e aggiungere una descrizione. Specificare inoltre se il file allegato deve essere firmato o cifrato.

Dopo avere creato il messaggio, è possibile inviarlo immediatamente selezionando *Message (Messaggio)* → *Send (Invia)* oppure spostarlo nella cartella outbox selezionando *Message (Messaggio)* → *Queue (Coda)*. Se si sceglie di inviare il messaggio e-mail e l'invio ha esito positivo, il messaggio viene copiato nella cartella `sent-mail`. I messaggi spostati nella cartella `outbox` possono essere modificati o cancellati.

12.3.3 Messaggi e-mail cifrati e firme

Per cifrare un messaggio e-mail, generare innanzitutto una coppia di chiavi come descritto nel Capitolo 6, *Cifratura con KGpg* (p. 107). Per configurare i dettagli della procedura di cifratura, selezionare *Settings (Impostazioni)* → *Configure KMail (Configura KMail)* → *Identities (Identità)* per specificare l'identità da utilizzare per inviare messaggi cifrati e con firma. Fare quindi clic su *Modify (Modifica)*. Quando si fa clic su *OK* per confermare l'operazione, la chiave dovrebbe venire visualizzata nel campo corrispondente. Chiudere la finestra di dialogo di configurazione facendo clic su *OK*.

12.3.4 Cartelle

Le cartelle dei messaggi consentono di organizzare i messaggi e-mail. Per default, si trovano nella directory `~/.kde/share/apps/kmail/mail`. Quando si avvia KMail per la prima volta, vengono create varie cartelle. `inbox` è la cartella in cui vengono inseriti inizialmente i nuovi messaggi recuperati da un server. `outbox` è la

cartella in cui vengono memorizzati temporaneamente i messaggi inseriti in coda per l'invio. `sent-mail` è la cartella in cui vengono conservate le copie dei messaggi inviati. `trash` è la cartella contenente le copie di tutti i messaggi e-mail cancellati con il tasto Canc oppure selezionando *Edit (Modifica)* → *Delete (Cancella)*. `drafts` è la cartella in cui vengono salvati i messaggi non ultimati. Se si utilizza IMAP, le cartelle IMAP sono elencate sotto quelle locali. L'elenco Folder (Cartella) contiene cartelle specifiche per ogni server di posta in entrata, ad esempio locale o IMAP.

Se si desidera organizzare i messaggi in cartelle aggiuntive, creare le nuove cartelle selezionando *Folder (Cartella)* → *New Folder (Nuova cartella)*. Viene visualizzata una finestra in cui è possibile specificare il nome e il formato della nuova cartella.

Fare clic con il pulsante destro del mouse sulla cartella per visualizzare un menu contestuale che consente di eseguire diverse operazioni sulle cartelle. Fare clic su *Expire (Scadenza)* per specificare la data di scadenza dei messaggi letti e non letti, l'operazione da eseguire dopo la scadenza e se i messaggi scaduti devono essere cancellati o spostati in una cartella. Se si desidera utilizzare la cartella per memorizzare i messaggi ricevuti da una mailing list, impostare le opzioni necessarie in *Folder (Cartella)* → *Mailing List Management (Gestione mailing list)*.

Per spostare uno o più messaggi da una cartella all'altra, evidenziarli e quindi premere M oppure selezionare *Message (Messaggio)* → *Move to (Sposta in)*. Verrà visualizzato un elenco nel quale è possibile selezionare la cartella in cui si desidera spostare i messaggi. Per spostare i messaggi, è inoltre possibile trascinarli dalla finestra superiore nella cartella appropriata della finestra di sinistra.

12.3.5 Filtri

I filtri rappresentano un utile strumento per elaborare automaticamente i messaggi e-mail in entrata. Possono essere utilizzati per spostare messaggi e-mail in determinate cartelle, cancellare messaggi e-mail indesiderati, rinviare messaggi e-mail al mittente o eseguire varie altre operazioni in base a particolari caratteristiche del messaggio, ad esempio il mittente o la dimensione.

Impostazione di un filtro

Per creare un filtro da zero, selezionare *Settings (Impostazioni)* → *Configure Filters (Configura filtri)*. Per creare un filtro in base a un messaggio esistente, selezionare il

messaggio desiderato nell'elenco Header (Intestazione), quindi selezionare *Tools (Strumenti) → Create Filter (Crea filtro)* e specificare i criteri di filtro desiderati.

Selezionare il metodo di corrispondenza desiderato per i criteri di filtro, ovvero specificare se è necessario che vengano soddisfatti tutti i criteri oppure solo uno di essi. Selezionare quindi i criteri applicabili solo ai messaggi desiderati. In *Filter Actions (Azioni filtro)* impostare le azioni che il filtro deve eseguire sui messaggi che soddisfano i criteri. *Advanced Options (Opzioni avanzate)* consente di controllare quando il filtro viene applicato e se è necessario considerare filtri aggiuntivi per questi messaggi.

Applicazione di filtri

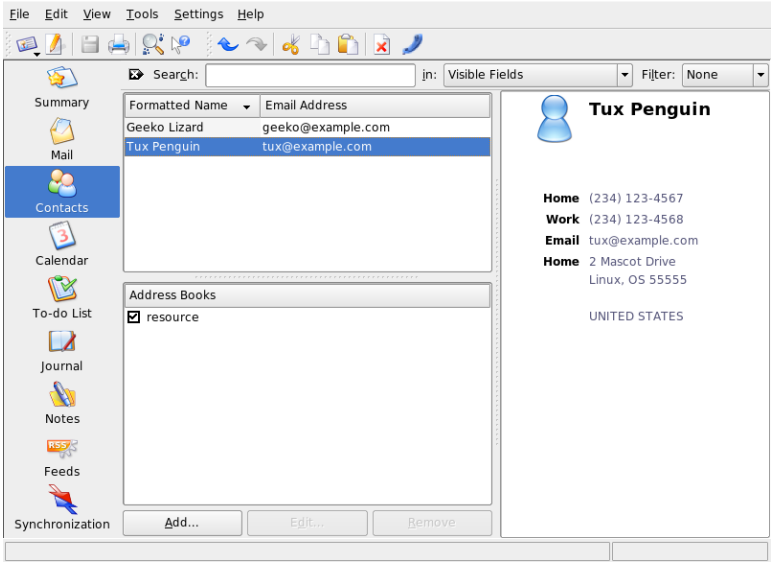
I filtri vengono applicati nell'ordine specificato nella finestra di dialogo a cui si accede selezionando *Settings (Impostazioni) → Configure Filters (Configura filtri)*. Per cambiare l'ordine, selezionare un filtro e fare clic sui pulsanti freccia. I filtri vengono applicati solo ai nuovi messaggi in entrata o ai messaggi inviati, in base alle impostazioni configurate nelle opzioni avanzate del filtro. Per applicare filtri a messaggi esistenti, selezionare i messaggi desiderati, quindi utilizzare *Message (Messaggio) → Apply Filters (Applica filtri)*.

Se i filtri non vengono applicati come previsto, selezionare *Tools (Strumenti) → Filter Log Viewer (Visualizzatore log filtri)* per controllare le modalità di applicazione. Quando la registrazione è abilitata in questa finestra di dialogo, vengono visualizzate le modalità in base a cui i filtri elaborano i messaggi per semplificare l'individuazione del problema.

12.4 Contatti

Il componente per i contatti utilizza KAddressBook. Per configurarlo, selezionare *Settings (Impostazioni) → Configure KAddressBook (Configura KAddressBook)*. Per cercare un particolare contatto, utilizzare la barra di ricerca. *Filter (Filtro)* consente di visualizzare solo i contatti di una determinata categoria. Fare clic con il pulsante destro del mouse su un contatto per visualizzare un menu in cui è possibile selezionare diverse opzioni, ad esempio per inviare le informazioni di contatto in un messaggio e-mail.

Figura 12.3 *Rubrica di Kontact*



12.4.1 Aggiunta di contatti

Per aggiungere nella rubrica un contatto con nome e indirizzo e-mail dall'interno di un messaggio e-mail, fare clic con il pulsante destro del mouse sull'indirizzo nel componente per la posta e selezionare *Open in Address Book (Apri nella rubrica)*. Per aggiungere un nuovo contatto senza utilizzare un messaggio e-mail, selezionare *File → New Contact (Nuovo contatto)* nel componente per la rubrica. Entrambe queste procedure consentono di visualizzare una finestra di dialogo in cui è possibile immettere informazioni sul contatto.

Nella scheda *General (Generale)* immettere le informazioni di base sul contatto, ad esempio il nome, gli indirizzi e-mail e i numeri di telefono. Per ordinare gli indirizzi è possibile utilizzare le categorie. *Details (Dettagli)* contiene informazioni più specifiche, ad esempio la data di compleanno e il nome del coniuge.

Se il contatto utilizza un servizio di messaggistica in tempo reale, è possibile aggiungere queste identità in *IM Addresses (Indirizzi messaggistica in tempo reale)*. Se si effettua questa operazione e viene eseguito Kopete o un altro programma di chat KDE contemporaneamente a Kontact, è possibile visualizzare le informazioni di stato su

queste identità in Kontact. In *Crypto Settings (Impostazioni cifratura)* immettere i dati relativi alla cifratura del contatto, ad esempio la chiave pubblica.

Misc (Varie) contiene ulteriori informazioni, ad esempio una fotografia e la posizione delle informazioni Free/Busy (Disponibilità) dell'utente. Utilizzare *Custom Fields (Campi personalizzati)* per aggiungere informazioni personalizzate al contatto o alla rubrica.

I contatti possono inoltre essere importati in numerosi formati. Utilizzare *File → Import (Importa)*, scegliere il formato desiderato, quindi selezionare il file da importare.

12.4.2 Creazione di una lista di distribuzione

Se si inviano spesso messaggi e-mail a uno stesso gruppo di persone, una lista di distribuzione consente di memorizzare più indirizzi e-mail come un singolo contatto, in modo da non dovere immettere tutti i nomi in ogni messaggio e-mail inviato a tale gruppo. Fare innanzitutto clic su *Settings (Impostazioni) → Show Extension Bar (Mostra barra estensioni) → Distribution List Editor (Editor lista di distribuzione)*. Nella nuova sezione visualizzata fare clic su *New List (Nuova lista)*. Immettere un nome per la lista e quindi fare clic su *OK*. Aggiungere contatti alla lista trascinandoli dall'elenco degli indirizzi nella finestra della lista di distribuzione. Quando si crea un messaggio e-mail, è possibile utilizzare questa lista come un normale contatto.

12.4.3 Aggiunta di rubriche

IMPORTANTE: rubriche groupware

Il modo migliore per aggiungere risorse groupware consiste nell'utilizzare uno strumento separato denominato Groupware Wizard (Configurazione guidata groupware). A tale scopo, chiudere Kontact, quindi eseguire `groupwarewizard` in una riga di comando o dal gruppo Office (Ufficio) del menu KDE. Selezionare il tipo di server, ad esempio SLOX, GroupWise o Exchange, dall'elenco visualizzato, quindi immettere l'indirizzo e i dati per l'autenticazione. La procedura guidata aggiungerà le risorse disponibili a Kontact.

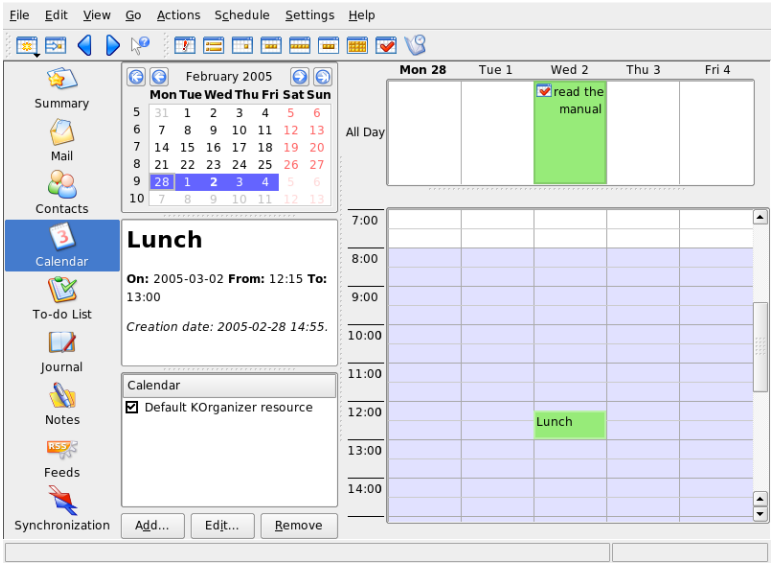
Kontact consente di accedere a più rubriche, ad esempio quelle condivise da Novell GroupWise o in un server LDAP. Selezionare *Settings (Impostazioni)* → *Show Extension Bar (Mostra barra estensioni)* → *Address Books (Rubriche)* per visualizzare le rubriche correnti. Fare clic su *Add (Aggiungi)* per aggiungerne una, quindi selezionare il tipo e immettere le informazioni richieste.

Le caselle di controllo accanto alle rubriche indicano lo stato di attivazione di ognuna di esse. Per impedire che una rubrica venga visualizzata senza però cancellarla, deselezionare la casella di controllo. *Remove (Rimuovi)* cancella la rubrica selezionata dall'elenco.

12.5 Calendario

Kontact utilizza KOrganizer come componente per il calendario. Per configurarlo, utilizzare *Settings (Impostazioni)* → *Configure KOrganizer (Configura KOrganizer)*. Nel calendario è possibile immettere appuntamenti e pianificare riunioni. Se lo si desidera, è possibile impostare un promemoria per gli eventi imminenti. È inoltre possibile importare, esportare e archiviare calendari utilizzando le opzioni del menu *File*.

Figura 12.4 *Calendario di Kontact*



12.5.1 Pianificazione di un evento

Per aggiungere un nuovo evento o una nuova riunione, selezionare *Actions (Azioni)* → *New Event (Nuovo evento)*. Immettere i dettagli desiderati. In *Reminder (Promemoria)* specificare il momento esatto (numero di minuti, ore o giorni in anticipo) in cui si desidera ricordare l'evento ai partecipanti. Se un evento è ricorrente, specificare l'intervallo appropriato. Un altro modo per creare un evento in un punto specifico del calendario consiste nel fare doppio clic sul campo corrispondente in una delle viste del calendario del programma. Viene visualizzata la stessa finestra di dialogo accessibile dal menu. In alternativa, selezionare un intervallo di tempo nella vista del calendario e fare clic con il pulsante destro del mouse.

Specificare i partecipanti a un evento immettendo i relativi dati manualmente nella finestra di dialogo oppure inserendo i dati dalla rubrica. Per immettere i dati manualmente, selezionare *New (Nuovo)*. Per importare i dati dalla rubrica, fare clic su *Select Addressee (Seleziona destinatario)*, quindi selezionare le voci corrispondenti nella finestra di dialogo. Per pianificare l'evento in base alla disponibilità dei partecipanti, utilizzare *Free/Busy (Disponibilità)* e fare clic su *Pick Date (Seleziona data)*.

Utilizzare la scheda *Recurrence (Ricorrenza)* per configurare un evento che si verifica periodicamente. *Attachments (Allegati)* può essere utile per collegare altre informazioni all'evento, ad esempio l'agenda per una riunione.

12.5.2 Aggiunta di calendari

IMPORTANTE: calendari groupware

Il modo migliore per aggiungere risorse groupware consiste nell'utilizzare uno strumento separato denominato Groupware Wizard (Configurazione guidata groupware). A tale scopo, chiudere Kontact, quindi eseguire `groupwarewizard` in una riga di comando o dal gruppo Office (Ufficio) del menu KDE. Selezionare il tipo di server, ad esempio SLOX, GroupWise o Exchange, dall'elenco visualizzato, quindi immettere l'indirizzo e i dati per l'autenticazione. La procedura guidata aggiungerà le risorse disponibili a Kontact.

Il modulo del calendario può connettersi contemporaneamente a più calendari. Questa funzionalità risulta utile, ad esempio, per utilizzare un calendario personale in combinazione con un calendario organizzativo. Per aggiungere un nuovo calendario,

fare clic su *Add (Aggiungi)*, quindi selezionare il tipo di calendario. Completare i campi necessari.

Le caselle di controllo accanto ai calendari indicano lo stato di attivazione di ognuno di essi. Per impedire che un calendario venga visualizzato senza però cancellarlo, deselezionare la casella di controllo. *Remove (Rimuovi)* cancella il calendario selezionato dall'elenco.

12.6 Sincronizzazione di dati con un palmare

Kontact è stato progettato in modo da supportare la sincronizzazione dei dati con dispositivi palmari, ad esempio Palm. È possibile visualizzare le informazioni sullo stato di KPilot nel riepilogo. Per informazioni sulla configurazione e sull'uso di KPilot, fare riferimento al Capitolo 13, *Sincronizzazione di un palmare con KPilot* (p. 201).

12.7 Informazioni su Kontact per gli utenti di GroupWise

Gli utenti che conoscono già GroupWise non avranno difficoltà a utilizzare Kontact. Questi due programmi condividono molti concetti di base e offrono un gran numero di servizi comuni a entrambi. In questa sezione vengono illustrate le differenze terminologiche più importanti e vengono forniti alcuni suggerimenti per consentire agli utenti di GroupWise di sfruttare al meglio le funzionalità di Kontact.

12.7.1 Differenze terminologiche

Nella seguente tabella vengono elencate alcune delle principali differenze terminologiche esistenti tra Kontact e GroupWise.

Tabella 12.1 *Differenze terminologiche tra Kontact e GroupWise*

GroupWise	Kontact
Appuntamenti	Events (Eventi)
Ricerca ore libere	Free/Busy (Disponibilità)
Annotazioni	Journal Entries (Voci del journal)
Elementi pubblicati, non pubblicati	Un evento senza partecipanti è pubblicato, un evento con partecipanti è un elemento inviato
Task	To-dos (Attività)

12.7.2 Suggerimenti per gli utenti di GroupWise

In questa sezione viene fornito qualche suggerimento per consentire agli utenti di GroupWise di familiarizzare con alcune delle differenze esistenti tra GroupWise e Kontact.

Informazioni di contatto

È possibile aggiungere il proprio GroupWise Messenger e i contatti e-mail alle informazioni di contatto di Kontact. È quindi possibile creare un messaggio e-mail oppure aprire una sessione di messaggistica in tempo reale con tale contatto facendo clic con il pulsante destro del mouse sul nome nella vista del contatto.

Codifica a colori

Può essere utile contrassegnare con un colore gli elementi sia di GroupWise sia provenienti da altre origini. La codifica a colori semplifica la scansione dei messaggi e-mail, dei contatti e di altre informazioni per gli elementi di una particolare origine.

Invito alla partecipazione di un evento

Kontact si differenzia da GroupWise in quanto il nome dell'utente che ha pianificato un evento non viene immesso automaticamente come partecipante. Ricordarsi pertanto di inviare un invito anche a se stessi.

12.8 Ulteriori informazioni

In Kontact è disponibile una guida contenente informazioni sia su questo programma che sui relativi componenti. Per accedervi, selezionare *Help (Guida)* → *Kontact Handbook (Manuale Kontact)*. Informazioni sul programma sono inoltre disponibili nella pagina Web del progetto all'indirizzo `http://www.kontact.org`.

Sincronizzazione di un palmare con KPilot

13

I palmari sono molto diffusi tra gli utenti che devono avere sempre a portata di mano pianificazioni, elenchi delle attività e annotazioni ovunque essi vadano. Spesso questi utenti hanno necessità di utilizzare gli stessi dati sia sul desktop che sul portatile. A tale scopo, è possibile ricorrere a KPilot, uno strumento che consente di sincronizzare i dati di un palmare con quelli utilizzati dalle applicazioni KDE KAddressBook, KOrganizer e KNotes, tutte facenti parte di Kontact.

Scopo principale di KPilot è consentire la condivisione di dati tra le applicazioni di un palmare e le applicazioni KDE corrispondenti. In KPilot sono incorporati un visualizzatore di promemoria, un visualizzatore degli indirizzi e un programma di installazione dei file, che non possono però essere utilizzati al di fuori dell'ambiente di KPilot. Per tutte queste funzioni, tranne il programma di installazione dei file, sono disponibili applicazioni KDE indipendenti.

Per le comunicazioni tra il palmare e i vari programmi desktop, KPilot si affida a conduit. KPilot è il programma che controlla lo scambio di dati tra i due computer. Per utilizzare sul desktop una particolare funzione del palmare è necessario abilitare e configurare il conduit corrispondente. Nella maggior parte dei casi, questi conduit sono progettati in modo da interagire con programmi KDE specifici, pertanto in genere non è possibile utilizzarli con altre applicazioni desktop.

Il conduit della sincronizzazione dell'orario si differenzia dagli altri in quanto non esiste un programma visibile all'utente. Viene attivato in background a ogni operazione di sincronizzazione, ma deve essere abilitato solo sui computer che utilizzano un server dell'orario di rete per correggere gli scostamenti.

All'avvio di una sincronizzazione, i conduit vengono attivati uno dopo l'altro per eseguire il trasferimento dei dati. Esistono due diversi metodi di sincronizzazione: un'operazione HotSync sincronizza solo i dati per i quali sono stati abilitati dei conduit, mentre un'operazione di backup esegue il backup completo di tutti i dati memorizzati nel palmare.

Alcuni conduit aprono un file durante la sincronizzazione, pertanto il programma corrispondente non deve essere in esecuzione in questa fase. In particolare, non eseguire KOrganizer durante un'operazione di sincronizzazione.

13.1 Conduit utilizzati da KPilot

Per abilitare e configurare i conduit utilizzati da KPilot, selezionare *Settings (Impostazioni)* → *Configure KPilot (Configura KPilot)*. Di seguito è riportato un elenco con alcuni conduit importanti:

Rubrica
Questo conduit gestisce lo scambio di dati con la rubrica del palmare. L'applicazione KDE corrispondente per la gestione di questi contatti è KAddressBook. Per avviarla, utilizzare il menu principale o il comando `kaddressbook`.

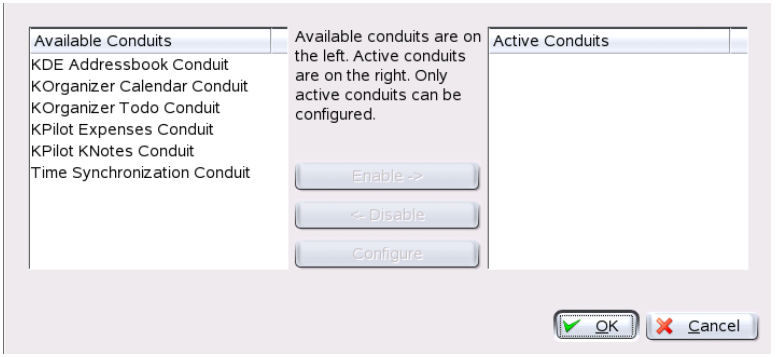
KNotes/Memos (KNotes/Promemoria)
Questo conduit consente di trasferire le annotazioni create con KNotes nell'applicazione per i promemoria del palmare. Per avviare l'applicazione KDE, utilizzare il menu principale o il comando `knotes`.

Calendar (Calendario - KOrganizer)
Questo conduit è preposto alla sincronizzazione degli appuntamenti (eventi) del palmare. L'applicazione corrispondente nel desktop è KOrganizer.

ToDos (Attività - KOrganizer)
Questo conduit è preposto alla sincronizzazione delle attività. L'applicazione corrispondente nel desktop è KOrganizer.

Time Synchronization Conduit (Conduit di sincronizzazione dell'orario)
L'abilitazione di questo conduit consente di regolare l'orologio del palmare con quello del desktop durante ogni operazione di sincronizzazione. Questa scelta è consigliata solo se l'orologio del desktop viene regolato da un server dell'orario a intervalli abbastanza frequenti.

Figura 13.1 *Finestra di dialogo di configurazione con i conduit disponibili*



13.2 Configurazione della connessione del palmare

Per poter utilizzare KPilot, impostare innanzitutto la connessione con il palmare. La configurazione dipende dal tipo di unità di alloggiamento utilizzato con il palmare. Ne esistono di due tipi: alloggiamenti o cavi USB e alloggiamenti o cavi seriali.

13.2.1 Configurazione della connessione da KPilot

Il modo più facile per impostare la connessione consiste nell'utilizzare l'apposito assistente. Selezionare *Settings (Impostazioni)* → *Configuration Assistant (Assistente configurazione)* per avviare l'assistente. Immettere innanzitutto il proprio nome utente e il nome del dispositivo al quale è connesso il palmare. L'assistente tenta di rilevare questi dati automaticamente se si seleziona *Autodetect Handheld (Rilevamento automatico palmare)& Username (Nome utente)*. Se il rilevamento automatico non riesce, fare riferimento alla Sezione 13.2.2, «Creazione di un collegamento /dev/pilot» (p. 204).

Dopo che l'utente ha fatto clic su *Next (Avanti)* per confermare questi dati, l'assistente chiede di specificare le applicazioni da utilizzare per la sincronizzazione. È possibile scegliere tra la suite di applicazioni KDE (impostazione di default), Evolution e nessuna

applicazione. Dopo avere selezionato l'opzione desiderata, chiudere la finestra facendo clic su *Finish (Fine)*.

13.2.2 Creazione di un collegamento /dev/pilot

L'impostazione della connessione con un alloggiamento seriale per palmare è diversa da quella con un alloggiamento USB. La necessità di creare un collegamento simbolico denominato `/dev/pilot` dipende dall'alloggiamento utilizzato.

USB
: In genere, un alloggiamento USB viene rilevato automaticamente e non dovrebbe essere necessario creare il collegamento simbolico.

Seriale
: Nel caso di un alloggiamento seriale, è necessario sapere a quale porta seriale è connesso. Ai dispositivi seriali vengono assegnati nomi del tipo `/dev/ttyS?`, a partire da `/dev/ttyS0` per la prima porta. Per impostare un alloggiamento connesso alla prima porta seriale, immettere il seguente comando:

```
ln -s /dev/ttyS0 /dev/pilot
```

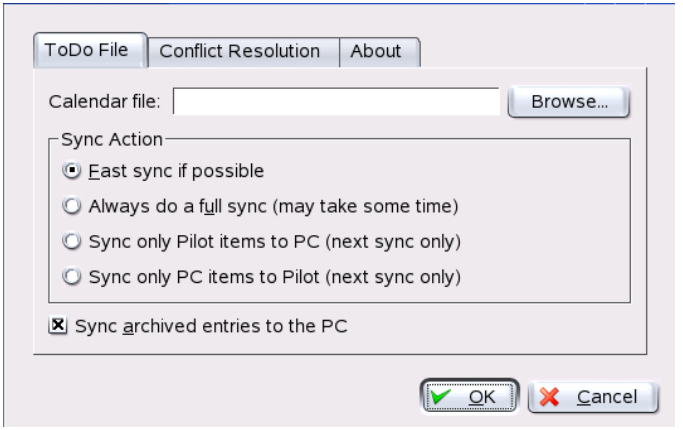
13.3 Configurazione del conduit KAddressBook

Inizialmente, dovrebbe essere sufficiente abilitare il conduit KAddressBook senza modificare le impostazioni di default. Dopo la prima sincronizzazione dei dati, configurare i seguenti dettagli: operazione da eseguire in caso di conflitti, modalità di salvataggio dei database di backup e modalità in base a cui determinati campi memorizzati nel palmare devono essere associati ai campi previsti da KAddressBook.

13.4 Gestione delle attività e degli eventi

Sul desktop KDE le attività (task) e gli eventi (appuntamenti) vengono gestiti tramite KOrganizer. Questa applicazione può essere avviata dal menu principale, tramite il comando `korganizer` o come componente di Kontact. Dopo avere abilitato i conduit del calendario e delle attività di KPilot, prima di utilizzarli è necessario impostare alcune opzioni di configurazione.

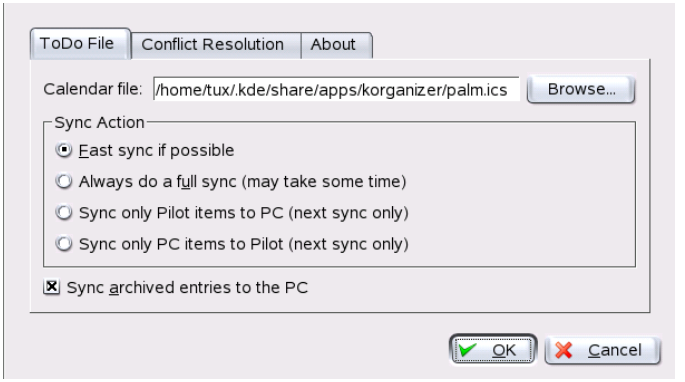
Figura 13.2 *Configurazione di KPilot*



KOrganizer memorizza i file nella directory `~/.kde/share/apps/korganizer`. Tuttavia, dato che la directory `.kde/` inizia con un punto, è possibile che non venga visualizzata nella finestra di dialogo per la selezione dei file. In tal caso, immettere il percorso completo manualmente o attivare esplicitamente la visualizzazione dei file nascosti (file dot) nella finestra di dialogo per la selezione dei file. Il tasto di scelta rapida di default è F8.

Dopo avere aperto la directory `~/.kde/share/apps/korganizer`, selezionare un file che possa essere utilizzato come file del calendario da KOrganizer. In questo esempio viene utilizzato il file `palm.ics`. Nel caso di un utente il cui nome è `tux`, il percorso completo e il nome di file saranno `/home/tux/.kde/share/apps/korganizer/palm.ics`, come illustrato nella Figura 13.3, «Finestra di dialogo in cui è indicato il percorso di un file del calendario di KOrganizer» (p. 206).

Figura 13.3 *Finestra di dialogo in cui è indicato il percorso di un file del calendario di KOrganizer*

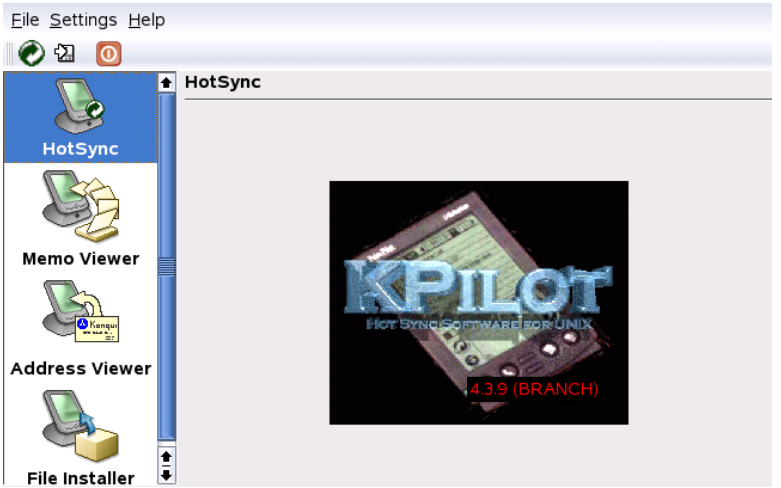


Durante lo scambio di dati con il palmare, KOrganizer non deve essere in esecuzione. In caso contrario, KPilot non riuscirà a portare a termine l'operazione di sincronizzazione.

13.5 Uso di KPilot

Sincronizzare i dati delle applicazioni KDE con quelli del palmare è molto semplice. È sufficiente avviare KPilot e quindi premere il pulsante HotSync sull'alloggiamento o sul cavo per avviare l'operazione di sincronizzazione.

Figura 13.4 *Finestra principale di KPilot*



13.5.1 Backup di dati dal palmare

Per eseguire un backup completo, selezionare *File → Backup*. Il backup verrà eseguito durante l'operazione di sincronizzazione successiva. Selezionare quindi *File → HotSync* dal menu. Se non si esegue questa operazione, durante l'operazione di sincronizzazione successiva verrà eseguito di nuovo tutto il lungo processo di backup completo.

Dopo un backup completo, tutte le copie dei programmi e dei database del palmare sono disponibili in `~/.kde/share/apps/kpilot/DBBackup/NOMEUTENTE`, dove *`NOMEUTENTE`* è il nome dell'utente registrato nel palmare.

I due visualizzatori incorporati di KPilot possono essere utilizzati per una ricerca rapida di indirizzi o promemoria, ma non sono stati progettati in modo da offrire funzionalità di gestione per questi dati. Per eseguire queste operazioni, è preferibile utilizzare le applicazioni KDE sopra indicate.

13.5.2 Installazione di programmi nel palmare

Il modulo *File Installer (Installazione file)* è un utile strumento per l'installazione dei programmi del palmare. Questi programmi in genere hanno l'estensione `prc` e possono essere avviati subito dopo il caricamento nel palmare. Prima di utilizzare questi programmi aggiuntivi, leggere le licenze e le istruzioni allegate.

13.5.3 Sincronizzazione di rubriche e calendari

Per sincronizzare i calendari e le rubriche, utilizzare lo strumento KDE MultiSynK. Per avviare questo strumento, utilizzare il comando `multisynk`. Creare una coppia di connettori prima di sincronizzare i dati. Selezionare *File → New (Nuovo)* e quindi i connettori desiderati. Chiudere la finestra facendo clic su *OK*.

Il nome viene elencato nella finestra principale. Per eseguire la sincronizzazione con il palmare, selezionare *File → Sync (Sincronizza)*.

14 Utilizzo di Beagle

Beagle è uno strumento di ricerca che indicizza lo spazio delle informazioni perosonali dell'utente per aiutarlo a trovare qualsiasi informazione stia cercando. È possibile utilizzare Beagle per trovare documenti, e-mail, cronologia Web, Instant Messenger e conversazioni ITC, codice sorgente, immagini, file musicali, applicazioni e molto altro ancora.

Beagle supporta i seguenti sorgenti di dati:

- File system
- Pulsanti di avvio per le applicazioni
- Evolution mail e address book
- log del sistema di messaggistica in tempo reale Gaim
- Pagine Web Firefox (come vengono visualizzate)
- Aggregator Blam e Liferea RSS
- Tomboy notes

Supporta anche i seguenti formati file:

- OpenOffice.org
- Microsoft Office (doc, ppt, xls)

- HTML
- PDF
- Images (jpeg, png)
- Audio (mp3, ogg, flac)
- AbiWord
- Rich Text Format (rtf)
- Texinfo
- Pagine man
- Codice sorgente (C, C++, C#, Fortran, Java, JavaScript, Pascal, Perl, PHP, Python)
- Testo

Beagle indicizza automaticamente qualsiasi cosa presente nella home directory, ma è possibile scegliere di escludere alcuni file o directory. Beagle comprende anche diversi strumenti da utilizzare per la ricerca dei dati.

14.1 Indicizzazione dei dati

Il daemon di Beagle (`beagled`) esegue automaticamente tutte le indicizzazioni. Come impostazione predefinita, qualsiasi cosa presente nella home directory viene indicizzata. Beagle è in grado di rilevare le modifiche apportate alla home directory indicizzando di nuovo i dati di conseguenza.

- I file vengono immediatamente indicizzati al momento della creazione, indicizzati di nuovo quando modificati e rilasciati dall'indice quando cancellati.
- Le e-mail vengono indicizzate all'arrivo.
- Le conversazioni IM vengono indicizzate mentre si chatta una riga alla volta.

L'indicizzazione dei dati richiede una certa potenza, anche se il daemon di Beagle cerca di essere meno intrusivo possibile. Contiene uno scheduler che ha il compito di dare la

priorità ai task e di controllare l'utilizzo della CPU usage, sulla base dell'utilizzo attivo della workstation da parte dell'utente.

14.1.1 Come impedire che file e directory siano indicizzati

Se si desidera impedire che una directory (e tutte le sue sottodirectory) venga indicizzata, creare un file vuoto dal nome `.noindex` e inserirlo nella directory. È possibile aggiungere una lista di file e directory al file `.noindex` per impedirne l'indicizzazione. Nel file `.noindex` è consentito l'uso dei caratteri jolly.

È anche possibile inserire un file `.neverindex` nella propria home directory contenente una lista di file che non devono mai essere indicizzati. Anche in questo file è consentito l'uso dei caratteri jolly. Utilizzare gli stessi caratteri jolly utilizzati per `glob` (ad esempio, `f*le??.txt`). È anche possibile utilizzare espressioni regolari più potenti aggiungendo una barra prima e dopo il pattern (ad esempio, `/file.*.txt/`). Per ulteriori informazioni, visitare il sito Web di glob-UNIX (http://docs.python.org/lib/module-glob.html).

14.1.2 Indicizzazione manuale

Beagle ha un sistema efficace per stabilire dove indicizzare i file cercando di non interferire con altre applicazioni in esecuzione. Beagle definisce di proposito quando effettuare l'indicizzazione in base al carico e all'inattività del sistema, in modo tale da non influire negativamente sul desktop. In ogni caso, se si desidera indicizzare subito la propria home directory, immettere il comando riportato qui di seguito in una finestra del terminale prima di eseguire Beagle:

```
export BEAGLE_EXERCISE_THE_DOG=1
```

14.1.3 Controllo dello stato dell'indice

Beagle comprende i seguenti comandi che consentono di visualizzare lo stato di indicizzazione corrente:

`beagle-index-info`
: Visualizza la quantità e il tipo di documenti indicizzati.

`beagle-status`
Visualizza l'attività corrente che il daemon di Beagle sta eseguendo (in modo continuativo).

14.2 Ricerca dati

Beagle offre i seguenti strumenti che consentono di effettuare ricerche all'interno dei dati indicizzati.

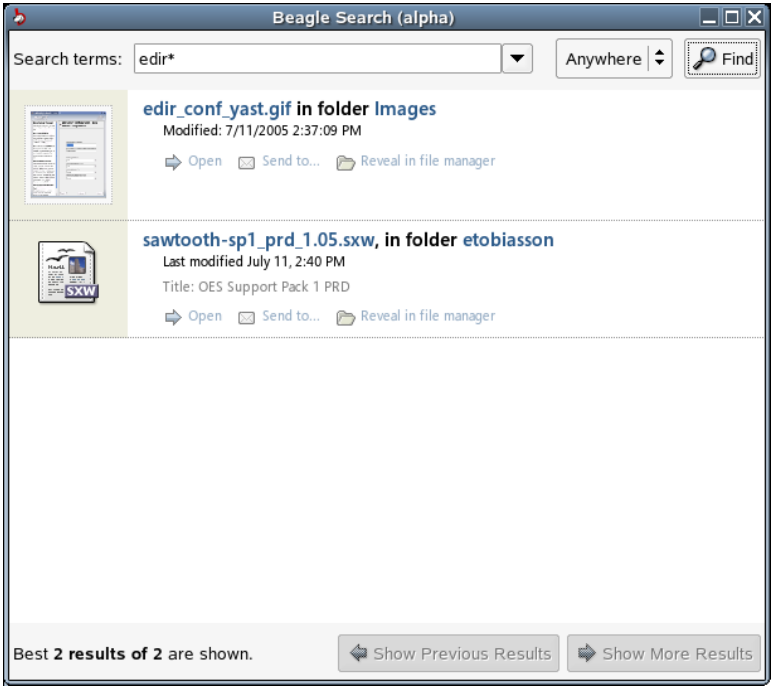
14.2.1 Best

Best (Bleeding Edge Search Tool) è uno strumento grafico che effettua la ricerca tra le informazioni indicizzate. Best non interroga direttamente l'indice, ma passa i termini di ricerca al daemon di Beagle che rimanda tutte le corrispondenze a Best. Best restituisce i risultati e consente all'utente di agire sugli oggetti corrispondenti.

Per aprire Best in KDE, cliccare su *K Menu → System → File System → Beagle Search*. In GNOME, cliccare su *Applicazioni → Sistema → File System → Ricerca Beagle*.

Per utilizzare Best, digitare semplicemente il testo di ricerca nella casella di inserimento in alto, quindi premere Invio o cliccare su *Trova*. Best interroga i file indicizzati e restituisce i risultati.

Figura 14.1 *Ricerca Beagle*



È possibile utilizzare la lista dei risultati per aprire un file, inviare un messaggio in tempo reale, rileggere un file, inoltrarlo o visualizzarlo in file manager. Le opzioni disponibili dipendono dal tipo di file.

È anche possibile utilizzare *Ovunque* per limitare la ricerca ai file presenti in una posizione specifica, ad esempio la rubrica degli indirizzi, o le pagine Web, oppure per visualizzare solo un tipo particolare di file nella lista dei risultati.

14.2.2 beagle-query

Beagle comprende uno strumento per la riga di comando che può essere utilizzato per la ricerca nell'indice di Beagle. Per utilizzare questo strumento, immettere il comando riportato qui di seguito nella finestra di un terminale:

```
beagle-query search
```

Sostituire *search* con il testo da trovare e beagle-query restituirà i risultati. Con questo comando è possibile utilizzare i caratteri jolly.

Utilizzare `beagle-query --verbose` *search* per visualizzare informazioni dettagliate sui risultati della ricerca.

Parte V. Immagini

15 Fotocamere digitali e Linux

La gestione delle fotografie scattate può essere divertente a patto di disporre degli strumenti appropriati. Linux offre varie utility pratiche per ordinare e organizzare le fotografie, tra cui gphoto2, Konqueror, Digikam e f-spot.

Un elenco completo delle fotocamere supportate è disponibile all'indirizzo `http://www.gphoto.org/proj/libgphoto2/support.php`. Se è stato installato gphoto2, recuperare l'elenco tramite il comando `gphoto2 --list-cameras`. Per informazioni sui comandi disponibili, digitare il comando `gphoto2 --help`.

SUGGERIMENTO: Fotocamere non supportate

Se la propria fotocamera non è presente nell'elenco di gphoto, non è detta l'ultima parola. È probabile che la fotocamera sia supportata come dispositivo di memorizzazione di massa USB. Per ulteriori informazioni, vedere la Sezione 15.2, «Accesso alla fotocamera» (p. 218).

15.1 Collegamento della fotocamera

Il modo più rapido e semplice per collegare fotocamere digitali al computer è il metodo USB, purché il kernel, la fotocamera e il computer lo supportino. Il kernel SUSE standard fornisce questo supporto. È anche necessario un cavo adatto.

Collegare la fotocamera alla porta USB e accendere la fotocamera. Potrebbe essere necessario attivare per la fotocamera una modalità di trasferimento dei dati particolare. Per questa procedura, consultare il manuale della fotocamera digitale.

15.2 Accesso alla fotocamera

Sono a disposizione tre metodi per accedere alle immagini presenti nella fotocamera. Il metodo varia a seconda della fotocamera e del protocollo da essa supportato. Di norma si tratta di memorizzazione di massa USB gestita dal sistema hotplug oppure del protocollo PTP (noto anche come PictBridge). Alcuni modelli di fotocamera non sono compatibili con nessuno dei due protocolli. Per il supporto di queste fotocamere, gphoto2 include driver specifici.

Il metodo più semplice è il supporto della memorizzazione di massa USB. Per saperne di più su questo argomento, leggere la documentazione della fotocamera. Alcune supportano 2 protocolli, come PTP e memorizzazione di massa USB. Purtroppo esistono anche delle fotocamere che comunicano con un protocollo proprietario, cosa che complica l'operazione. Se la fotocamera non supporta la memorizzazione di massa USB o PTP, le seguenti descrizioni non sono applicabili. Per raccogliere le informazioni necessarie, digitare il comando `gphoto2 --list-cameras` e leggere il contenuto della pagina `http://www.gphoto.org/`.

Se la fotocamera è compatibile con la memorizzazione di massa USB, selezionare quella opzione. Una volta collegata alla porta USB del computer e accesa, la fotocamera viene rilevata come sistema hotplug. Questo meccanismo prepara automaticamente il montaggio e consente l'accesso alla fotocamera. Al termine del montaggio, il desktop KDE mostra l'icona di una fotocamera.

Se il montaggio è corretto, l'utente potrà vedere una nuova directory sotto `/media`, la cui prima voce è `usb` e una serie di numeri. A ciascun fornitore e prodotto viene assegnato un numero che viene sempre proposto ogni volta che si collega il dispositivo al computer. La voce proposta varia a seconda del dispositivo collegato al bus USB. Il problema è individuare la voce corretta relativa alla fotocamera. Esaminare le sottodirectory `DCIM/`*`xxx`*. Ciascuna fotocamera presenta una diversa struttura ad albero e quindi non esiste una regola generale. La fotocamera si trova probabilmente nella directory contenente dei file JPEG.

Una volta trovata la directory corretta, è possibile copiare, spostare o eliminare i file della fotocamera tramite un file manager, come Konqueror, o tramite i comandi della shell (vedere la Sezione 27.3, «Comandi Linux importanti» (p. 429) e il *Riferimento*).

15.3 Uso di Konqueror

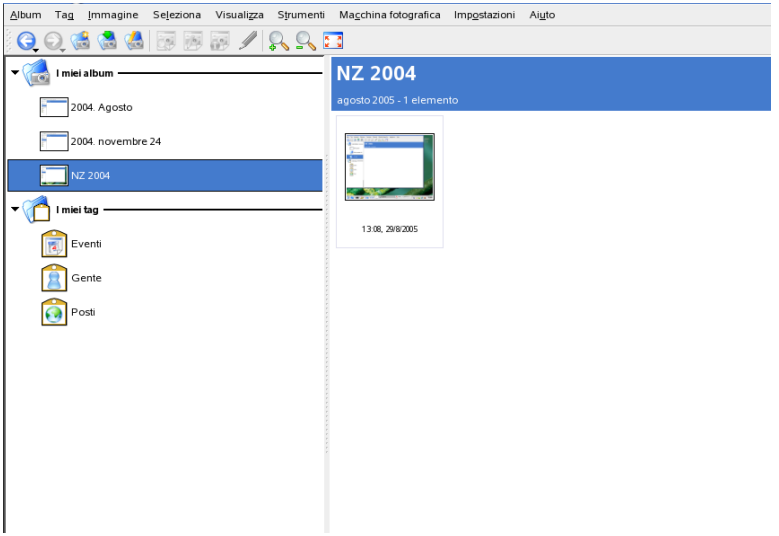
Gli utenti di KDE possono facilmente accedere alle fotocamere digitali tramite l'interfaccia Konqueror, con cui hanno familiarità. Collegare la fotocamera alla porta USB. L'icona di una fotocamera verrà visualizzata sul desktop. Fare clic su questa icona per aprire la fotocamera in Konqueror. È possibile accedere alla fotocamera anche immettendo l'URL `camera:/` in Konqueror. Esplorare la struttura della directory della fotocamera per visualizzare i file. Utilizzare le consuete funzioni di gestione dei file di Konqueror per copiare i file come desiderato. Per ulteriori informazioni sull'uso di Konqueror vedere il Capitolo 3, *Browser Web Konqueror* (p. 79).

15.4 Uso di Digikam

Digikam è un programma KDE per lo scaricamento di fotografie dalle fotocamere digitali. Al primo avvio è necessario indicare a Digikam dove memorizzare l'album delle fotografie. Se si sceglie una directory già contenente una raccolta di fotografie, Digikam considera ogni sottocartella come un album.

All'avvio di Digikam, viene visualizzata una finestra con 2 sezioni: gli album a sinistra e le fotografie dell'album selezionato a destra. Vedere la Figura 15.1, «Finestra principale di Digikam» (p. 220).

Figura 15.1 *Finestra principale di Digikam*



15.4.1 Configurazione della fotocamera

Per configurare una fotocamera in Digikam, selezionare *Camera (Fotocamera)* → *Add Camera (Aggiungi fotocamera)*. Provare a rilevare automaticamente la fotocamera con *Rilevamento automatico*. Se non vengono ottenuti risultati, scegliere *Aggiungi* e scorrere l'elenco alla ricerca del proprio modello. Se il modello della fotocamera non è incluso nell'elenco, provare un modello meno recente o usare *Fotocamera memorizzazione di massa USB/IEEE*. Confermare con *OK*.

15.4.2 Scaricamento di immagini dalla fotocamera

Una volta la fotocamera correttamente configurata, collegarsi ad essa; per fare ciò, dal menu *Camera (Fotocamera)*, scegliere il nome specificato nella finestra di dialogo in Sezione 15.4.1, «Configurazione della fotocamera» (p. 220). Digikam aprirà una finestra e inizierà a scaricare le miniature e le visualizzerà come descritto in Figura 15.2, «Scaricamento di immagini dalla fotocamera» (p. 221). Fare clic con il pulsante destro del mouse per aprire un menu a comparsa contenente le seguenti opzioni riguardanti

l'immagine: *View (Visualizza)*, *Properties (Proprietà)* o *EXIF Information (Informazioni EXIF)*, *Download (Scarica)* o *Delete (Elimina)*. La voce *Advanced (Avanzate)* offre delle opzioni di ridenominazione e dei comandi per la gestione delle informazioni fornite dalla fotocamera (EXIF).

Figura 15.2 *Scaricamento di immagini dalla fotocamera*

Le opzioni di ridenominazione possono essere molto utili se la fotocamera non applica nomi di file espliciti. Con Digikam è possibile rinominare le fotografie automaticamente. Fornire un prefisso univoco e se necessario, data, ora o numero sequenziale. Il resto verrà eseguito da Digikam.

Selezionare le fotografie da scaricare dalla fotocamera premendo il pulsante sinistro del mouse oppure facendo clic sulle singole fotografie premendo Ctrl. Le fotografie selezionate vengono visualizzate con i colori invertiti. Fare clic su *Download (Scarica)*.

Selezionare la destinazione nell'elenco o creare un nuovo album scegliendo *New Album (Nuovo album)*. Verrà automaticamente suggerito un nome di file con la data corrente. Confermare con *OK* per scaricare.

15.4.3 Informazioni sulle fotografie

Non è difficile ottenere informazioni sulle fotografie. Posizionare il mouse sulla miniatura per visualizzare un breve riepilogo sotto forma di tecnica d'uso. Per informazioni più complete, fare clic con il pulsante destro del mouse sulla fotografia e scegliere *Properties (Proprietà)*. Verrà visualizzata una finestra di dialogo con tre schede: *General (Generale)*, *EXIF* e *Histogram (Istogramma)*.

La scheda *General (Generale)* elenca nome, tipo, proprietario e altre informazioni di base. La scheda *EXIF* è quella più interessante. La fotocamera memorizza dei metadati per ciascuna fotografia. Tali proprietà vengono lette da Digikam e visualizzate in questo elenco. Le informazioni includono il tempo di esposizione, la dimensione dei pixel e altro. Per ottenere altre informazioni sulla voce selezionata, premere Shift + F1. Verrà visualizzata una piccola tecnica d'uso. L'ultima scheda, *Istogramma*, mostra alcune informazioni statistiche.

15.4.4 Gestione degli album

Per default, Digikam inserisce una cartella denominata *My Albums (Album)* per raccogliervi le proprie fotografie. Queste possono essere memorizzate più tardi in sottocartelle. Gli album possono essere ordinati in base al layout, al nome della raccolta definito nelle proprietà dell'album o alla data di creazione (che può comunque essere modificata nelle proprietà).

Per creare un nuovo album, sono a disposizione più possibilità:

- Scaricare nuove fotografie dalla fotocamera
- Creare un nuovo album facendo clic su *New Album (Nuovo album)* nella barra degli strumenti
- Importare una cartella di fotografie esistente dal disco rigido selezionando *Album → Import (Importa) → Import Folders (Importa cartelle)*)

- Fare clic con il pulsante destro del mouse su *My Albums (Album)* e selezionare *New Album (Nuovo album)*

Dopo avere selezionato il metodo preferito di creazione di un album, viene visualizzata una finestra di dialogo. Assegnare un nome all'album. Se necessario, scegliere una raccolta, inserire commenti e selezionare una data. La raccolta è il modo in cui si organizzano gli album in base a un'etichetta comune. Questa etichetta viene sfruttata quando si seleziona *View (Visualizza) → Sort Albums (Ordina album) → By Collection (Per raccolta)*. Il commento verrà visualizzato nel banner superiore della finestra principale. La data dell'album viene sfruttata quando si seleziona *View (Visualizza) → Sort Albums (Ordina album) → By Date (Per data)*.

Digikam usa la prima fotografia nell'album come anteprima dello stesso nell'elenco *My Albums (Album)*. Per selezionarne un'altra, fare clic con il pulsante destro del mouse sulla fotografia preferita e selezionare *Set as Album Thumbnail (Imposta come miniatura dell'album)* dal menu contestuale.

15.4.5 Gestione dei tag

La gestione di numerose fotografie in più album può essere a volte un'operazione complessa. Per organizzare le singole fotografie, Digikam offre il sistema *My Tag*.

Ad esempio, si supponga di avere diverse fotografie di Paolo in varie occasioni e in diversi album e di volerle raccogliere tutte. L'individuazione di tutte le fotografie è molto semplice. Innanzitutto, creare un nuovo tag facendo clic su *My Tags (Tag) → People (Persone)*. Dal menu contestuale, scegliere *New Tag (Nuovo tag*. Nella finestra di dialogo che verrà visualizzata, immettere *Paolo* come titolo ed eventualmente come icona. Confermare con *OK*.

Dopo la creazione del tag, assegnarlo alle fotografie desiderate. In ciascun album, selezionare le fotografie desiderate. Fare clic con il pulsante destro del mouse e scegliere *Assign Tag (Assegna tag) → People (persone) → Paolo*. In alternativa, trascinare le photographs sul nome del tag sotto *My Tags (Tag)*, quindi rilasciarle. Ripetere l'operazione con gli album desiderati. Per visualizzare tutte le fotografie fare clic su *My Tags (Tag) → People (Persone) → Paolo*. A ogni fotografia è possibile assegnare più tag.

La modifica di tag e commenti può essere noioso. Per semplificare questa operazione, fare clic con il pulsante destro del mouse sulla fotografia e selezionare *Edit Comments*

& Tags (Modifica commenti e tag). Verrà visualizzata una finestra di dialogo contente un'anteprima, un commento e un elenco di tag. Ora è possibile inserire tutti i tag desiderati e aggiungere un commento. Per scorrere l'album, scegliere *Forward (Avanti)* e *Back (Indietro)*. Per salvare le modifiche, scegliere *Apply (Applica)* poi *Ok* per chiudere la finestra.

15.4.6 Esportazione delle raccolte di immagini

Digikam offre varie opzioni di esportazione per l'archiviazione e pubblicazione delle raccolte di immagini personali. L'esportazione può essere fatta verso CD o DVD (tramite k3b), verso HTML o una galleria remota.

Per salvare la raccolta di immagini su CD o DVD, procedere come segue:

1. Selezionare *File → Export (Esporta) → Archive to CD/DVD (Archivia su CD/DVD)*.

2. Apportare le opportune modifiche nella finestra di dialogo *Create CD/DVD Archive (Crea archivio CD/DVD)* tramite i vari sottomenu a disposizione. Al termine, fare clic su *OK* per iniziare il processo di masterizzazione.

   a. *Selection (Selezione)*: consente di determinare quali parti della raccolta archiviare in base alla selezione di album e tag.

   b. *HTML Interface (Interfaccia HTML)*: consente di indicare se la raccolta di immagini deve essere accessibile tramite interfaccia HTML e se aggiungere una funzionalità di esecuzione automatica all'archivio CD/DVD. Consente anche di selezionare titolo e immagine, font e proprietà dello sfondo.

   c. *Media Volume Descriptor (Descrittore del volume di supporto)*: consente di modificare le impostazioni della descrizione del volume, se necessario.

   d. *Media Burning (Masterizzazione)*: consente di regolare le opzioni di masterizzazione, se necessario.

Per creare un'esportazione HTML della raccolta di immagini, procedere come segue:

1. Selezionare *File → Export (Esporta) → HTML Export (Esporta in HTML)*.

2. Regolare le impostazioni in *Create Image Galleries (Crea galleria di immagini)* in base alle proprie esigenze tramite i vari sottomenu. Al termine, fare clic su *OK* per iniziare la creazione della galleria.

   a. *Selection (Selezione)*: consente di determinare quali parti della raccolta archiviare in base alla selezione di album e tag.

   b. *Look (Aspetto)*: consente di impostare titolo e aspetto della galleria HTML.

   c. *Album*: consente di determinare l'ubicazione della galleria sul disco nonché dimensione, compressione, formato delle immagini e quantità di metadati da visualizzare nella galleria.

   d. *Thumbnails (Miniature)*: analogamente alle immagini di destinazione, consente di specificare dimensione, compressione e formato delle miniature usate per esplorare la galleria.

Per esportare la raccolta a una galleria di immagini esterna su Internet, procedere come segue:

1. Ottenere un conto presso un sito Web esterno per caricarvi la galleria.

2. Selezionare *File → Export (Esporta) → Export to Remote Gallery (Esporta a galleria remota)* e fornire URL, nome utente e parola d'ordine del sito esterno quando richiesti.

   Digikam stabilisce una connessione al sito specificato e apre una nuova finestra denominata *Gallery Export (Esportazione galleria)*.

3. Determinare l'ubicazione del nuovo album all'interno della galleria.

4. Fare clic su *New Album (Nuovo album)* e fornire le informazioni richieste da Digikam.

5. Per caricare le immagini nel nuovo album, premere *Add Photos (Aggiungi fotografie)*.

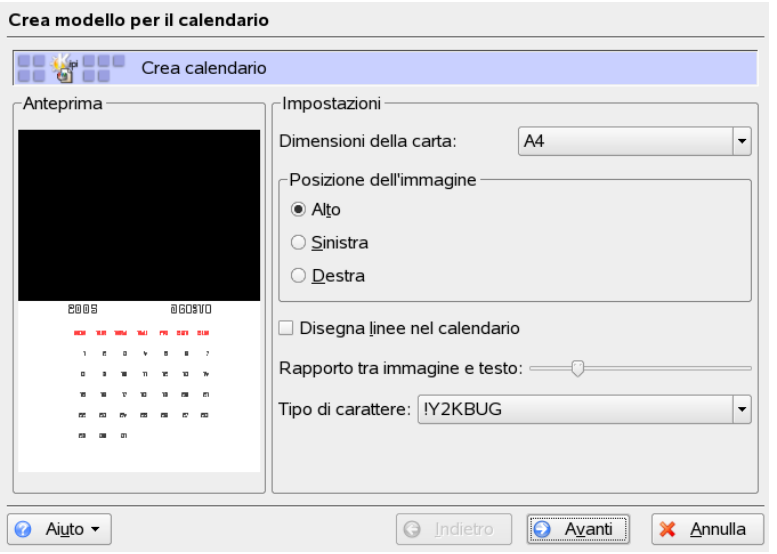
15.4.7 Strumenti utili

Digikam offre numerosi strumenti per semplificare alcune operazioni. Questi sono disponibili nel menu *Tools (Strumenti)*. Di seguito viene fornita la descrizione di alcuni di essi.

Creazione di un calendario

Un calendario personalizzato può essere una buona idea per un regalo. Selezionare *Tools (Strumenti)* → *Create Calendar (Crea calendario)* per aprire una procedura guidata come quella in Figura 15.3, «Creazione di un modello per un calendario» (p. 226).

Figura 15.3 *Creazione di un modello per un calendario*



Personalizzare le impostazioni (dimensione carta, posizione immagine, font, ecc.) e confermare selezionando *Next (Avanti)*. Immettere l'anno e selezionare le immagini da usare. Fare di nuovo clic su *Next (Avanti)* per visualizzare un riepilogo. Infine fare clic su *Next (Avanti)* per aprire la finestra di dialogo KDE Printer (Stampante KDE) che consente di visualizzare un'anteprima, salvare in formato PDF o stampare direttamente.

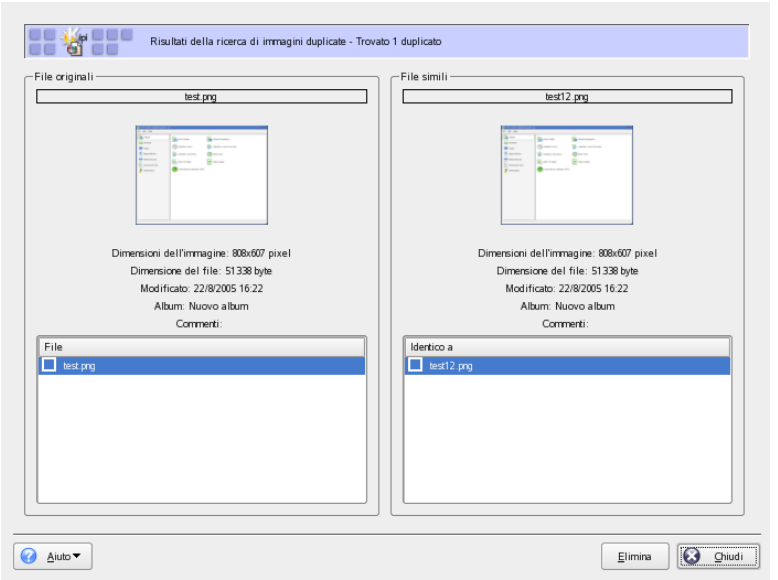
Ricerca delle fotografie duplicate

A volte in un gruppo di fotografie di scene simili, se ne vogliono conservare solo le più belle. Per questa operazione, il plug-in *Find Duplicate (Trova duplicati)* è l'ideale.

Selezionare *Tools (Strumenti)* → *Find Duplicate Images (Trova immagini duplicate)*. Selezionare gli album o i tag da gestire. Sotto *Method & Cache (Metodo e cache)*, scegliere il metodo di ricerca: uno più preciso o uno più rapido. Confermare con *OK* per avviare la ricerca.

I duplicati eventualmente trovati verranno visualizzati in una finestra come quella in Figura 15.4, «Risultati della ricerca» (p. 227). Selezionare le immagini da eliminare e fare clic su *Delete (Elimina)*. Chiudere la finestra selezionando *Close (Chiudi)*.

Figura 15.4 *Risultati della ricerca*



Processi batch

Digikam offre inoltre alcuni processi batch per eseguire una specifica operazione su più file alla volta. In questo ambito è possibile rinominare, convertire, ridimensionare

e altro ancora. I comandi sono disponibili sotto *Tools (Strumenti) → Batch Processes (Processi batch)*.

15.4.8 Visualizzazione e modifica di base delle immagini con Digikam

Digikam include un programma intuitivo di visualizzazione e modifica di immagini. Per aprirlo fare doppio clic sulla miniatura di un'immagine.

Lo strumento consente di effettuare alcune modifiche di base sulle immagini scaricate dalla fotocamera. È possibile ritagliare, ruotare o capovolgere le immagini, effettuare alcune regolazioni di base dei colori, applicare vari filtri colorati (ad esempio per esportare in bianco e nero un'immagine a colori) e ridurre in modo efficace gli occhi rossi nei primi piani.

I menu più importanti sono:

Immagine
: Per immettere commenti a una data immagine e per assegnare a essa un tag (categoria), usare *Edit Comments & Tags (Modifica commenti e tag)*. La voce *Properties (Proprietà)* apre una finestra con 3 schede relative a informazioni generali, informazioni EXIF e istogramma dell'immagine.

Fix (Ripara)
: Questo menu contiene alcune delle funzioni di modifica più utili nella fotografia digitale. *Colors (Colori)* apre un sottomenu per modificare tutte le impostazioni di base dei colori. È possibile anche sfuocare o modificare il contrasto di tutta o solo di una parte dell'immagine selezionata. Per ridurre gli occhi rossi in un primo piano, selezionare l'area dell'occhio tenendo premuto il pulsante sinistro del mouse e trascinando per espandere la selezione, selezionare *Red Eye Reduction (Riduzione occhi rossi)*, quindi scegliere una riduzione leggera o aggressiva a seconda se la selezione include l'intera area o solo gli occhi.

Transform (Trasforma)
: Il menu *Transform (Trasforma)* consente di ritagliare, ruotare, capovolgere e ridimensionare. L'opzione *Aspect Ratio Crop (Ritaglio con proporzioni)* consente di ritagliare mantenendo le proporzioni.

Filtri

Per trasformare gli scatti a colori in fotografie in bianco e nero o per dare loro l'aspetto seppia, aprire il menu *Filters (Filtri)* e scegliere le varie opzioni di esportazione.

Per saperne di più su questo strumento, consultare la guida in linea di Digikam in *digiKam Image Editor*, accessibile tramite il pulsante *Help (Guida)* nella barra dei menu di Digikam.

SUGGERIMENTO: Elaborazione avanzata delle immagini

L'elaborazione professionale delle immagini può essere svolta tramite lo strumento The GIMP. Per ulteriori informazioni su The GIMP, vedere il Capitolo 17, *Manipolazione delle immagini con The GIMP* (p. 247).

15.5 Utilizzo di f-spot

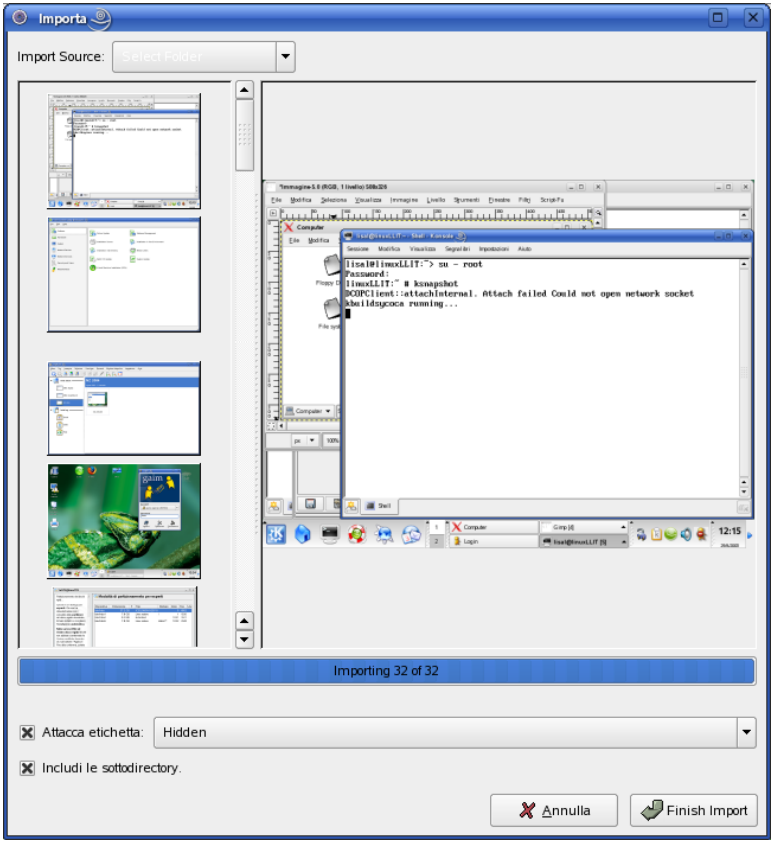
f-spot è uno strumento di gestione della raccolta di immagini digitali concepito per il desktop GNOME. Esso consente di assegnare tag differenti alle immagini in modo da poterle classificare e offre diverse opzioni di modifica.

Al primo avvio di f-spot, è necessario indicare l'ubicazione delle immagini da importare per la raccolta f-spot. Se si dispone già di una raccolta di immagini memorizzate sul disco rigido, immettere il percorso della relativa directory ed eventualmente includere le sottocartelle. f-spot importerà le immagini nel proprio database.

SUGGERIMENTO: Aggiunta di tag alle immagini durante l'importazione

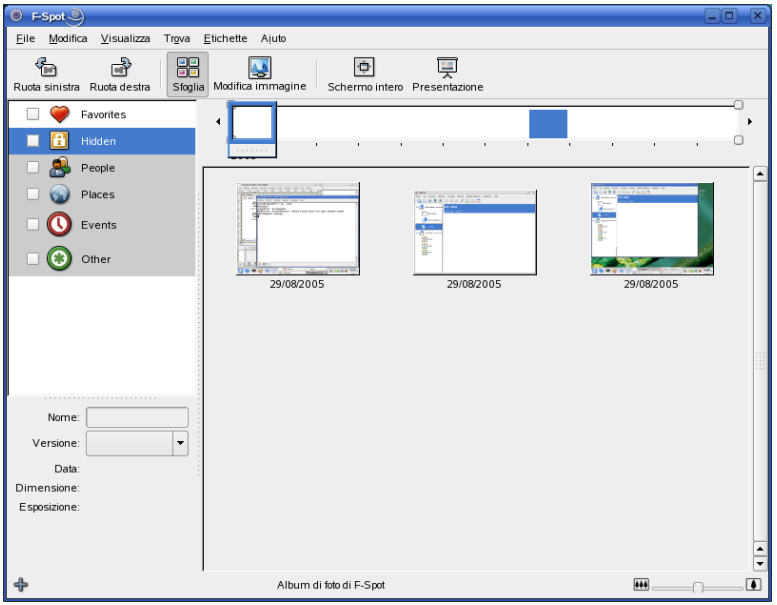
Se tutte le immagini da importare appartengono alla stessa categoria, è possibile allegare il tag appropriato al momento dell'importazione. Selezionare *Attach Tag (Allega tag)* e scegliere il tag corrispondente dal menu a discesa.

Figura 15.5 *Importazione di immagini in f-spot*



La finestra principale di f-spot è suddivisa in 3 aree principali. Nel riquadro a sinistra, sono visualizzati categorie, tag e informazioni dettagliate relativi alle immagini selezionate. Al centro compaiono le miniature di tutte le immagini associate al tag o alla categoria selezionata. Se nessuna immagini è selezionata, l'intera raccolta viene visualizzata nel riquadro a destra.

Figura 15.6 *Finestra principale di f-spot*



Una barra dei menu nella parte superiore della finestra fornisce l'accesso ai menu principali. Una barra degli strumenti posta sotto offre varie funzioni rappresentate da una corrispondente icona:

Rotate (Left or Right) (Ruota a destra o a sinistra)
Questa scorciatoia consente di cambiare l'orientamento di un'immagine.

Sfoglia
La modalità *Browse (Sfoglia)* consente di visualizzare e cercare nell'intera raccolta o solo in alcune parti in cui sono presenti dei tag. Le immagini possono anche essere ricercate in base alla data di creazione.

Edit Image (Modifica immagine)
Questa modalità consente di selezionare un'immagine per sottoporla all'elaborazione di base. Per maggiori dettagli vedere la Sezione 15.5.6, «Elaborazione di base delle immagini con f-spot» (p. 236).

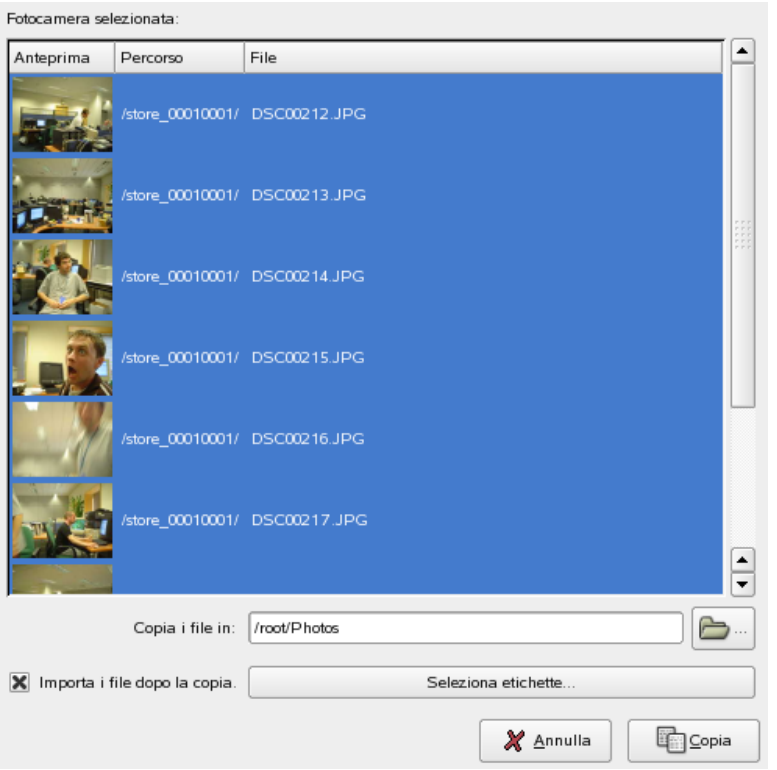
Fullscreen (Schermo intero)
Consente di passare alla visualizzazione a tutto schermo.

Slideshow (Presentazione)
Consente di avviare una presentazione.

15.5.1 Scaricamento di immagini dalla fotocamera

Per importare nuove immagini dalla fotocamera digitale collegata alla porta USB del computer, usare *File → Import from Camera (Importa da fotocamera)*. Il tipo di fotocamera viene automaticamente rilevato.

Figura 15.7 *Importazione dalla fotocamera*



f-spot apre una finestra di anteprima per visualizzare tutte le immagini scaricabili dalla fotocamera. I file vengono copiati nella directory di destinazione specificata tramite

Copy Files to (Copia file in). Se l'opzione *Import files after copy (Importa file dopo la copia)* è selezionata, tutte le immagini copiate dalla fotocamera vengono automaticamente importate nel database di f-spot. L'aggiunta di tag può essere fatta durante l'importazione tramite il comando *Select Tags (Seleziona tag)*. Per non importare una fotografia dalla fotocamera, è sufficiente deselezionarla nella finestra di anteprima.

15.5.2 Informazioni sulle fotografie

Quando un'immagine è selezionata, vengono visualizzate alcune informazioni di base nell'angolo inferiore sinistro della finestra. Tali informazioni includono il nome del file, la sua versione (copia o immagine originale), la data di creazione, la sua dimensione e l'esposizione usata. Per visualizzare i dati EXIF associati al file immagine, scegliere *View (Visualizza)* → *EXIF Data (Dati EXIF)*.

15.5.3 Gestione dei tag

I tag sono utili per classificare le immagini e creare sottoinsiemi nell'ambito di una raccolta. Ad esempio, per filtrare i primi piani nell'ambito di una raccolta, procedere come segue:

1. In f-spot, selezionare la modalità *Browse (Sfoglia)*.

2. Nel riquadro di sinistra della finestra f-spot, selezionare la categoria *People (Persone)*, fare clic con il pulsante destro del mouse su di essa, quindi scegliere *Create New Tag (Crea nuovo tag)*. I nuovi tag verranno visualizzati come sottocategoria sotto la categoria *People (Persone)*:

   a. Creare un nuovo tag denominato `Friends (Amici)`.

   b. Creare un nuovo tag denominato `Family (Famiglia)`.

3. A questo punto associare i tag alle immagini o gruppi di immagini selezionati. Fare clic con il pulsante destro del mouse su un'immagine, scegliere *Attach Tag (Allega tag)*, quindi selezionare il tag appropriato per l'immagine. Per allegare un tag a un gruppo di immagini, fare clic sulla prima immagine e premere Shift quindi selezionare le altre tenendo premuto il tasto Shift. Fare clic con il pulsante

destro del mouse sul gruppo di immagini selezionate e selezionare la categoria corrispondente.

Una volta le immagini classificate, è possibile sfogliare la raccolta in base ai tag. È sufficiente selezionare *People (Persone)* → *Family (Famiglia)* per visualizzare la solo le immagini della raccolta associate al tag `Family (Famiglia)`. È inoltre possibile effettuare ricerche nella raccolta in base ai tag selezionando *Find (Trova)* → *Find by Tag (Trova per tag)*. Il risultato della ricerca verrà visualizzato nella finestra delle miniature.

La modalità di rimozione dei tag da una o più immagini è analoga a quella adottata per l'aggiunta degli stessi. Le funzioni di modifica dei tag sono accessibili anche tramite il menu *Tags (Tag)* nella barra dei menu.

15.5.4 Ricerca avanzata

Come menzionato prima in Sezione 15.5.3, «Gestione dei tag» (p. 233), i tag possono essere usati come mezzo per trovare immagini specifiche. Un altro modo, alquanto esclusivo di f-spot, è quello di usare la funzione *Timeline* (Sequenza temporale) sotto la barra degli strumenti. Trascinare il piccolo quadretto lungo la sequenza temporale per visualizzare solo le miniature delle immagini scattate in quel determinato intervallo di tempo. f-spot dispone di una sequenza temporale di default che può essere modificata spostando i cursori a destra o a sinistra.

15.5.5 Esportazione delle raccolte di immagini

f-spot offre una gamma di diverse funzioni di esportazione della raccolta sotto *File* → *Export (Esporta)*. Il comando probabilmente più usato è *Export to Web Gallery (Esporta a galleria Web)* e *Export to CD (Esporta a CD)*.

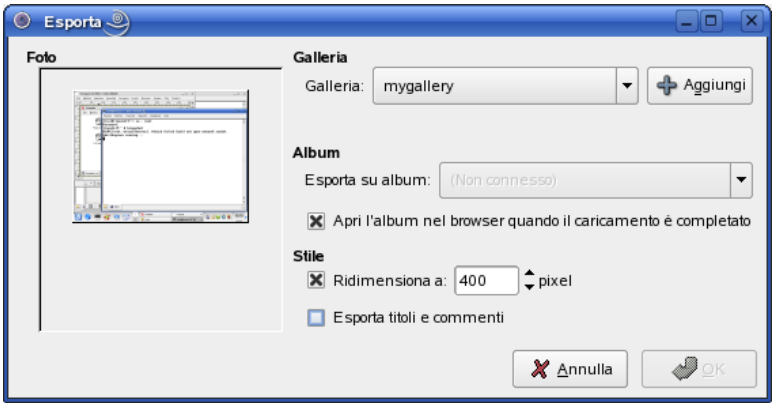
Per esportare una selezione di immagini a una galleria Web, procedere come segue:

1. Selezionare le immagini da esportare.

2. Fare clic su *File* → *Export (Esporta)* → *Export to Web Gallery (Esporta a galleria Web)* e selezionare una galleria a cui esportare le immagini, oppure crearne una.

f-spot stabilità una connessione al sito Web contenente la galleria. Selezionare l'album in cui esportare le immagini e decidere se ridimensionarle automaticamente e se esportare titoli e commenti.

Figura 15.8 *Esportazione di immagini a una galleria Web*



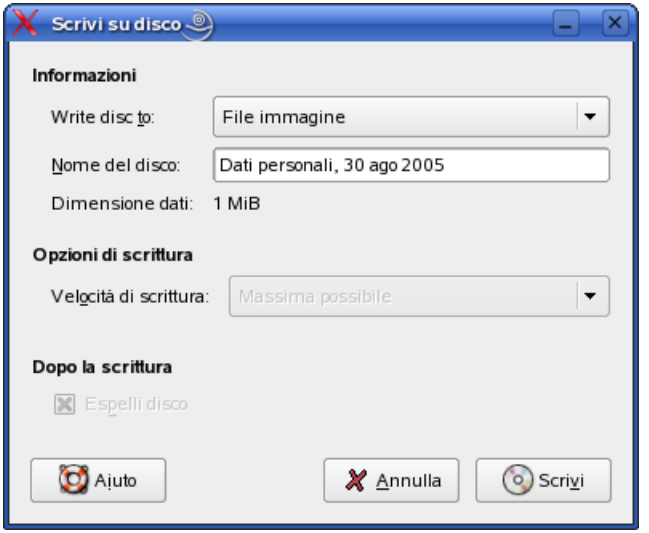
Per esportare una selezione di immagini a un CD, procedere come segue:

1. Selezionare le immagini da esportare.

2. Selezionare *File → Export (Esporta) → Export to CD (Esporta a CD)* e fare clic su *OK*.

   f-spot copia i file e apre la finestra di masterizzazione. Assegnare un nome al disco e definire la velocità di scrittura. Fare clic su *Write (Scrivi)* per avviare la masterizzazione.

Figura 15.9 *Esportazione di immagini a un CD*



15.5.6 Elaborazione di base delle immagini con f-spot

f-spot offre numerose funzioni di base per la modifica delle immagini. Per accedere alla modalità di modifica di f-spot, fare clic sull'icona *Edit Image (Modifica immagine)* posta nella barra degli strumenti o fare doppio clic sull'immagine. Per passare da un'immagine all'altra, servirsi dei tasti freccia posti in basso a sinistra. Le funzioni di modifica disponibili sono:

Sharpen (Contrasta)
: Per accedere a questa funzione, scegliere *Edit (Modifica)* → *Sharpen (Contrasta)*. Regolare i valori di *Amount (Quantità)*, *Radius (Raggio)* e *Threshold (Soglia)* e fare clic su *OK*.

Crop Image (Ritaglia immagine)
: Per ritagliare una selezione dell'immagine, scegliere una percentuale di ritaglio fissa o l'opzione *No Constraint (Senza restrizioni)* dal menu a discesa in basso a sinistra, selezionare l'area da ritagliare, quindi fare clic sull'icona forbici a fianco del menu percentuale.

Red Eye Reduction (Riduzione occhi rossi)
Nei primi piani, selezionare l'area dell'occhio e fare clic sull'icona occhio rosso.

Adjust Color (Regola colore)
Esaminare l'istogramma usato per creare lo scatto e se necessario correggere esposizione e intensità del colore.

SUGGERIMENTO: Elaborazione avanzata delle immagini

L'elaborazione professionale delle immagini può essere svolta tramite lo strumento The GIMP. Per ulteriori informazioni su The GIMP, vedere il Capitolo 17, *Manipolazione delle immagini con The GIMP* (p. 247).

15.6 Per ulteriori informazioni

Per ulteriori informazioni sull'uso di fotocamere digitali con Linux, fare riferimento ai seguenti siti Web:

- `http://digikam.sourceforge.net/`—Informazioni su Digikam
- `http://www.gphoto.org`—Informazioni su gPhoto2
- `http://www.gphoto.org/proj/libgphoto2/support.php`—Elenco completo delle fotocamere supportate
- `http://www.thekompany.com/projects/gphoto/`—Informazioni su Kamera, un'applicazione front-end di KDE per gPhoto2

Kooka—Applicazione per la scansione

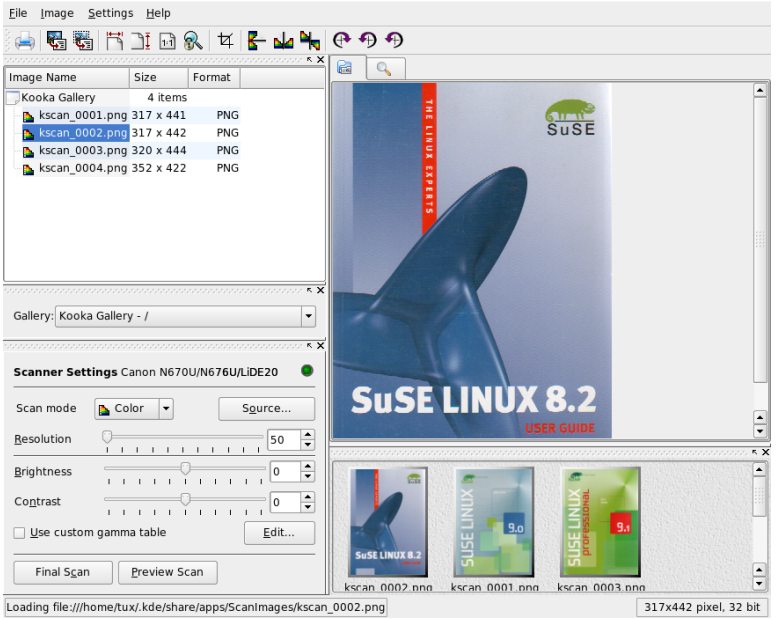
16

Kooka è un'applicazione KDE per la scansione. In questo capitolo vengono descritte l'interfaccia utente e le funzionalità dell'applicazione. Oltre alla creazione di file di immagine da materiale stampato quale riviste o fotografie, Kooka consente il riconoscimento dei caratteri. In questo modo è possibile convertire un testo scritto in un file che potrà essere modificato.

Avviare Kooka dal menu principale o immettere il comando `kooka`. Una volta avviata, in Kooka viene aperta una finestra costituita da tre frame con una barra dei menu in alto a sinistra e una barra degli strumenti subito sotto. Tutte le finestre possono essere liberamente ridimensionate o riposizionate con il mouse. È inoltre possibile staccare completamente singoli frame dalla finestra di Kooka per collocarli sul desktop in base alle proprie esigenze. Per spostare i frame, fare clic e trascinare la doppia riga sottile proprio sopra il frame. Ogni frame, ad eccezione della finestra principale, può essere posizionato all'interno di qualsiasi altro frame allineato a sinistra, a destra, in alto, in basso o centrato. Le finestre centrate hanno le stesse dimensioni, sono impilate e possono essere portate in primo piano con le schede.

Per default, i frame *Visualizzatore di immagini* e *Anteprima* condividono una finestra. Le schede consentono di passare da un frame all'altro. Nel frame a sinistra è disponibile la galleria. Si tratta di un piccolo browser di file per l'accesso alle immagini acquisite. Il frame in basso a destra viene condiviso da OCR (Optical Character Recognition, Riconoscimento ottico dei caratteri) e miniature, che possono essere caricate nel visualizzatore di immagini con un semplice clic del mouse. Vedere la Figura 16.1, «Finestra principale di Kooka» (p. 240).

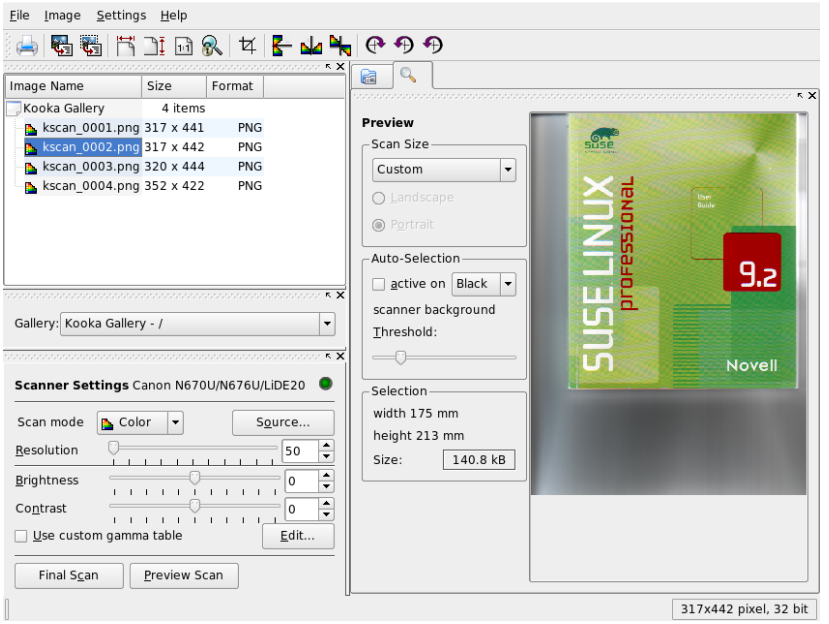
Figura 16.1 *Finestra principale di Kooka*



16.1 Anteprima

È necessario creare sempre un'anteprima quando l'oggetto di cui eseguire la scansione è più piccolo dell'area di scansione totale. Impostare alcuni parametri a sinistra del frame di anteprima. Selezionare la dimensione di scansione con *Personalizzato* o uno dei formati standard. Vedere la Figura 16.2, «Finestra di anteprima di Kooka» (p. 241). L'impostazione *Personalizzato* è più flessibile, poiché consente una selezione dell'area desiderata con il mouse. Dopo aver definito le impostazioni, richiedere l'anteprima dell'immagine di cui eseguire la scansione facendo clic su *Scansione di anteprima* in *Parametro di scansione*.

Figura 16.2 *Finestra di anteprima di Kooka*

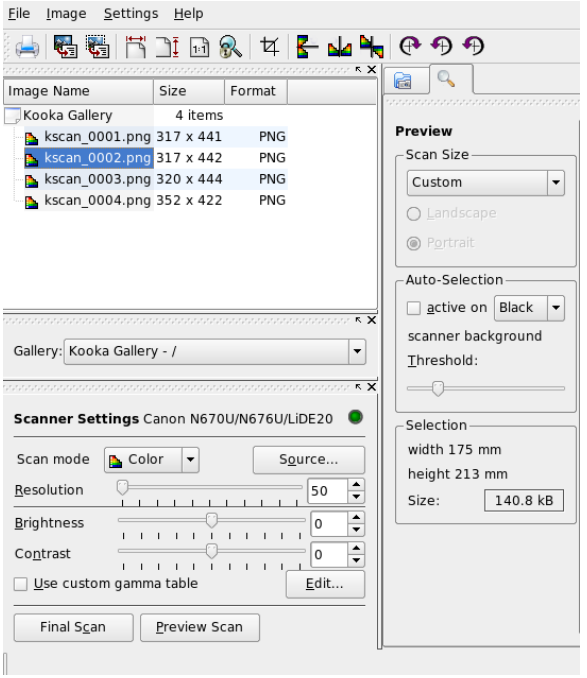


16.2 Scansione finale

Se è stata selezionata l'opzione *Personalizzato* per la dimensione di scansione, utilizzare il mouse per selezionare l'area rettangolare di cui eseguire la scansione. L'area selezionata è delimitata da un bordo punteggiato.

Scegliere tra la scansione a colori e in bianco e nero, quindi impostare la risoluzione con il dispositivo di scorrimento. Vedere la Figura 16.3, «Parametri di scansione Kooka» (p. 242). Maggiore è la risoluzione, migliore sarà la qualità dell'immagine di cui è stata eseguita la scansione. Tuttavia, questo determina anche un aumento delle dimensioni del file corrispondente e un prolungamento del processo di scansione in caso di risoluzioni elevate. Attivare *Usa tabella gamma personalizzata* e fare clic su *Modifica* per modificare le impostazioni di luminosità, contrasto e gamma.

Figura 16.3 *Parametri di scansione Kooka*



Una volta definite tutte le impostazioni, fare clic su *Scansione finale* per eseguire la scansione dell'immagine. L'immagine di cui è stata eseguita la scansione viene visualizzata nel visualizzatore di immagini e come miniatura. Quando richiesto, selezionare il formato in cui salvare l'immagine. Per salvare tutte le immagini future nello stesso formato, selezionare la casella corrispondente. Confermare con *OK*.

16.3 Menu

Alcune delle funzioni della barra degli strumenti sono disponibili anche nei menu *File* e *Immagine*. Modificare le impostazioni delle preferenze per Kooka in *Impostazioni*.

File

Utilizzare questo menu per avviare l'assistente di stampa KPrinter, creare una nuova cartella per le immagini e per salvare, cancellare e chiudere i file. I risultati OCR

di un documento di testo di cui è stata eseguita la scansione possono essere salvati qui. È inoltre possibile utilizzare questo menu per chiudere Kooka.

Immagine
Il menu *Immagine* consente di avviare un'applicazione di grafica per il postprocessing o il riconoscimento ottico dei caratteri di un'immagine. Il testo riconosciuto tramite un'operazione OCR viene visualizzato nel relativo frame. Sono disponibili diversi strumenti per la scala, la rotazione e il ribaltamento di un'immagine. È possibile accedere a queste funzioni anche dalla barra degli strumenti. *Crea da selezione* consente di salvare un'area di un'immagine precedentemente selezionata con il mouse.

Impostazioni

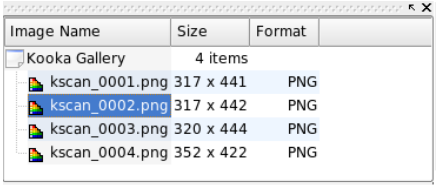
Il menu *Impostazioni* consente di regolare l'aspetto di Kooka. La barra degli strumenti e la barra di stato possono essere attivate e disattivate ed è possibile definire le scorciatoie da tastiera per le voci di menu. *Configura le barre degli strumenti* fornisce un elenco di tutte le funzioni disponibili nella barra degli strumenti. *Configura Kooka* apre una finestra di dialogo per la configurazione che consente di modificare l'aspetto di Kooka. In genere, tuttavia, le impostazioni di default sono sufficienti. In *Strumento viste*, abilitare e disabilitare il visualizzatore di miniature, l'anteprima, la galleria, i parametri di scansione e la finestra dei risultati OCR.

Aiuto
Il menu *Guida* consente di accedere al manuale della Guida in linea per Kooka. Inoltre consente di accedere a un canale di feedback per problemi e suggerimenti. Fornisce inoltre informazioni sulla versione, gli autori e la licenza di Kooka e KDE.

16.4 Galleria

La finestra della galleria mostra la cartella di default in cui vengono memorizzati tutti i file di immagine di Kooka. Nella Figura 16.4, «Galleria di Kooka» (p. 244) è illustrato un esempio. Per salvare un'immagine nella home directory personale, fare clic sulla miniatura e selezionare *File* → *Salva immagine*. Successivamente, immettere la home directory personale e assegnare al file un nome descrittivo.

Figura 16.4 *Galleria di Kooka*

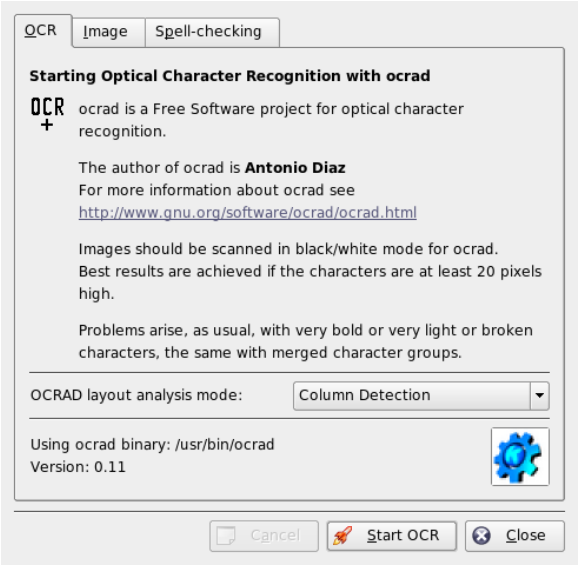


Per aggiungere immagini alla galleria, trascinare e rilasciare le immagini da Konqueror. Avviare Konqueror, accedere alla directory contenente le immagini da aggiungere alla galleria, quindi trascinarle con il mouse in una cartella della galleria di Kooka.

16.5 Riconoscimento ottico dei caratteri

Se è installato il modulo per il riconoscimento dei caratteri, è possibile eseguire la scansione dei documenti in modalità *lineart*, salvarli nel formato proposto, quindi elaborali per il riconoscimento del testo dal menu *Immagine*. Elaborare l'intero documento o solo un'area selezionata in precedenza. Viene visualizzata una finestra di configurazione in cui viene specificato al modulo se il testo originale è stampato, scritto a mano o di tipo standard. Impostare anche la lingua in modo che il modulo possa elaborare il documento correttamente. Vedere la Figura 16.5, «OCR con Kooka» (p. 245).

Figura 16.5 *OCR con Kooka*



Passare alla finestra *Testo prodotto dall'OCR* e controllare il testo, per cui potrebbe essere necessaria una revisione. Per eseguire questa operazione, salvare il testo mediante *File* → *Salva il testo prodotto dall'OCR*. Il testo può essere elaborato con OpenOffice.org o KWrite.

17 Manipolazione delle immagini con The GIMP

GIMP (*GNU Image Manipulation Program*) è un programma che consente di creare e modificare la grafica pixel. Per molti aspetti, le relative funzioni sono paragonabili a quelle di Adobe Photoshop e altri programmi commerciali. È possibile utilizzarlo per ridimensionare e ritoccare fotografie, progettare la grafica per le pagine Web, creare copertine per i propri CD personalizzati o quasi ogni altro progetto di grafica. È in grado di soddisfare le esigenze di dilettanti e professionisti.

Come molti altri programmi Linux, The GIMP è sviluppato grazie alla collaborazione di sviluppatori di tutto il mondo che hanno offerto il loro tempo e le loro conoscenze per il progetto. Poiché il programma è in costante fase di sviluppo, la versione inclusa in SUSE LINUX potrebbe variare leggermente rispetto alla versione descritta qui. Soprattutto il layout delle singole finestre e sezioni di finestre è l'elemento che potrebbe differire.

The GIMP è un programma estremamente complesso. In questo capitolo vengono discussi solo alcune funzioni, strumenti e voci di menu. Per suggerimenti su dove trovare ulteriori informazioni sul programma, vedere la Sezione 17.6, «Ulteriori informazioni» (p. 254).

17.1 Formati grafici

Esistono due formati principali per la grafica, ovvero pixel e vettoriale. The GIMP funziona solo con grafica in pixel, che è il formato normale per fotografie e immagini di cui è stata eseguita la scansione. La grafica in pixel è costituita da piccoli blocchi di colore che insieme creano l'immagine intera. Le dimensioni dei file possono diventare

abbastanza grandi a causa di questo fattore. Non è altrettanto possibile aumentare le dimensioni di un'immagine in pixel senza perdere la qualità.

A differenza della grafica in pixel, nella grafica vettoriale non è possibile memorizzare informazioni per tutti i singoli pixel. Al contrario, vengono memorizzate informazioni sul modo in cui aree, righe e punti dell'immagine vengono raggruppati. Inoltre le immagini vettoriali possono essere ridotte in scala facilmente. L'applicazione grafica di OpenOffice.org, ad esempio, utilizza questo formato.

17.2 Avvio di GIMP

Avviare GIMP dal menu principale. In alternativa, immettere `gimp &` nella riga di comando.

17.2.1 Configurazione iniziale

Quando si avvia GIMP per la prima volta, viene visualizzata una procedura guidata che consente di eseguire la configurazione preliminare. Le impostazioni di default sono adatte per la maggior parte delle finalità. Fare clic su *Continua* in ogni finestra di dialogo, a meno che non si conoscano le impostazioni e si preferisca un'altra configurazione.

17.2.2 Finestre di default

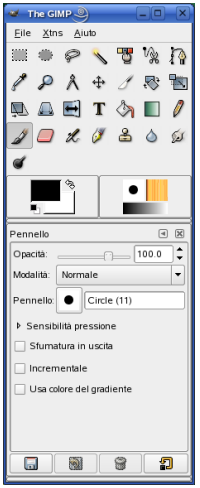
Tre finestre vengono visualizzate per default. Possono essere posizionate sullo schermo e, ad eccezione dell'area strumenti, chiuse in base alle proprie esigenze. La chiusura dell'area strumenti determina la chiusura dell'applicazione. Nella configurazione di default, GIMP salva il layout delle finestre quando si esce dal programma. Le finestre di dialogo lasciate aperte verranno visualizzate di nuovo al successivo avvio del programma.

Area strumenti

La finestra principale di GIMP, illustrata nella Figura 17.1, «Finestra principale» (p. 249), contiene i controlli principali dell'applicazione. La chiusura della finestra determina la chiusura dell'applicazione. Nella parte in alto, la barra dei menu offre l'accesso alla Guida, alle estensioni e alle funzioni dei file. Al di sotto, è possibile trovare le icone

dei diversi strumenti. Posizionare il puntatore del mouse su un'icona per visualizzare le relative informazioni.

Figura 17.1 *Finestra principale*



I colori di sfondo e in primo piano attuale vengono mostrati in due caselle sovrapposte. I colori di default sono nero per il primo piano e bianco per lo sfondo. Fare clic sulla casella per aprire la finestra di dialogo per la selezione del colore. Cambiare i colori di sfondo e in primo piano con il simbolo di freccia curva nella parte in altro a destra della caselle. Utilizzare il simbolo del bianco e del nero nella parte in basso a sinistra per ripristinare i colori di default.

A destra, vengono mostrati il pennello, il motivo e la sfumatura attuale. Fare clic sull'elemento visualizzato per accedere alla finestra di selezione. La parte inferiore della finestra contiene le opzioni di configurazione disponibili per lo strumento corrente.

Livelli, canali, percorsi e annullamento delle modifiche

Nella prima sezione, utilizzare la casella di riepilogo a discesa per selezionare l'immagine a cui si riferiscono le schede. Se si fa clic su *Automatico*, controllare se l'immagine attiva è scelta automaticamente. Per default, l'opzione *Automatico* viene abilitata.

L'opzione *Livelli* mostra i differenti livelli delle immagini attuali e può essere utilizzata per manipolarli. L'opzione *Canali* mostra i canali dei colori dell'immagine e consente di manipolarli.

I percorsi sono un metodo avanzato di selezione delle parti di un'immagine. Possono essere anche utilizzati per il disegno. L'opzione *Percorsi* mostra i percorsi disponibili per un'immagine e fornisce l'accesso alle funzioni dei percorsi. L'opzione *Annulla* mostra una cronologia limitata di modifiche apportate all'immagine attuale.

La parte inferiore della finestra contiene tre schede. Con queste, selezionare il pennello, il motivo e la sfumatura attuale.

17.3 Introduzione a GIMP

Sebbene GIMP possa sembrare complicato per i nuovi utenti, il suo utilizzo sarà reso più facile mediante l'acquisizione di alcune nozioni fondamentali. Le funzioni di base di GIMP sono la creazione, l'apertura e il salvataggio di immagini.

17.3.1 Creazione di una nuova immagine

Per creare una nuova immagine, selezionare *File (File)* → *New (Nuovo)* o premere Ctrl + N. Viene aperta una finestra di dialogo in cui definire le impostazioni per la nuova immagine. È possibile utilizzare *Da modello* per selezionare un modello su cui basare la nuova immagine. GIMP include alcuni modelli tra i quali è possibile scegliere che variano da fogli in formato A4 a copertine di CD. Per creare un modello personalizzato, selezionare *File* → *Finestre* → *Modelli...* e utilizzare i controlli offerti dalla finestra aperta.

Nella sezione *Dimensione immagine*, impostare la dimensione dell'immagine da creare in pixel o un'altra unità. Fare clic sull'unità per selezionare un'altra unità dall'elenco di unità disponibili. Il rapporto tra pixel e unità è impostato nella finestra *Resolution (Risoluzione)* che viene visualizzata quando si apre la sezione *(Advanced Options) Opzioni avanzate*. Una risoluzione di 72 pixel per pollice corrisponde alla visualizzazione dello schermo. È sufficiente per la grafica di pagine Web. Si deve utilizzare una risoluzione superiore per le immagini da stampare. Per la maggior parte delle stampanti, una risoluzione di 300 pixel per pollice produce una qualità accettabile.

In *Colorspace (Colorspace)*, scegliere se si desidera ottenere l'immagine a colori (*RGB*) o in gradazioni di grigio (*Grayscale*). Selezionare *Tipo di riempimento* per la nuova immagine. *Foreground Color (Colore primo piano)* e *Background Color (Colore di sfondo)* utilizzano i colori selezionati nella casella degli strumenti. L'opzione *Bianco* utilizza uno sfondo bianco nell'immagine. L'opzione *Trasparente* crea un'immagine trasparente. L'opzione *Transparency (Trasparenza)* è rappresentata da una scacchiera grigia. Immettere un commento per la nuova immagine in *Comment (Commento)*.

Se le impostazioni soddisfano le proprie esigenze, fare clic su *OK*. Per ripristinare la impostazioni di default, fare clic su *Reimposta*. Per interrompere la creazione di una nuova immagine, fare clic su *Annulla*.

17.3.2 Apertura di un'immagine esistente

Per aprire un'immagine esistente, selezionare *File (File)* → *Open (Apri)* o premere Ctrl + O. Nella finestra di dialogo visualizzata, selezionare il file desiderato. Fare clic su *OK* per aprire l'immagine selezionata. Fare clic su *Annulla* per ignorare l'apertura di un'immagine.

17.3.3 Finestra dell'immagine

L'immagine nuova o aperta in precedenza viene visualizzata nella relativa finestra. La barra dei menu nella parte superiore della finestra fornisce l'accesso a tutte le funzioni delle immagini. In alternativa, accedere al menu facendo clic con il pulsante destro del mouse sull'immagine oppure facendo clic sul piccolo pulsante freccia nell'angolo sinistro dei righelli.

Il menu *File (File)* offre le opzioni di file standard, ad esempio *Save (Salva)* e *Print (Stampa)*. *Chiudi* chiude l'immagine attuale. *Esci* chiude l'intera applicazione.

Le voci del menu *View (Visualizza)* consentono di controllare la visualizzazione delle immagini e la finestra delle immagini. *Nuova vista* apre una seconda finestra di visualizzazione dell'immagine attuale. Le modifiche apportate in una vista vengono applicate a tutte le altre viste di quell'immagine. Viste alternative sono utili per l'ingrandimento di una parte di un'immagine per la manipolazione durante la visualizzazione dell'immagine completa in un'altra vista. Regolare il livello di ingrandimento della finestra attuale con *Zoom*. Quando si seleziona *Giusto sulla finestra*,

la finestra dell'immagine viene ridimensionata in modo da adattarsi esattamente alla visualizzazione dell'immagine attuale.

17.4 Salvataggio delle immagini

Una delle funzioni più importanti per le immagini è la funzione *File (File) → Save (Salva)*. Si consiglia di salvare molto spesso. Scegliere *File (File) → Save as (Salva con nome)* per salvare le immagini con un nuovo nome di file. Si consiglia di salvare stadi di immagini con nomi differenti o eseguire backup in un'altra directory in modo da poter ripristinare facilmente uno stato precedente.

Quando si salva per la prima volta o si sceglie *Save as (Salva con nome)*, viene visualizzata una finestra di dialogo che consente di specificare il nome e il tipo di file. Immettere il nome del file nel campo situato nella parte superiore. Per *Save in folder (Salva nella cartella)*, selezionare la directory nella quale si desidera salvare il file da un elenco di directory normalmente utilizzate. Se si desidera utilizzare una directory diversa o crearne una nuova, aprire *Browse for other folders (Cerca altre cartelle)*. Si consiglia di lasciare l'opzione *Select File Type (Seleziona tipo file)* impostata su *By Extension (Per estensione)*. Con questa impostazione GIMP determina il tipo di file in base all'estensione associata al nome di file. I seguenti tipi di file sono utilizzati di frequente:

XCF
: È il formato nativo dell'applicazione. Consente di salvare tutte le informazioni sui percorsi e sui livelli insieme all'immagine stessa. Anche se è necessaria un'immagine in un altro formato, si consiglia in genere di salvare una copia in formato XCF per semplificare le future modifiche.

PAT
: È il formato utilizzato per gli schemi GIMP. Salvando un'immagine in questo formato, è possibile utilizzare l'immagine come schema di riempimento in GIMP.

JPG
: JPG o JPEG è un formato comune per fotografie e per la grafica di pagine Web senza la trasparenza. Il relativo metodo di compressione consente la riduzione delle dimensioni dei file, ma comporta anche la perdita di informazioni durante la compressione. Si consiglia di utilizzare l'opzione di anteprima durante la regolazione del livello di compressione. I livelli compresi tra 85% e 75% spesso determinano una qualità dell'immagine accettabile con una compressione ragionevole. Si consiglia

anche di salvare un backup in un formato che non comporti perdita di dati, ad esempio XCF. Se si modifica un'immagine, salvare solo l'immagine completata in formato JPG. Se si carica ripetutamente un file JPG e si salva, la qualità dell'immagine risulterà scarsa.

GIF
: Sebbene molto conosciuto in passato per la grafica con effetti di trasparenza, tale formato è oggi meno utilizzato per problemi di licenza. Il formato GIF viene utilizzato anche per immagini animate. Tale formato consente di salvare solo immagini *indicizzate*. Le dimensioni del file possono spesso risultare piccole solo se si utilizzano pochi colori.

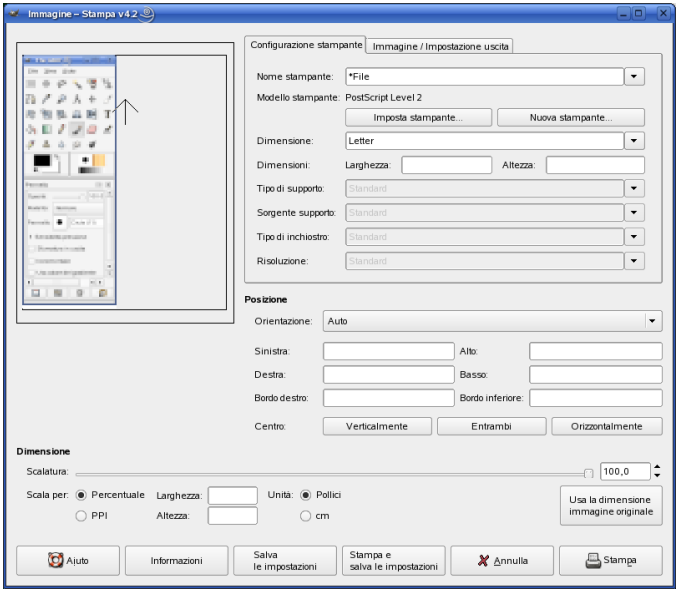
PNG
: Con il supporto per la trasparenza, la compressione senza perdita di dati, la disponibilità gratuita e il crescente supporto da parte dei browser, tale formato sta sostituendo il formato GIF nella grafica di pagine Web con effetti di trasparenza. Tra gli altri vantaggi, il formato PNG offre una trasparenza parziale, non disponibile con il formato GIF. Ciò consente di eseguire transizioni più uniformi dalle aree colorate a quelle trasparenti (*antialias*).

Per salvare l'immagine nel formato selezionato, premere *Save (Salva)*. Per interrompere l'operazione, fare clic su *Cancella*. Se l'immagine presenta caratteristiche che non possono essere salvate nel formato scelto, viene visualizzata una finestra di dialogo con le opzioni per la risoluzione del problema. Se si sceglie *Esporta*, se disponibile, in genere vengono forniti i risultati desiderati. Viene aperta una finestra con le opzioni del formato. Vengono forniti i valori di default appropriati.

17.5 Stampa di immagini

Per stampare un'immagine, scegliere *File (File)* → *Print (Stampa)* dal menu dell'immagine. Se la stampante è configurata in SUSE, verrà visualizzata nell'elenco. In alcuni casi, potrebbe essere necessario selezionare un driver appropriato con *Imposta stampante*. Selezionare il formato carta appropriato con *Media Size (Formato del supporto)* e il tipo in *Media Type (Tipo di supporto)*. Altre impostazioni sono disponibili nella scheda *Impostazioni di output/immagine*.

Figura 17.2 *Finestra di dialogo Stampa*



Nella parte inferiore della finestra, regolare le dimensioni dell'immagine. Fare clic su *Usa dimensioni originali* per ottenere le impostazioni dall'immagine stessa. Si consiglia di eseguire questa operazione se si imposta una risoluzione e una dimensione di stampa appropriate nell'immagine. Regolare la posizione dell'immagine nella pagina mediante i campi nella sezione *Position (Posizione)* oppure trascinando l'immagine nella sezione *Preview (Anteprima)*.

Se si è soddisfatti delle impostazioni, fare clic su *Stampa*. Per salvare le impostazioni per il futuro, utilizzare *Stampa e salva impostazioni*. L'opzione *Cancella* consente di interrompere la stampa.

17.6 Ulteriori informazioni

Di seguito sono elencate alcune risorse che possono essere utili per l'utente di GIMP. Purtroppo molte di queste risorse fanno riferimento a versioni precedenti.

- L'opzione *Aiuto* consente di accedere alla guida interna al sistema. Questa documentazione è disponibile anche nei formati HTML e PDF all'indirizzo `http://docs.gimp.org`.
- Il Gruppo utenti di GIMP offre informazioni in un sito Web interessante all'indirizzo `http://gug.sunsite.dk`.
- `http://www.gimp.org` è la home page ufficiale di GIMP.
- *Grokking the GIMP* scritto da Carey Bunks è un eccellente manuale su una versione precedente di GIMP. Sebbene alcuni aspetti dei programmi siano stati modificati, tale manuale rappresenta un'ottima guida alla manipolazione delle immagini. La versione in linea è disponibile all'indirizzo `http://gimp-savvy.com/BOOK/` .
- `http://gimp-print.sourceforge.net` è la pagina Web per il plug-in di stampa di GIMP. Il manuale dell'utente disponibile nel sito offre informazioni dettagliate per la configurazione e l'utilizzo del programma.

Parte VI. Mobilità

18 Informatica portatile e Linux

Nel presente capitolo viene fornita una panoramica sui vari aspetti relativi all'utilizzo di Linux per l'informatica portatile. Vengono brevemente introdotti i vari campi di applicazione e descritte le funzioni essenziali dell'hardware impiegato. Il contenuto copre anche le soluzioni software per requisiti e opzioni speciali per ottimizzare le prestazioni nonché i suggerimenti per ridurre al minimo il consumo energetico. Infine, una panoramica sulle più importanti fonti di informazioni sull'argomento chiude il capitolo.

La maggior parte degli utenti associa l'informatica portatile ai computer portatili, palmari e cellulari, e allo scambio di dati tra questi. Questo capitolo estende il concetto ai componenti hardware portatili, come i dischi rigidi esterni o le fotocamere, che possono essere collegati ai computer portatili o ai sistemi fissi.

18.1 Computer portatili

L'hardware dei computer portatili differisce da quello di un normale sistema fisso. Questo perché i criteri come l'interscambiabilità, lo spazio disponibile e il consumo energetico sono fattori importanti. I produttori di hardware portatili hanno sviluppato lo standard PCMCIA (Personal Computer Memory Card International Association). Questo standard copre le schede di memoria, le schede di rete, le schede ISDN e modem, e i dischi rigidi. La modalità di implementazione di tali hardware in Linux, i criteri da tenere presenti durante la configurazione, i software disponibili per il controllo del PCMCIA e la risoluzione dei possibili problemi sono descritti in Capitolo 19, *PCMCIA* (p. 269).

18.1.1 Risparmio energetico

L'inclusione nei computer portatili di componenti di sistema in grado di ottimizzare l'energia contribuisce a renderli adatti ad ambienti in cui la disponibilità di corrente è assente. Le funzioni di risparmio energetico sono importanti quanto quella del sistema operativo. SUSE Linux supporta vari metodi che influenzano il consumo di energia di un computer portatile e che incidono sul tempo di funzionamento durante l'alimentazione a batteria. Il seguente elenco descrive in ordine di importanza decrescente il contributo nei confronti del risparmio energetico:

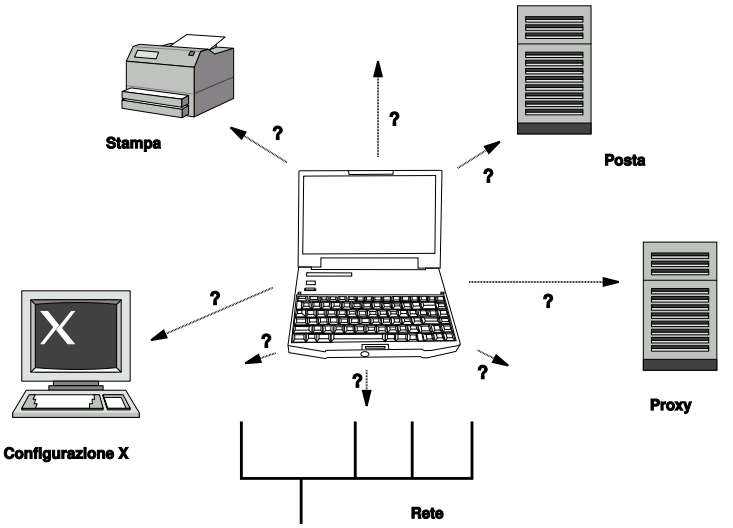
- Throttling della velocità della CPU
- Spegnimento dello schermo durante le pause
- Regolazione manuale della luminosità dello schermo
- Disconnessione di accessori hotplug (CD-ROM USB, mouse esterno, schede PCMCIA, ecc.) inutilizzati
- Arresto del disco rigido quando inattivo

Per informazioni nozionistiche sul risparmio energetico in SUSE Linux e sul funzionamento del modulo power management di YaST, vedere il Capitolo 21, *Risparmio energetico* (p. 283).

18.1.2 Integrazione e cambio dell'ambiente operativo

Il sistema deve sapersi adattare al cambio dell'ambiente operativo se utilizzato in un contesto di informatica portatile. Numerosi servizi dipendono dall'ambiente e i client sottostanti devono essere riconfigurati; operazione di cui si incarica SUSE Linux.

Figura 18.1 *Integrazione di un computer portatile in una rete*



I servizi interessati nel caso di un computer portatile impiegato sia in una rete domestica che in una aziendale sono:

Configurazione di rete
: Ciò include l'assegnazione di un indirizzo IP, risoluzione del nome, connettività Internet e connettività ad altre reti.

Stampa
: A seconda della rete, è necessario che sia presente un database aggiornato delle stampanti disponibili nonché un server di stampa.

E-mail e server proxy
: Analogamente alla stampa, anche in questo caso è necessario disporre dell'elenco aggiornato dei server corrispondenti.

Configurazione di X
: Se il computer portatile è temporaneamente collegato a un proiettore o schermo esterno, è necessario che siano disponibili le varie configurazioni di visualizzazione.

SUSE Linux offre due modi per integrare un computer portatile con ambienti operativi esistenti. È possibile avere una combinazione dei due.

SCPM
SCPM (system configuration profile management, ossia gestione del profilo di configurazione del sistema) consente di memorizzare stati di configurazione personalizzati di un sistema in una specie di «istantanea» detta *profilo*. È possibile avere un profilo per ogni singola situazione. I profili sono utili quando un sistema viene utilizzato in diversi ambienti (rete domestica, rete aziendale). È sempre possibile passare da un profilo all'altro. Per informazioni su SCPM, vedere il Capitolo 20, *System Configuration Profile Management* (p. 271). L'applet del kicker Selezionatore dei profili in KDE consente di cambiare profilo. Per cambiare profilo, è necessario immettere la parola d'ordine radice.

SLP
Il protocollo SLP (service location protocol) semplifica il collegamento di un computer portatile a una rete esistente. Senza SLP, l'amministratore di un computer portatile richiederebbe una conoscenza dettagliata dei servizi disponibili in una rete. Il protocollo SLP informa tutti i client della rete locale riguardo la disponibilità di un certo tipo di servizio. Le applicazioni che supportano SLP possono elaborare le informazioni diffuse da SLP e operare una configurazione automatica. SLP può anche essere utilizzato per l'installazione di un sistema e semplificare le ricerca di una fonte di installazione adatta. Informazioni dettagliate su SLP sono disponibili in Capitolo 39, *Servizi SLP in rete* (p. 639).

Il vantaggio di SCPM consiste nella capacità di abilitare e aggiornare condizioni di sistema riproducibili. SLP semplifica notevolmente la configurazione di un computer collegato in rete automatizzando gran parte delle operazioni.

18.1.3 Opzioni software

In ambito portatile esistono diverse aree di attività speciali gestite da software dedicati: monitoraggio del sistema (in particolare la carica della batteria), sincronizzazione dei dati e comunicazione wireless con periferiche e Internet. Le seguenti sezioni illustrano le più importanti applicazioni fornite da SUSE Linux per ciascuna attività.

Monitoraggio del sistema

SUSE Linux offre 2 strumenti KDE per il monitoraggio del sistema. La visualizzazione dello stato della batteria ricaricabile del computer è gestito dall'applet KPowersave nel kicker. Il monitoraggio complesso del sistema è garantito da KSysguard. In ambiente

GNOME, le funzioni descritte sono fornite da GNOME ACPI (come applet del pannello) e System Monitor.

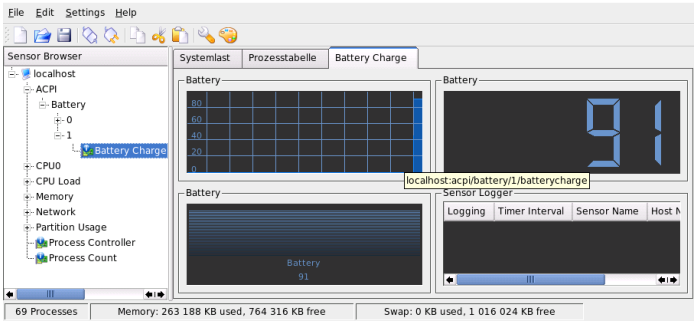
KPowersave

KPowersave è un applet che visualizza lo stato della batteria ricaricabile nel pannello di controllo. L'aspetto dell'icona varia a seconda del tipo di alimentazione. Con l'alimentazione a corrente alternata AC viene visualizzata una piccola spina. Con l'alimentazione a batteria l'icona assume l'aspetto di una batteria. Il menu corrispondente apre il modulo YaST di risparmio energetico dopo immissione della parola d'ordine radice. Questo menu consente di impostare il comportamento del sistema in diversi tipi di alimentazione. Per ulteriori informazioni sul risparmio energetico e il corrispondente modulo YaST, vedere il Capitolo 21, *Risparmio energetico* (p. 283).

KSysguard

KSysguard è un'applicazione indipendente che raccoglie tutti i parametri misurabili del sistema in un unico ambiente. Le funzioni di KSysguard includono il monitoraggio di: ACPI (stato della batteria), carico sulla CPU, rete, partizionamento e utilizzo della memoria. Vengono inoltre controllati e visualizzati tutti i processi del sistema. La presentazione e filtro dei dati raccolti possono essere personalizzati. È possibile monitorare diversi parametri di sistema in varie pagine di dati o raccogliere i dati di più computer collegati in rete. KSysguard può anche essere eseguito come daemon nei computer senza ambiente KDE. Per ulteriori informazioni su KSysguard, consultare la relativa guida o le pagine della guida di SUSE.

Figura 18.2 *Monitoraggio dello stato della batteria tramite KSysguard*



Sincronizzazione dei dati

Quando il lavoro dell'utente si svolge in parte su un computer portatile scollegato dalla rete e in parte sul computer dell'ufficio collegato alla rete aziendale, è necessario mantenere i dati elaborati sincronizzati in entrambi i contesti. Ciò include le cartelle delle e-mail, le directory e i singoli file che devono essere disponibili sia durante le trasferte che in ufficio. In entrambi i casi la soluzione è la seguente:

Sincronizzazione delle e-mail
: Nella rete aziendale le e-mail devono essere memorizzate in base a un account IMAP. Per accedere alle e-mail dalla postazione fissa, è possibile utilizzare qualsiasi client di e-mail abilitato per IMAP, come Mozilla Thunderbird Mail, Evolution o KMail in base a come descritto in *Start-Up*. Il client di e-mail deve essere configurato in modo che i `messaggi inviati` vengano memorizzati nella stessa cartella. Questo metodo garantisce la presenza di tutti i messaggi e dei relativi stati al termine della sincronizzazione. Per l'invio dei messaggi e per ottenere un riscontro affidabile dell'operazione, definire il server SMTP a livello del client di posta; evitare l'utilizzo di Postfix MTA in tutto il sistema o di Sendmail.

Sincronizzazione di file e directory
: Esistono numerose utility adatte alla sincronizzazione dei dati tra computer portatile e postazione fissa. Per ulteriori informazioni, vedere il Capitolo 47, *Sincronizzazione dei file* (p. 771).

Comunicazione wireless

Il collegamento tra computer portatile e rete domestica o aziendale può essere effettuato tramite un cavo oppure tramite una comunicazione senza fili; quest'ultimo metodo è valido anche per collegare il computer a periferiche, cellulari o PDA. Linux supporta 3 tipi di comunicazione wireless:

WLAN
: Grazie alla gamma più sviluppata per queste tecnologie, la soluzione WLAN è la più adatta per la costituzione di grandi reti in alcuni casi addirittura dislocate in ubicazioni non unite fisicamente. I singoli computer possono essere collegati gli uni agli altri per costituire una rete wireless indipendente o per accedere a Internet. I dispositivi detti punti di accesso fungono da emittenti di base per i dispositivi abilitati per WLAN e da intermediari per l'accesso a Internet. Un utente mobile può passare da un punto di accesso all'altro a seconda dell'ubicazione e del punto di

accesso più efficiente. Analogamente ai telefoni cellulari, gli utenti di una WLAN possono accedere a un'ampia rete senza doverlo fare da un'ubicazione specifica. Per informazioni dettagliate su WLAN, vedere la Sezione 22.1, «LAN wireless» (p. 309).

Bluetooth
Bluetooth offre lo spettro di applicazione più ampio per tutte le tecnologie wireless. Il metodo può essere utilizzato per le comunicazioni tra computer (portatili) e PDA o cellulari, analogamente al metodo a infrarossi IrDA. Viene utilizzata per collegare più computer presenti nello campo visivo. Bluetooth è anche utilizzato per collegare componenti di sistema wireless, come la tastiera o il mouse. La sua applicazione non consente tuttavia di collegare sistemi remoti a una rete. La tecnologia più adatta per collegare unità separate da ostacoli fisici rimane WLAN. Per ulteriori informazioni sull'utilizzo di Bluetooth e della sua configurazione, vedere la Sezione 22.2, «Bluetooth» (p. 320).

IrDA
IrDA è la tecnologia wireless che offre la copertura più ridotta. Entrambe le unità di comunicazione devono essere nello stesso campo visivo. Gli ostacoli come i muri non possono essere superati. Una possibile applicazione di IrDA è la trasmissione di un file da un computer portatile a un cellulare. Questo metodo è in grado di coprire la breve distanza che separa il computer portatile dal cellulare. Il trasporto a lunga distanza del file fino al destinatario è gestita dalla rete dalla rete mobile. Un'altra applicazione di IrDA è la trasmissione wireless dei lavori di stampa nell'ambito dell'ufficio. Per ulteriori informazioni su IrDA, vedere la Sezione 22.3, «Trasmissione dati a infrarossi» (p. 332).

18.1.4 Sicurezza dei dati

I dati nel computer portatile possono essere protetti contro gli accessi non autorizzati in più modi. Le possibili misure di sicurezza sono collegabili alle seguenti aree:

Protezione contro i furti
Ove possibile proteggere sempre fisicamente il sistema contro i furti. In commercio sono disponibili svariati strumenti di sicurezza come le catene.

Protezione dei dati nel sistema
I dati importanti devono essere cifrati sia durante la trasmissione che nel disco rigido. In questo modo ne viene assicurata la protezione in caso di furto. La creazione

di una partizione cifrata con SUSE Linux è descritta nella Sezione 23.3, «Cifratura di partizioni e file» (p. 354).

IMPORTANTE: Sicurezza dei dati e sospensione su disco

Durante un evento di sospensione su disco, le partizioni cifrate non vengono smontate. Di conseguenza, tutti i dati in queste partizioni rimangono accessibili da eventuali ladri in grado di riattivare il disco rigido.

Sicurezza della rete

Tutti i trasferimenti di dati devono essere protetti a ogni costo. Per informazioni sui problemi di sicurezza generali relativi a Linux e alle reti, vedere la Sezione 23.4, «Sicurezza e riservatezza» (p. 358). Le misure di sicurezza relative alle reti wireless sono disponibili in Capitolo 22, *Comunicazione wireless* (p. 309).

18.2 Hardware portatile

SUSE Linux supporta il rilevamento automatico dei dispositivi di memorizzazione portatili collegati alla porta Firewire (IEEE 1394) o USB. Il termine *dispositivo di memorizzazione portatile* si riferisce a tutti i dischi rigidi firewire o USB, unità flash USB o fotocamere digitali. Questi dispositivi vengono automaticamente rilevati e configurati tramite hotplug non appena vengono collegati all'interfaccia appropriata del sistema. I moduli subfs e submount garantiscono il montaggio dei dispositivi nelle corrispondenti posizioni nel file system. L'utente non deve impegnarsi in montaggi e smontaggi manuali come nelle precedenti versioni di SUSE Linux. Il dispositivo può essere semplicemente scollegato non appena cessano gli accessi dei programmi.

Dischi rigidi esterni (USB e Firewire)

Quando il sistema riconosce un disco rigido esterno, esso visualizza un'icona in *Il mio sistema* (KDE) o in *Computer* (GNOME) nell'elenco delle unità montate. Fare clic sull'icona per visualizzare il contenuto dell'unità. In questo ambito è possibile creare cartelle e file, modificarli o cancellarli. Per modificare il nome di un disco rigido attribuito dal sistema, fare clic con il pulsante destro del mouse e selezionare la voce di menu appropriata. La modifica del nome verrà solo visualizzata nel file manager. La modifica non incide sul descrittore tramite cui il dispositivo è montato in `/media/usb-xxx` o in `/media/ieee1394-xxx`.

Unità flash USB
: Questi dispositivi sono gestiti dal sistema come dischi rigidi esterni. Le corrispondenti voci che vengono visualizzate nel file manager possono essere rinominate.

Fotocamere digitali (USB e Firewire)
: Le fotocamere digitali riconosciute dal sistema vengono visualizzate come unità esterne nel file manager. KDE consente di leggere e accedere alle immagini tramite l'URL `camera:/`. Le immagini possono essere in seguito elaborate tramite Digikam o The GIMP. In ambiente GNOME, Nautilus visualizza le immagini nelle relative cartelle. L'elaborazione e la gestione di base delle immagini può essere svolta tramite f-spot. L'elaborazione avanzata delle foto può essere svolta tramite The GIMP. Per ulteriori informazioni su fotocamere digitali e gestione delle immagini, vedere il Capitolo 15, *Fotocamere digitali e Linux* (p. 217).

18.3 Cellulari e PDA

Tra un sistema fisso/computer portatile e un cellulare è possibile stabilire una comunicazione tramite via Bluetooth o IrDA. Alcuni modelli supportano entrambi i protocolli, altri uno solo. I campi di applicazione dei due protocolli e un'ampia documentazione sono descritti in sezione chiamata «Comunicazione wireless» (p. 264). Per la configurazione di questi protocolli nei cellulari, consultare la documentazione dei cellulari. Per la configurazione di questi protocolli in ambiente Linux, vedere la Sezione 22.2, «Bluetooth» (p. 320) e Sezione 22.3, «Trasmissione dati a infrarossi» (p. 332).

Il supporto per la sincronizzazione dei dati prodotto da Palm, Inc., è incorporato in Evolution e Kontact. In entrambi i casi, il primo collegamento con il dispositivo è facilitato grazie a una procedura guidata. Una volta configurato il supporto per Palm Pilot, è necessario identificare il tipo di dati da sincronizzare (indirizzi, appuntamenti, ecc.). Entrambe le applicazioni groupware sono descritte in *Start-Up*.

Il programma KPilot è integrato con Kontact ma è disponibile anche come utility autonoma. Per una descrizione del prodotto, vedere *Start-Up*. La sincronizzazione degli indirizzi può essere effettuata anche tramite KitchenSync.

18.4 Ulteriori informazioni

Per un riferimento centrale sulle problematiche riguardanti i dispositivi portatili e Linux, visitare la pagina all'indirizzo http://tuxmobil.org/. Svariate sezioni di questo sito Web trattano gli aspetti hardware e software di computer portatili, PDA, cellulari e altri hardware portatili.

Un approccio simile a quello presentato alla pagina http://tuxmobil.org/ è disponibile all'indirizzo http://www.linux-on-laptops.com/. Questo sito offre informazioni su computer portatili e palmari.

SUSE gestisce una lista di distribuzione in tedesco dedicata all'argomento dei computer portatili. Vedere http://lists.suse.com/archive/suse-laptop/. In questa lista, utenti e sviluppatori possono discutere tutti gli aspetti dell'informatica portatile in ambiente SUSE Linux. Esistono degli interventi in lingua inglese ma la maggior parte delle informazioni archiviate sono in tedesco.

In caso di problemi di risparmio energetico in ambiente SUSE Linux nei computer portatili, si consiglia di leggere il file README in /usr/share/doc/packages/powersave. Questa directory spesso contiene informazioni dell'ultimo minuto provenienti da tester e sviluppatori e che possono essere preziose per risolvere dei problemi.

19 PCMCIA

In questa sezione sono illustrati aspetti specifici dell'hardware e software PCMCIA relativi ai computer portatili. L'acronimo PCMCIA corrisponde a *Personal Computer Memory Card International Association* ed è un termine generale che si riferisce a tutto l'hardware e il software correlato.

19.1 Hardware

Il componente più importante è la scheda PCMCIA. Esistono due tipi di scheda PCMCIA:

PC Card
: Queste schede, introdotte sin dalle origini della tecnologia PCMCIA, utilizzano un bus a 16 bit per la trasmissione dei dati e hanno solitamente un costo contenuto. Alcuni bridge PCMCIA di ultima generazione hanno difficoltà a rilevare queste schede. Una volta rilevate, tuttavia, queste schede funzionano in genere correttamente e non causano problemi.

Schede CardBus
: Si tratta di uno standard più recente basato su bus a 32 bit che rende queste schede più veloci, ma anche più costose. Sono integrate nel sistema come le schede PCI e funzionano correttamente.

Il secondo componente importante è il controller PCMCIA o il bridge PC Card o CardBus, che stabilisce la connessione tra la scheda e il bus PCI. Sono supportati tutti

i modelli più comuni. Nel caso di un dispositivo PCI incorporato, il comando `lspci -vt` fornisce ulteriori informazioni.

19.2 Software

Con il kernel corrente, i bridge PCMCIA e le schede PCMCIA vengono gestite dal sottosistema hotplug. Esistono eventi `pcmcia_socket` per ogni bridge ed eventi `pcmcia`. udevd carica tutti i moduli necessari e chiama gli strumenti richiesti per configurare questi dispositivi. Queste azioni sono definite in `/etc/udev/rules.d/`.

`/etc/pcmcia/config.opts` è utilizzato per la configurazione delle risorse. Il driver necessario viene determinato in base alle tabelle del dispositivo nei driver. Informazioni sullo stato corrente dei socket e delle schede sono disponibili in `/sys/class/pcmcia_socket/` e tramite `pccardctl`.

A causa delle continue modifiche al sistema PCMCIA, questa documentazione risulta incompleta. Per una panoramica esaustiva, consultare `/usr/share/doc/packages/pcmciautils/README.SUSE`.

System Configuration Profile Management

20

Con l'ausilio di SCPM (system configuration profile management), è possibile adattare la configurazione del proprio computer ai vari ambienti operativi o configurazioni hardware. SCPM consente di gestire un insieme di profili di sistema per i vari scenari. SCPM consente di passare facilmente da un profilo di sistema a un altro, senza dover riconfigurare manualmente il sistema.

In alcune situazioni, è necessaria una configurazione del sistema modificata. È il caso di computer che devono essere in grado di funzionare in ubicazioni diverse. Se un sistema desktop dovesse temporaneamente funzionare utilizzando componenti hardware diversi da quelli consueti, SCPM diventa utile. Il ripristino della configurazione originale del sistema dovrebbe essere facile e la modifica della configurazione riproducibile. SCPM consente di tenere qualsiasi parte della configurazione del sistema in un profilo personalizzato.

Il principale campo di applicazione di SCPM è la configurazione di rete sui computer portatili. Per configurazioni di rete diverse, spesso, sono necessarie impostazioni diverse di altri servizi ad esempio la posta elettronica o i proxy. Seguono poi gli altri elementi, ad esempio stampanti diverse a casa e in ufficio, una configurazione personalizzata del server X per i proiettori multimediali durante le conferenze, speciali impostazioni per il risparmio di energia quando si è in viaggio, o un fuso orario diverso se ci si trova presso una filiale oltreoceano.

20.1 Terminologia

Qui di seguito sono riportati alcuni termini utilizzati nella documentazione di SCPM e nel modulo YaST.

- Il termine *configurazione del sistema* si riferisce alla configurazione completa del computer. Comprende tutte le impostazioni principali, come l'utilizzo delle partizioni del disco rigido, le impostazioni di rete, la selezione del fuso orario e le mappature della tastiera.

- Un *profilo*, chiamato anche*profilo di configurazione*, è uno stato che è stato mantenuto e può essere ripristinato in qualsiasi momento.

- *Profilo attivo* si riferisce al profilo selezionato come ultimo. Questo non significa che la configurazione corrente del sistema non corrisponda esattamente a questo profilo, perchè la configurazione può essere modificata in qualsiasi momento.

- Una *risorsa*, nel contesto SCPM, è un elemento che contribuisce alla configurazione del sistema. Può essere un file o un collegamento temporaneo comprendente metadati (come l'utente), permessi od ore di accesso. Può anche essere un servizio del sistema a eseguire questo profilo che, però, non è attivato su un altro sistema.

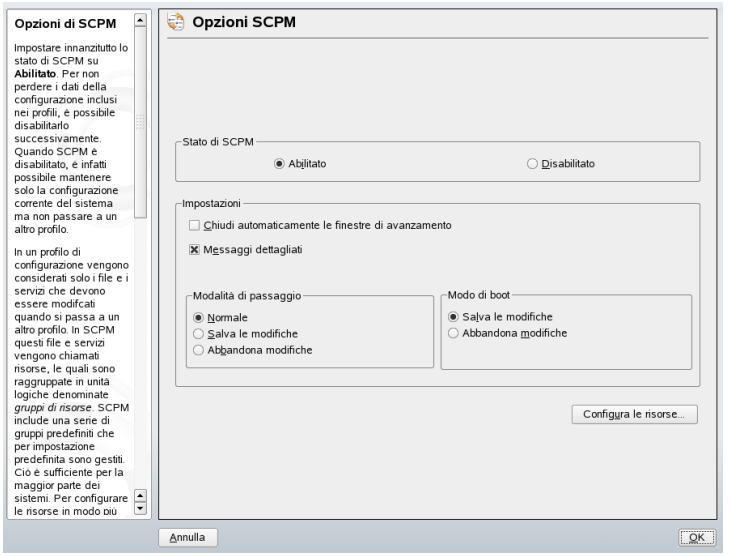
- Ogni risorsa appartiene a un certo *gruppo di risorse*. Questi gruppi contengono tutte le risorse che, logicamente, devono rimanere insieme—la maggior parte dei gruppi conterrà sia il servizio, sia i file di configurazione ad esso relativi. È molto facile riunire le risorse gestite da SCPM perchè non è necessaria alcuna conoscenza dei file di configurazione del servizio desiderato. SCPM viene fornito con una selezione di gruppi di risorse preconfigurati che, nella maggior parte dei casi, dovrebbero essere sufficienti.

20.2 Utilizzo del Manager profili YaST

Avviare il manager profili YaST dal centro di controllo YaST con *Sistema* → *Manager profili*. Al primo avvio, abilitare esplicitamente SCPM selezionando *Abilitato*nella finestra di dialogo *Opzioni SCPM* rappresentata in Figura 20.1, «Opzioni SCPM YaST» (p. 273). In *Impostazioni*, indicare se le pop-up di avanzamento devono essere chiuse

automaticamente e devono essere visualizzati i messaggi verbose circa l'avanzamento della configurazione di SCPM. In *Modalità modifica*, definire se le risorse modificate del profilo attivo devono essere salvate o scartate quando il profilo viene modificato. Se la *Modalità modifica*è impostata su*Normale*, tutte le modifiche nel profilo attivo vengono salvate quando il profilo viene modificato. Per definire il comportamento di SCPM all'avvio, impostare *Modalità di avvio* su *Salva modifiche* (impostazione predefinita) *Rilascia modifiche*.

Figura 20.1 *Opzioni SCPM YaST*

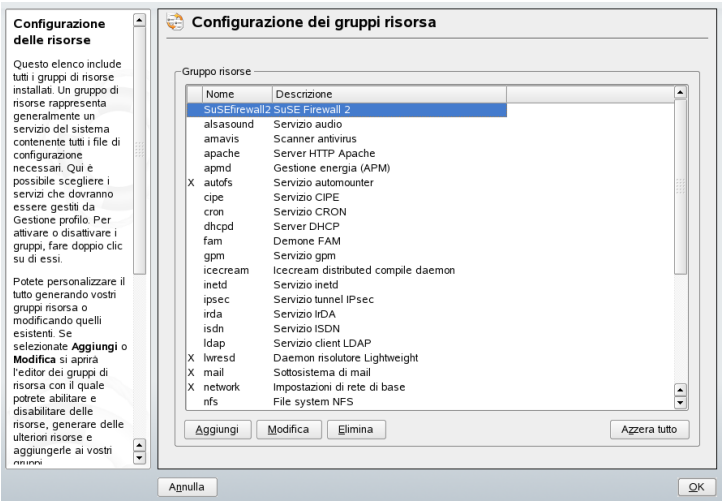


20.2.1 Configurazione dei gruppi di risorse

Per apportare modifiche alla configurazione delle risorse correnti, selezionare *Configura risorse* nella finestra di dialogo *Opzioni SCPM*. Nella finestra di dialogo successiva, rappresentata in Figura 20.2, «Configurazione dei gruppi di risorse» (p. 274), è riportata una lista di tutti i gruppi di risorse disponibili sul sistema. Per aggiungere o modificare un gruppo di risorse, indicare o modificare*Gruppo risorse* e *Descrizione*. Per un servizio LDAP, ad esempio, immettere `ldap` come *Gruppo risorse* e `Client service LDAP` come *Descrizione*. Immettere quindi le risorse appropriate (servizi, file di configurazione, o entrambe) oppure modificare quelle esistenti. Cancellare le risorse che non sono utilizzate. Per ripristinare lo stato delle risorse selezionate—scartare tutte

le modifiche apportate e tornare ai valori di configurazione—selezionare *Ripristina gruppo*. Le modifiche apportate vengono salvate nel profilo attivo.

Figura 20.2 *Configurazione dei gruppi di risorse*

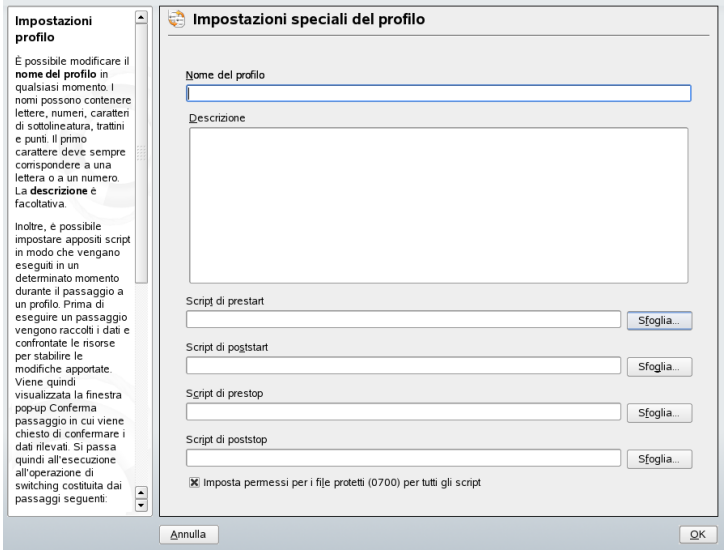


20.2.2 Creazione di un nuovo profilo

Per creare un nuovo profilo, cliccare su *Aggiungi* nella finestra di dialogo iniziale (*System Configuration Profile Management*). Nella finestra che si apre, indicare se il nuovo profilo deve essere basato sulla configurazione corrente del sistema (SCPM recupera automaticamente la configurazione corrente e la scrive nel profilo) o su un profilo esistente. Se si utilizza la configurazione corrente del sistema come base per il nuovo profilo, è possibile contrassegnare il nuovo profilo come nuovo profilo attivo. In questo modo non vengono apportate modifiche al vecchio profilo e non vengono avviati o interrotti servizi.

Fornire un nome e una breve descrizione per il nuovo profilo nella finestra di dialogo seguente. Per l'esecuzione da parte di SCPM di script speciali su una modifica di profili, immettere i percorsi a ciascun eseguibile (vedere la Figura 20.3, «Impostazioni speciali del profilo» (p. 275)). Per ulteriori informazioni consultare Sezione 20.3.4, «Impostazioni avanzate dei profili» (p. 279). SCPM consente di eseguire un controllo per le risorse del nuovo profilo. Una volta terminata questa prova con esito positivo, il nuovo profilo è pronto per l'uso.

Figura 20.3 *Impostazioni speciali del profilo*



20.2.3 Modifica dei profili esistenti

Per modificare un profilo esistente, selezionare *Modifica* nella finestra di dialogo iniziale (*System Configuration Profile Management*). Quindi modificare il nome, la descrizione, gli script e le risorse in base alle proprie esigenze.

20.2.4 Passaggio da un profilo all'altro

Per passare da un profilo all'altro, aprire manager profili. Il profilo attivo è contrassegnato da una freccia. Selezionare il profilo al quale passare e cliccare su*Passa a*. SCPM consente di controllare le nuove risorse o quelle modificate e, se necessario, di aggiungerle.

Se una risorsa è stata modificata, in YaST si apre la finestra di dialogo *Conferma passaggio*. In *Gruppi risorse modificate del profilo attivo* sono elencati tutti i gruppi di risorse del profilo attivo che sono stati modificati, ma non ancora salvati nel profilo attivo. In*Salva o Ignora* per il gruppo di risorse attualmente selezionato è possibile indicare se le modifiche a questo gruppo di risorse devono essere salvata nel profilo

attivo o scartate. In alternativa, selezionare ogni risorsa e fare clic su *Dettagli* per analizzare le modifiche in modo dettagliato. In Dettagli, appare una una lista di tutti i file di configurazione o eseguibili appartenenti al gruppo di risorse che sono state modificate. Per un confronto riga per riga della vecchia versione con quella nuova, cliccare su *Mostra modifiche*. Dopo aver analizzato le modifiche, decidere cis fare in *Azione*:

Salva risorsa
Consente di salvare questa risorsa nel profilo attivo lasciando tutti gli altri profili intatti.

Ignora risorsa
Consente di lasciare la risorsa attiva intatta. Questa modifica è scartata.

Salva su tutti i profili
Consente di copiare l'intera configurazione di questa risorsa in tutti gli altri profili.

Patch per tutti i profili
Consente di applicare solo le modifiche più recenti a tutti i profili.

Salva o Ignora tutto consente di salvare o di scartare le modifiche di tutte le risorse che appaiono in questa finestra di dialogo.

Dopo aver confermato le modifiche al profilo attivo, uscire dalla finestra di dialogo *Conferma passaggio* facendo clic su *OK*. SCPM passa poi al nuovo profilo. Durante il passaggio, vengono eseguiti script di prearresto e di postarresto del vecchio profilo e script di preavvio e di postavvio per quello nuovo.

20.3 Configurazione di SCPM utilizzando la riga di comando

In questa sezione viene presentata la configurazione di SCPM utilizzando la riga di comando. Viene descritto il modo in cui avviare, configurare la riga di comando e lavorare con i profili.

20.3.1 Avvio di SCPM e definizione dei gruppi di risorse

SCPM deve essere attivato prima dell'uso. È possibile attivarlo con `scpm enable` . Quando viene eseguito per la prima volta, SCPM viene inizializzato, operazione che richiede qualche secondo. Disattivare SCPM con `scpm disable` in qualsiasi momento per evitare un involontario cambiamento ai profili. Una successiva riattivaziione, consente semplicemente di riprendere l'inizializzazione.

Come impostazione predefinita, SCPM gestisce le impostazioni di rete e della stampante nonchè la configurazione di X.Org. Per la gestione di servizi speciali o di file di configurazione, attivare i rispettivi gruppi di risorse. Per elencare i gruppi di risorse predefiniti, utilizzare `scpm list_groups` . Per vedere solo i gruppi già attivati, utilizzare `scpm list_groups -a` . Emettere questi comandi come `root` sulla riga di comando.

```
scpm list_groups -a

nis                 Network Information Service client
mail                Mail subsystem
ntpd                Network Time Protocol daemon
xf86                X Server settings
autofs              Automounter service
network             Basic network settings
printer             Printer settings
```

Attivare o disattivare un gruppo con `scpm activate_group NAME` o`scpm deactivate_group NAME` . Sostituire`NOME` con il relativo nome gruppo.

20.3.2 Creazione e gestione dei profili

Un profilo chiamato `predefinito` esiste già dopo l'attivazione di SCPM. Con`scpm list` è possibile ottenere una lista dei profili disponibili. L'unico profilo esistente è anche quello attivo, che può essere verificato con`scpm active` . Il profilo `predefinito`è una configurazione principale dalla quale derivano gli altri profili. Per questa ragione, tutte le impostazioni che devono essere identiche in tutti i profili, devono essere immesse per prime. Quindi salvare queste modifiche nel profilo attivo con`scpm reload` . Il profilo `predefinito` può essere copiato e rinominato come base per nuovi profili.

Esistono due modi per aggiungere un profilo. Se il nuovo profilo (chiamato `lavoro`) deve essere creato sulla base del profilo `predefinito`, crearlo con `scpm copy default work` . Il comando `scpm switch work` consente di passare al nuovo profilo che può essere modificato. È possibile modificare la configurazione del sistema per fini speciali e salvare le modifiche in un nuovo profilo. Il comando `scpm add work` consente di creare un nuovo profilo salvando la configurazione del sistema corrente nel profilo`work` contrassegnandola come attiva. L'esecuzione del comando `scpm reload` consente di salvare le modifiche al profilo `lavoro`.

È possibile rinominare o cancellare i profili con i comandi `scpm rename x y` e `scpm delete z` . Ad esempio, per rinominare`lavoro` con `progetto`, immettere `scpm rename work project` . Per cancellare `progetto`, immettere `scpm delete project` . impossibile eliminare il profilo attivo

20.3.3 Modifica ai profili di configurazione

Il comando `scpm switch work` passa a un altro profilo (il profilo `lavoro`, in questo caso). Passare al profilo attivo per inserire nel profilo le impostazioni modificate della configurazione del sistema. Questa operazione corrisponde al comando`scpm reload` .

Quando si modificano i profili SCPM consente in primo luogo di controllare quali risorse del profilo attivo sono state modificate. Effettua poi delle interrogazioni per sapere se le modifiche a ciascuna risorsa devono essere aggiunte al profilo attivo o rilasciate. Se si preferisce una lista separata delle risorse, (come nelle precedenti versioni di SCPM), utilizzare il comando switch con il parametro `–r`: `scpm switch –r work` .

```
scpm switch –r work.

Controllo delle risorse modificate
Controllo delle risorse da avviare/chiudere
Controllo delle dipendenze
Ripristino del profilo predefinito
```

SCPM confronta poi la configurazione attuale del sistema con il profilo al quale passare. In questa fase, SCPM valuta quali servizi di sistema devono essere fermati o riavviati a causa delle reciproche dipendenze o per rispecchiare le modifiche all'interno della configurazione. Questa fase è analoga a un riavvio parziale del sistema che riguarda solo una piccola parte di esso mentre il resto continua a funzionare senza modifiche.

Solo a questo punto i servizi di sistema vengono fermati, vengono scritte tutte le risorse modificate come i file di configurazione e i servizi di sistema riavviati.

20.3.4 Impostazioni avanzate dei profili

È possibile inserire una descrizione per ogni profilo che viene visualizzato con `scpm list` . Per il profilo attivo, impostarla con`scpm set description "text"` . Fornire il nome del profilo per i profili non attivi, ad esempio, `scpm set description "text" work` . A volte, durante la modifica dei profili, potrebbe essere utile eseguire altre operaizoni che non sono previste da SCPM. Allegare fino a quattro eseguibili per ciascun profilo. Vengono invocati in fasi diverse del processo di modifica. Queste fasi vengono chiamate:

Prearresto
: prima di fermare i servizi quando si esce dal profilo

Postarresto
: dopo aver fermato i servizi quando si esce dal profilo

Preavvio
: prima di avviare i servizi quando si attiva il profilo

Postavvio
: dopo aver avviato i servizi quando si attivano i profili

Inserire queste azioni con il comando `set` immettendo `scpm set prestop filename` , `scpm set poststop filename` , `scpm set prestart filename` , o`scpm set poststart filename` . Gli script devono essere eseguibili e fare riferimento al giusto interprete.

AVVERTIMENTO: Integrazione di uno script personalizzato

Altri script che devono essere eseguiti da SCPM devono essere leggibili ed eseguibili per il superutente (`root`). L'accesso a questi file deve essere bloccato per tutti gli altri utenti. Immettere i comandi `chmod 700 filename` e `chown root:root filename` per dare a `root` permessi di accesso esclusivi ai file.

Interrogare tutte le altre impostazioni immesse con `set` e con `get`. Il comando `scpm get poststart` , ad esempio, restituisce il nome della chiamata del postavvio o semplicemente nulla se non è stato allegato nulla. Ripristinare queste impostazioni sovrascrivendole con `""`. Il comando `scpm set prestop ""` rimuove il programma di prearresto allegato.

Tutti i comandi`set` e `get` possono essere applicati a un profilo arbitrario nello stesso modo in cui si aggiungono i commenti. Ad esempio, `scpm get prestop filename work` o `scpm get prestop work .`

20.4 Utilizzo della Applet Profile Chooser

La applet Profile Chooser sul riquadro del desktop GNOME o KDE consente di controllare facilmente le impostazioni di SCPM. Creare, modificare o cancellare i profili tramite YaST come descritto nella Sezione 20.2, «Utilizzo del Manager profili YaST» (p. 272) e in modifica profili. La modifica ai profili può essere effettuata da un normale utente a condizione che l'amministratore del sistema lo consenta. Avviare Profile Chooser from dal menu del desktop con *Sistema → Desktop Applet → Profile Chooser*.

Abilitare i normali utenti a modificare i profili cliccando con il pulsante destro del mouse sull'icona di Profile Chooser sul riquadro del desktop e selezionando*Consenti modifica all'utente* dal menu che si apre. Fornire la parola d'ordine del root. D'ora in poi, qualsiasi utente autorizzato presente sul sisema può modificare i profili.

Tutti i profili configurati in YaST, direttamente tramite una chiamata a YaST o tramite *Avvia modulo profile manager YaST2* vengono visualizzati dopo aver cliccato sull'icona di Profile Chooser. Selezionare il profilo da modificare utilizzando i tasti del cursore, in questo modo SCPM passerà automaticamente al nuovo profilo.

20.5 Soluzione dei problemi

Questa sezione descrive i problemi frequentemente incontrati con SCPM. Consente di capire come sorgono e come è possibile risolverli.

20.5.1 Arresto durante il processo di modifica

A volte SCPM si ferma durante una procedura di modifica. Questo fatto potrebbe essere provocato da effetti esterni, ad esempio un'interruzione da parte dell'utente, mancanza di corrente, o perfino da un errore in SCPM. Se si verifica questo problema, viene visualizzato un messaggio per annunciare che SCPM è bloccato all'avvio successivo. Questo per la sicurezza del sistema, perchè i dati memorizzati nel database possono essere differenti rispetto allo stato del sistema. Per risolvere questo problema, eseguire `scpm recover` . In questo modo SCPM eseguirà tutte le operazioni mancanti della precedente esecuzione. È anche possibile eseguire`scpm recover -b` , che cerca di annullare tutte le operazioni già effettuate durante l'esecuzione precedente. Se si utilizza il manager profili YaST, all'avvio appare una finestra di dialogo che consente di eseguire i comandi descritti sopra.

20.5.2 Modifica della configurazione del gruppo risorse

Per modificare la configurazione del gruppo risorse quando SCPM è già inizializzato, immettere `scpm rebuild` dopo aver aggiunto o rimosso gruppi. In questo modo le nuove risorse vengono aggiunte a tutti i profili e quelle rimosse vengono cancellate in modo permanente. Se le risorse cancellate sono configurate in modo diverso all'interno dei vari profili, questi dati di configurazione vanno persi, eccetto la versione corrente all'interno del sistema che SCPM non tocca. Se si modifica la configurazione con YaST, non si deve immettere il comando rebuild perchè è gestito da YaST.

20.6 Selezione di un profilo all'avvio del sistema

Per selezionare un profilo all'avvio del sistema, premere F3 nella videata di avvio per accedere a una lista di profili disponibili. Utilizzare i tasti freccia per selezionare un profilo e confermare la selezione con Invio. Il profilo selezionato viene poi utilizzato come opzione di avvio.

20.7 Per ulteriori informazioni

La documentazione più recente è disponibile sulle pagine info di SCPM (info scpm). Le informazioni per gli sviluppatori sono disponibili in `/usr/share/doc/packages/scpm`.

21 Risparmio energetico

Il risparmio energetico è particolarmente importante sui computer portatili ma risulta utile anche su altri sistemi. Sono disponibili due tecnologie: APM (advanced power management) e ACPI (advanced configuration and power interface). È inoltre possibile controllare la scala di frequenza della CPU per risparmiare energia o ridurre il rumore. È possibile configurare queste opzioni manualmente oppure utilizzando un modulo speciale di YaST.

A differenza di APM, utilizzato in precedenza sui computer portatili soltanto per il risparmio energetico, lo strumento di configurazione e di informazioni hardware ACPI è disponibile su tutti i computer moderni (computer portatili, desktop e server). Tutte le tecnologie di risparmio energetico richiedono hardware adeguato e routine BIOS. La maggior parte dei computer portatili e molti desktop e server moderni soddisfano questi requisiti.

APM è stato utilizzato in molti computer precedenti. Poiché APM è costituito principalmente da un set di funzioni implementate nel BIOS, il livello del supporto APM può variare a seconda dell'hardware. Ciò si verifica a maggior ragione con ACPI che è anche più complesso. Per questo motivo, è praticamente impossibile consigliare l'uno piuttosto che l'altro. È sufficiente verificare le diverse procedure sul proprio hardware e quindi selezionare la tecnologia che viene meglio supportata.

IMPORTANTE: Risparmio energetico per i processori AMD64

I processori AMD64 con kernel a 64 bit supportano soltanto ACPI.

21.1 Funzioni di risparmio energetico

Le funzioni di risparmio energetico sono importanti non solo per l'utilizzo dei computer portatili ma anche per i desktop. Le funzioni principali e il relativo utilizzo nei sistemi di risparmio energetico APM e ACPI sono:

Stand-by
Questa modalità di funzionamento spegne il monitor. Su alcuni computer, la prestazione del processore è sottoposta a throttling, funzione non disponibile in tutte le implementazioni di APM, che corrisponde allo stato S1 o S2 di ACPI.

Sospensione (salvataggio stato su memoria)
Questa modalità scrive lo stato dell'intero sistema nella RAM. Di conseguenza, l'intero sistema eccetto la RAM viene messo nello stato sleep. In questo stato, il computer consuma pochissima energia con il vantaggio che è possibile riprendere il lavoro allo stesso punto in pochi secondi senza dover eseguire il processo di avvio o riavviare le applicazioni. Di norma è possibile sospendere i dispositivi che utilizzano APM abbassando lo schermo e attivarli aprendolo. Questa funzione corrisponde allo stato S3 di ACPI. Il supporto di questo stato è ancora in fase di sviluppo quindi dipende essenzialmente dall'hardware.

Sospensione (salvataggio stato su disco)
In questa modalità di funzionamento, lo stato dell'intero sistema viene scritto sul disco rigido e il sistema viene disattivato. La riattivazione da questo stato impiega da 30 a 90 secondi. Viene ripristinato lo stato precedente alla sospensione. Alcuni produttori offrono utili varianti ibride di questa modalità, ad esempio RediSafe negli IBM Thinkpad. Lo stato corrispondente di ACPI è S4. In Linux, il salvataggio dello stato su disco viene eseguito da routine del kernel indipendenti da APM e ACPI.

Monitor della batteria
ACPI e APM verificano lo stato di carica della batteria e forniscono le relative informazioni. Entrambi i sistemi coordinano inoltre le azioni da eseguire quando si raggiunge uno stato di carica critico.

Power off automatico
Dopo lo shutdown, il computer viene disattivato. Ciò risulta particolarmente importante quando viene eseguito lo shutdown automatico poco prima che la batteria si scarichi.

Shutdown dei componenti del sistema
La disattivazione del disco rigido è l'unico aspetto più importante del risparmio energetico potenziale dell'intero sistema. A seconda dell'affidabilità dell'intero sistema, è possibile mettere il disco rigido nello stato sleep per un certo periodo di tempo. Il rischio di perdere dati aumenta tuttavia con la durata dei periodi nello stato sleep. È possibile disattivare gli altri componenti tramite ACPI (almeno in teoria) oppure in modo permanente nella configurazione del BIOS.

Controllo della velocità del processore
Con la CPU, è possibile risparmiare energia in tre modi diversi: adattamento della frequenza/tensione (definito anche PowerNow! oppure Speedstep), throttling e stato sleep del processore (stato C). È possibile anche combinare questi tre metodi a seconda della modalità di funzionamento del computer.

21.2 APM

Alcune funzioni di risparmio energetico vengono eseguite dall'APM BIOS stesso. In molti computer portatili, gli stati di stand-by e di sospensione si possono attivare con combinazioni di tasti oppure abbassando lo schermo senza bisogno di una funzione speciale del sistema operativo. Per attivare queste modalità con un comando, è necessario tuttavia avviare alcune azioni prima di sospendere il sistema. Per visualizzare il livello di carica della batteria, sono necessari pacchetti di programmi speciali e un kernel appropriato.

I kernel di SUSE Linux dispongono di un supporto APM integrato. APM viene attivato solo se ACPI non è implementato nel BIOS e viene rilevato un APM BIOS. Per attivare il supporto APM, è necessario che ACPI sia disabilitato con `acpi=off` al prompt di avvio. Digitare `cat /proc/apm` per verificare che APM sia attivo. Un output costituito da diversi numeri indica che tutto è OK. Ora è possibile spegnere il computer con il comando `shutdown -h` .

Le implementazioni BIOS che non sono completamente conformi agli standard possono causare problemi con APM. È possibile aggirare alcuni problemi con parametri speciali di avvio. Tutti i parametri vengono immessi al prompt di avvio nella forma `apm=parameter`:

on oppure off
Attivazione o disattivazione del supporto APM.

(no-)allow-ints
Consentire le interruzioni durante l'esecuzione delle funzioni del BIOS.

(no-)broken-psr
La funzione «GetPowerStatus» del BIOS non funziona correttamente.

(no-)realmode-power-off
Consente di reimpostare il processore nella modalità reale prima dello shutdown.

(no-)debug
Consente la registrazione degli eventi APM nel log di sistema.

(no-)power-off
Consente di disattivare il sistema dopo lo shutdown.

bounce-interval=*n*
Il tempo in centesimi di secondo dopo un evento di sospensione durante il quale vengono ignorati eventi aggiuntivi di sospensione.

idle-threshold=*n*
Percentuale di inattività del sistema con cui viene eseguita la funzione del BIOS `idle` (0=sempre, 100=mai).

idle-period=*n*
Il tempo in centesimi di secondo con cui viene misurata l'attività del sistema.

Il daemon APM (apmd) non viene più utilizzato. Questa funzionalità viene ora gestita dal nuovo comando powersaved che supporta anche ACPI e l'adattamento della frequenza della CPU.

21.3 ACPI

ACPI (advanced configuration and power interface) è stato progettato per abilitare il sistema operativo per la configurazione e il controllo dei singoli componenti hardware. ACPI sostituisce sia PnP che APM. Fornisce informazioni sulla batteria, l'adattatore CA, la temperatura, la ventola e gli eventi del sistema, ad esempio «chiusura schermo» o «batteria scarica».

Il BIOS fornisce tabelle contenenti informazioni sui metodi di accesso dei singoli componenti e dell'hardware. Il sistema operativo utilizza queste informazioni per compiti quali l'assegnazione di interruzioni o l'attivazione e la disattivazione dei componenti. Poiché il sistema operativo esegue comandi memorizzati nel BIOS, la funzionalità dipende dall'implementazione del BIOS. Le tabelle che ACPI è in grado di rilevare e caricare sono riportate in `/var/log/boot.msg`. Per ulteriori informazioni sulla risoluzione dei problemi relativi a ACPI, vedere la Sezione 21.3.4, «Risoluzione dei problemi» (p. 292).

21.3.1 ACPI in azione

Se il kernel rileva un ACPI BIOS all'avvio del sistema, ACPI viene attivato automaticamente e viene disattivato APM. Per alcuni computer meno recenti potrebbe essere necessario il parametro di avvio `acpi=force`. Il computer deve supportare ACPI 2.0 o versioni successive. Verificare i messaggi di avvio del kernel in `/var/log/boot.msg` per controllare che ACPI sia stato attivato.

È necessario poi caricare diversi moduli con lo script di avvio del daemon powersave. Se uno di questi moduli crea problemi, è possibile escluderlo dal caricamento o dallo scaricamento in `/etc/sysconfig/powersave/common`. Il log di sistema (`/var/log/messages`) contiene i messaggi dei moduli che consentono di controllare quali componenti sono stati rilevati.

`/proc/acpi` ora contiene diversi file che forniscono informazioni sullo stato del sistema o che possono essere utilizzate per modificare qualcuno di questi stati. Alcune funzionalità non sono ancora attive poiché sono ancora in fase di sviluppo e il supporto di alcune funzioni dipende essenzialmente dall'implementazione del produttore.

È possibile leggere tutti i file (eccetto `dsdt` e `fadt`) con il commando `cat`. In alcuni file, è possibile modificare le impostazioni con il commando `echo`, ad esempio, `echo X > file` per specificare i valori appropriati per X. Si consiglia di utilizzare sempre il comando `powersave` per accedere a queste informazioni e alle opzioni di controllo. Di seguito vengono descritti i file più importanti:

`/proc/acpi/info`
: Informazioni generali su ACPI.

/proc/acpi/alarm
Specificare quando il sistema deve riattivarsi dopo lo stato sleep. Questa funzionalità non è al momento completamente supportata.

/proc/acpi/sleep
Fornisce informazioni sui possibili stati sleep.

/proc/acpi/event
Tutti gli eventi sono riportati in questo file e vengono elaborati dal daemon Powersave (`powersaved`). Se nessun daemon è in grado di accedere a questo file, gli eventi, quali ad esempio un breve clic sul pulsante Power o la chiusura dello schermo, possono essere letti con il comando `cat /proc/acpi/event` (terminare con Ctrl + C).

/proc/acpi/dsdt e /proc/acpi/fadt
Questi file contengono le tabelle ACPI: DSDT (differentiated system description table) e FADT (fixed ACPI description table) che si possono leggere con i comandi `acpidmp`, `acpidisasm` e `dmdecode`. Questi programmi e la relativa documentazione si trovano nel pacchetto `pmtools`. Ad esempio, `acpidmp DSDT | acpidisasm .`

/proc/acpi/ac_adapter/AC/state
Indica se l'adattatore CA è connesso.

/proc/acpi/battery/BAT*/{alarm,info,state}
Informazioni dettagliate sullo stato della batteria. Il livello di carica viene letto mettendo a confronto l'`ultima piena capacità` indicata nelle `informazioni` con la `capacità rimanente` indicata nello `stato`. Per una più comoda consultazione, utilizzare uno dei programmi speciali introdotti in Sezione 21.3.3, «Strumenti di ACPI» (p. 292). In `avviso` è possibile specificare il livello di carica in cui viene attivato un evento della batteria.

/proc/acpi/button
In questa directory sono contenute le informazioni sui vari comandi.

/proc/acpi/fan/FAN/state
Indica se la ventola è correntemente attiva. Per attivare o disattivare la ventola manualmente, scrivere in questo file `0` (on) oppure `3` (off). Sia il codice ACPI nel kernel sia l'hardware (oppure il BIOS) sovrascrivono questo parametro quando la ventola si surriscalda.

/proc/acpi/processor/*
Per ciascuna CPU esiste una subdirectory separata inclusa nel sistema.

/proc/acpi/processor/*/info
Informazioni sulle opzioni di risparmio energetico del processore.

/proc/acpi/processor/*/power
Informazioni sullo stato corrente del processore. L'asterisco accanto a `C2` indica che il processore è inattivo. Questo è lo stato più frequente come si può rilevate dal valore `utilizzo`.

/proc/acpi/processor/*/throttling
Può essere utilizzato per impostare il throttling dell'orologio del processore. Di norma il throttling è possibile in otto livelli ed è indipendente dal controllo della frequenza della CPU.

/proc/acpi/processor/*/limit
Se la prestazione (non aggiornata) e il throttling vengono controllati automaticamente da un daemon, in questo file è possibile specificare il limite massimo. Alcuni di questi limiti vengono stabiliti dal sistema mentre altri possono essere regolati dall'utente.

/proc/acpi/thermal_zone/
Per ciascun zona termica esiste una subdirectory separata. La zona termica è un'area con proprietà termiche simili dotata di numero e nomi assegnati dal produttore hardware. Molte possibilità offerte da ACPI vengono tuttavia implementate raramente. Il controllo della temperatura, invece, viene gestito per convenzione dal BIOS. Il sistema operativo non ha grandi possibilità di intervenire poiché è in gioco la durata dell'hardware. Perciò alcuni file hanno solo valore teorico.

/proc/acpi/thermal_zone/*/temperature
Temperatura corrente della zona termica.

/proc/acpi/thermal_zone/*/state
Lo stato indica se tutto è `ok` oppure se ACPI applica il raffreddamento `attivo` o `passivo`. Se il controllo della ventola è indipendente da ACPI, questo stato indicherà sempre `ok`.

/proc/acpi/thermal_zone/*/cooling_mode
Consente di selezionare il metodo di raffreddamento controllato da ACPI e di scegliere la modalità di raffreddamento passivo (minore prestazione, economica) oppure attivo (piena prestazione, rumore della ventola).

/proc/acpi/thermal_zone/*/trip_points
Consente di stabilire i limiti della temperatura per l'avvio di azioni specifiche, come ad esempio il raffreddamento passivo o attivo, la sospensione (`caldo`) oppure lo shutdown (`critico`). Le azioni possibili sono definite nella DSDT (dipendente dal dispositivo). I trip point stabiliti nella specifica ACPI sono `critico`, `caldo`, `passivo`, `attivo1` e `attivo2`. Anche se non sono stati implementati tutti, è necessario immetterli in questo file in questo ordine. Ad esempio, la voce `echo 90:0:70:0:0 > trip_points` imposta la temperatura per `critico` a `90` e la temperatura per `passivo` a `70` (tutte le temperature sono misurate in gradi centigradi).

/proc/acpi/thermal_zone/*/polling_frequency
Se il valore presente nel file `temperature` non viene aggiornato automaticamente quando la temperatura cambia, modificare la modalità polling in questo file. Il comando `echo X > /proc/acpi/thermal_zone/*/polling_frequency` consente di richiedere la temperatura ogni `X` secondi. Impostare `X=0` per disabilitare il polling.

Non è necessario modificare manualmente nessuna di queste impostazioni, informazioni o eventi. È possibile eseguire tale modifica con il daemon Powersave (powersaved) e varie applicazioni quali ad esempio powersave, kpowersave e wmpowersave. Vedere la Sezione 21.3.3, «Strumenti di ACPI» (p. 292). Poiché powersaved copre le funzionalità dell'acpid precedente, questo non è più necessario.

21.3.2 Controllo della prestazione della CPU

La CPU può risparmiare energia in tre modi. È possibile combinare questi tre metodi a seconda della modalità di funzionamento del computer. Risparmiare energia significa anche che il sistema si riscalda di meno e le ventole vengono attivate con minore frequenza.

Adattamento della frequenza e della tensione
PowerNow! e Speedstep sono utilizzati da AMD e Intel per questa tecnologia, che viene applicata anche nei processori di altri produttori. La frequenza dell'orologio della CPU e il relativo voltaggio principale vengono ridotti nello stesso momento, consentendo un risparmio maggiore dell'energia lineare. Ciò significa che quando la frequenza viene dimezzata (prestazione a metà), il consumo di energia è molto inferiore alla metà. Questa tecnologia è indipendente da APM o ACPI e richiede un daemon per adattare la frequenza e l'esigenza corrente per la prestazione. È possibile eseguire le impostazioni nella directory `/sys/devices/system/cpu/cpu*/cpufreq/`.

Throttling della frequenza dell'orologio
Questa tecnologia omette una determinata percentuale di impulsi del segnale orario per la CPU. Con un valore di 25% del throttling, viene omesso un impulso su quattro. Con un valore di 87,5%, solo un impulso su otto arriva al processore. I risparmi energetici sono tuttavia poco inferiori rispetto all'energia lineare. Il throttling viene utilizzato di norma soltanto se non è disponibile l'adattamento della frequenza oppure per ottimizzare i risparmi energetici. Anche questa tecnologia deve essere controllata con un processo speciale. L'interfaccia del sistema è `/proc/acpi/processor/*/throttling`.

Mettere il processore nello stato sleep
Il sistema operativo mette il processore nello stato sleep durante un periodo di inattività e invia alla CPU un comando `halt`. Gli stati sono tre: C1, C2 e C3. Nello stato più economico, C3, viene arrestata anche la sincronizzazione della cache del processore con la memoria principale. Questo stato può essere applicato, quindi, soltanto se nessun altro dispositivo modifica il contenuto della memoria principale tramite attività del bus master. Alcuni driver impediscono l'utilizzo dello stato C3. Lo stato corrente viene visualizzato in `/proc/acpi/processor/*/power`.

L'adattamento della frequenza e il throttling sono importanti solo se il processore è occupato poiché lo stato economico C viene applicato in ogni caso quando il processore è inattivo. Se la CPU è occupata, si consiglia di utilizzare l'adattamento della frequenza come metodo di risparmio energetico. Di solito il processore lavora soltanto con un carico parziale. In questo caso, è possibile utilizzarlo con una frequenza inferiore. In genere, l'adattamento della frequenza dinamico controllato da un daemon, ad esempio powersaved, è l'approccio migliore. L'impostazione statica su una frequenza bassa è utile per il funzionamento a batteria oppure se il computer deve restare freddo oppure in modo silenzioso.

Utilizzare il throttling solo se indispensabile, ad esempio, per estendere il tempo di funzionamento a batteria nonostante un elevato carico del sistema. Alcuni sistemi tuttavia non funzionano correttamente se vengono sottoposti a throttling in modo eccessivo. Inoltre, il throttling della CPU non risulta utile se la CPU ha un'attività ridotta.

In SUSE Linux queste tecnologie vengono controllare dal daemon powersave. La configurazione è spiegata in Sezione 21.5, «Il paccheto powersave» (p. 295).

21.3.3 Strumenti di ACPI

La gamma di utilità più o meno complete di ACPI comprende strumenti che visualizzano semplicemente informazioni quali ad esempio il livello di carica e la temperatura della batteria (acpi, klaptopdaemon, wmacpimon, ecc.), strumenti che facilitano l'accesso alle strutture in `/proc/acpi` oppure offrono supporto per il monitoraggio delle modifiche (akpi, acpiw, gtkacpiw) e strumenti per la modifica delle tabelle di ACPI nel BIOS (pacchetto `pmtools`).

21.3.4 Risoluzione dei problemi

Esistono due diversi tipi di problemi. Il codice ACPI del kernel potrebbe contenere errori che non sono stati rilevati in tempo. In questo caso, verrà resa disponibile una soluzione da scaricare. Si verifica più spesso che i problemi siano causati dal BIOS. A volte, le deviazioni dalla specifica ACPI sono integrate appositamente nel BIOS per aggirare gli errori nell'implementazione di ACPI in altri sistemi operativi diffusi. I componenti hardware con gravi errori nell'implementazione di ACPI sono registrati in una lista nera che impedisce al kernel di Linux di utilizzare ACPI per questi componenti.

In caso di problemi si consiglia innanzitutto di aggiornare il BIOS. Se il computer non si avvia, si consiglia di utilizzare uno dei seguenti parametri di avvio:

pci=noacpi
: Non utilizzare ACPI per la configurazione dei dispositivi PCI.

acpi=oldboot
: Eseguire soltanto una semplice configurazione delle risorse. Non utilizzare ACPI per altri scopi.

acpi=off
Consente di disabilitare ACPI.

AVVERTIMENTO: Problemi di avvio senza ACPI

Alcuni computer recenti (in particolare i sistemi SMP e AMD64) richiedono ACPI per la configurazione corretta dell'hardware. Su altri computer, se ACPI viene disabilitato possono sorgere dei problemi.

Controllare i messaggi di avvio del sistema con il comando `dmesg | grep -2i acpi` (oppure tutti i messaggi poiché il problema potrebbe non essere causato da ACPI) dopo l'avvio. In caso di errore durante l'analisi di una tabella ACPI, è possibile sostituire la tabella principale – la DSDT – con una versione migliorata. In questo caso, la tabella difettosa del BIOS viene ignorata. La procedura è descritta nella Sezione 21.5.4, «Risoluzione dei problemi» (p. 301).

Nella configurazione del kernel, è presente un commando per attivare i messaggi di debug di ACPI. Se viene compilato e installato un kernel con la funzione di debug di ACPI, gli utenti esperti che cercano un errore trovano supporto con informazioni dettagliate.

In caso di problemi con il BIOS oppure con l'hardware, si consiglia di rivolgersi sempre ai produttori. Specialmente se non offrono sempre assistenza per Linux, dovrebbero affrontare questi problemi. I produttori prendono seriamente il problema solo se realizzano che un numero considerevole dei loro clienti utilizza Linux.

Ulteriori informazioni

Documentazione aggiuntiva e guida su ACPI:

- `http://www.cpqlinux.com/acpi-howto.html` (ACPI HOWTO dettagliato, contiene patch per DSDT)
- `http://www.intel.com/technology/iapc/acpi/faq.htm` (ACPI FAQ @Intel)
- `http://acpi.sourceforge.net/` (progetto ACPI4Linux su Sourceforge)
- `http://www.poupinou.org/acpi/` (patch per DSDT di Bruno Ducrot)

21.4 Disco rigido a riposo

In Linux, se il disco rigido non è necessario è possibile metterlo completamente nello stato sleep oppure utilizzarlo in modo più economico o più silenzioso. Sui computer portatili moderni, non è necessario disattivare i dischi rigidi manualmente, poiché passano automaticamente alla modalità di funzionamento economica quando non sono necessari. Tuttavia, per ottimizzare il risparmio energetico, è possibile provare qualcuno dei metodi seguenti. La maggior parte delle funzioni possono essere controllate con powersaved e il modulo power management di YaST, descritto in dettaglio nella Sezione 21.6, «Modulo power management di YaST» (p. 304).

È possibile utilizzare l'applicazione hdparm per modificare diverse impostazioni del disco rigido. Con l'opzione `-y` il disco rigido passa subito al modo stand-by. Con l'opzione `-Y` passa allo stato sleep. `hdparm -S x` comporta il rallentamento del disco rigido dopo un determinato periodo di inattività. Sostituire *x* nel seguente modo: `0` disattiva questo meccanismo e fa funzionare il disco costantemente. I valori da `1` a `240` vengono moltiplicati per 5 secondi. I valori da `241` a `251` corrispondono da 1 a 11 moltiplicato 30 minuti.

È possibile controllare le opzioni interne di risparmio energetico del disco rigido con l'opzione `-B`. Selezionare un valore da `0` a `255` per il risparmio massimo alla massima velocità. Il risultato dipende dal disco rigido utilizzato ed è di difficile valutazione. Per rendere più silenzioso un disco rigido, utilizzare l'opzione `-M`. Selezionare un valore da `128` a `254` per il funzionamento silenzioso e veloce.

Spesso non è facile far passare il disco rigido allo stato sleep. In Linux, molti processi scrivono sul disco rigido, causandone ripetutamente la riattivazione. Perciò, è importante comprendere come Linux gestisce i dati da scrivere sul disco rigido. Innanzitutto, tutti i dati vengono memorizzati nel buffer della RAM. Questo buffer viene controllato dal daemon per l'aggiornamento del kernel (kupdated). Al raggiungimento di un determinato periodo limite di permanenza o quando il buffer è pieno fino a un certo limite, il contenuto del buffer viene eliminato e spostato nel disco rigido. La dimensione del buffer è dinamica e dipende dalla dimensione della memoria e dal carico del sistema. Per default, kupdated è impostato in modo da raggiungere la massima integrità dei dati in intervalli brevi. Verifica il buffer ogni 5 secondi e informa il daemon bdflush quando i dati hanno superato una permanenza superiore a 30 secondi oppure se il buffer ha raggiunto il livello di riempimento del 30%. Il daemon bdflush scrive quindi i dati sul disco rigido e li scrive anche a prescindere da kupdated se, ad esempio, il buffer è pieno.

AVVERTIMENTO: Danneggiamento dell'integrità dei dati

Le modifiche apportate alle impostazioni del daemon per l'aggiornamento del kernel mettono a rischio l'integrità dei dati.

Oltre a questi processi, il diario dei file system, ad es. ReiserFS e Ext3, scrive i metadati a prescindere da bdflush, che inoltre impedisce al disco rigido di rallentare. Per evitare che ciò avvenga, è stata sviluppata un'estensione speciale del kernel per i dispositivi mobili. Per i dettagli, vedere `/usr/src/linux/Documentation/laptop-mode.txt`.

Un altro fattore importante è il comportamento dei programmi attivi. Ad esempio, alcuni editor scrivono di norma sul disco rigido i backup nascosti del file attualmente modificato causando la riattivazione del disco. È possibile disabilitare funzionalità di questo tipo a scapito dell'integrità dei dati.

A tale proposito, Postfix del daemon di posta utilizza la variabile `POSTFIX_LAPTOP`. Se questa variabile è impostata su `sì`, Postfix accede al disco rigido molto più raramente. Risulta tuttavia irrilevante se è stato aumentato l'intervallo per kupdated.

21.5 Il paccheto powersave

Il pacchetto `powersave` è responsabile della funzione di risparmio energetico nei computer portatili durante il funzionamento a batteria. Alcune delle funzionalità sono utili anche per workstations e server normali, quali ad esempio la sospensione, lo stand-by, la funzionalità del pulsante ACPI e il passaggio dei dischi rigidi IDE allo stato sleep.

In questo pacchetto sono incluse tutte le funzionalità di power management del computer. Supporta hardware che utilizza dischi rigidi ACPI, APM, IDE e tecnologie PowerNow! oppure SpeedStep. Le funzionalità dei pacchetti `apmd`, `acpid`, `ospmd`, e `cpufreqd` (ora `cpuspeed`) sono state consolidate nel pacchetto `powersave`. Si consiglia di non eseguire i daemon di questi pacchetti contemporaneamente con il daemon powersave.

Anche se il sistema non contiene tutti gli elementi hardware sopra elencati, si consiglia di utilizzare il daemon powersave per il controllo della funzione di risparmio energetico. Poiché ACPI e APM sono mutualmente esclusivi, è possibile utilizzare soltanto uno

dei due a esclusione dell'altro sul computer. Il daemon rileva automaticamente qualsiasi modifica apportata alla configurazione dell'hardware.

21.5.1 Configurazione del pacchetto powersave

In genere, la configurazione di powersave è distribuita su diversi file:

`/etc/sysconfig/powersave/common`
Questo file contiene le impostazioni generali del daemon powersave. Ad esempio, è possibile aumentare la quantità di messaggi di debug in `/var/log/messages` aumentando il valore della variabile `DEBUG`.

`/etc/sysconfig/powersave/events`
Il daemon powersave utilizza questo file per l'elaborazione degli eventi di sistema. È possibile assegnare a un evento azioni esterne o azioni eseguite dal daemon stesso. Per le azioni esterne, il daemon prova a eseguire un file eseguibile in `/usr/lib/powersave/scripts/`. Azioni interne predefinite:

- ignora
- throttle
- dethrottle
- sospensione_su_disco
- sospensione_su_ram
- stand-by
- esegui_sospensione_su_disco
- esegui_sospensione_su_ram
- esegui_stand-by

`throttle` rallenta il processore in base al valore definito in `MAX_THROTTLING`. Questo valore dipende dallo schema corrente. `dethrottle` imposta il processore sulla prestazione piena. `sospensione_su_disco`, `sospensione_su_ram`,

e `stand-by` attivano l'evento del sistema per lo stato sleep. Queste tre azioni sono di norma responsabili dell'attivazione dello stato sleep, ma devono essere sempre associate a eventi del sistema specifici.

La directory `/usr/lib/powersave/scripts` contiene script per l'elaborazione degli eventi:

notify
Notifica di un evento tramite console, X window oppure segnale acustico.

screen_saver
Attiva lo screen saver.

switch_vt
Risulta utile se lo schermo si trova in stato di sospensione o di stand-by.

wm_logout
Consente di salvare le impostazioni ed esegue il log out da GNOME, KDE o altri gestori di finestre.

wm_shutdown
Consente di salvare le impostazioni GNOME o KDE e chiude il sistema.

Se, ad esempio, è impostata la variabile `EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk"`, i due script o azioni vengono elaborati nell'ordine specifico appena l'utente da il comando a powersaved per lo stato sleep `sospensione su disco`. Il daemon esegue lo script esterno `/usr/lib/powersave/scripts/prepare_suspend_to_disk`. Dopo l'elaborazione corretta dello script, il daemon esegue l'azione interna `esegui_sospensione_su_disco` e imposta il computer sullo stato sleep dopo che lo script ha scaricato i moduli critici e i servizi arrestati.

Le azioni per l'evento di un pulsante sleep possono essere modificate come in `EVENT_BUTTON_SLEEP="notify suspend_to_disk"`. In questo caso, l'utente viene informato della sospensione dallo script esterno `notifica`. Successivamente, viene generato l'evento `EVENT_GLOBAL_SUSPEND2DISK` che comporta l'esecuzione delle azioni indicate e una modalità sicura di sospensione del sistema. Lo script `notifica` può essere personalizzato utilizzando la variabile `NOTIFY_METHOD` in `/etc/sysconfig/powersave/common`.

/etc/sysconfig/powersave/cpufreq
Contiene variabili per l'ottimizzazione delle impostazioni della frequenza dinamica della CPU.

/etc/sysconfig/powersave/battery
Contiene i limiti della batteria e altre impostazioni specifiche della batteria.

/etc/sysconfig/powersave/sleep
In questo file, attivare gli stati sleep e stabilire quali moduli critici devono essere scaricati e quali servizi devono essere arrestati prima dell'evento di sospensione o di stand-by. Alla ripresa del sistema, questi moduli vengono ricaricati e i servizi riavviati. È possibile anche ritardare uno stato sleep avviato, ad esempio, per salvare dei file. Le impostazioni di default interessano essenzialmente i moduli USB e PCMCIA. Un errore di sospensione o di stand-by viene causato in genere da determinati moduli. Vedere la Sezione 21.5.4, «Risoluzione dei problemi» (p. 301) per ulteriori informazioni sull'identificazione dell'errore.

/etc/sysconfig/powersave/thermal
Consente di attivare il controllo per il raffreddamento e termico. Informazioni dettagliate su questo argomento sono disponibili nel file `/usr/share/doc/packages/powersave/README.thermal`.

/etc/sysconfig/powersave/scheme_*
Questi sono i vari schemi che regolano il consumo di energia secondo determinati scenari di distribuzione. Esistono diversi schemi preconfigurati che possono essere utilizzati così come sono. Gli schemi personalizzati possono essere salvati qui.

21.5.2 Configurazione di APM e ACPI

Sospensione e stand-by

Per default, gli stati sleep sono inattivi poiché su alcuni computer non funzionano. Esistono tre stati sleep ACPI di base e due stati sleep APM:

Sospensione su disco (ACPI S4, APM suspend)
Consente di salvare tutto il contenuto della memoria sul disco rigido. Il computer viene disattivato completamente e non vi è consumo di alimentazione.

Sospensione su RAM (ACPI S3, APM suspend)
Consente di salvare gli stati di tutti i dispositivi nella memoria principale. Soltanto la memoria principale continua a consumare energia.

Stand-by (ACPI S1, APM standby)
Consente di disattivare alcuni dispositivi (a seconda del produttore).

Assicurarsi che le seguenti opzioni di default siano impostate nel file `/etc/sysconfig/powersave/events` per l'elaborazione corretta di sospensione, stand-by e ripresa (impostazioni di default secondo l'installazione di SUSE Linux):

```
EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk do_suspend_to_disk"
EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
    "prepare_standby do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

Personalizzazione degli stati della batteria

Nel file `/etc/sysconfig/powersave/battery`, definire i tre livelli di carica della batteria (in percentuale) che attivano gli avvisi del sistema o le azioni specifiche quando vengono visualizzati.

```
BATTERY_WARNING=20
BATTERY_LOW=10
BATTERY_CRITICAL=
```

Le azioni o gli script da eseguire quando i livelli di carica scendono al di sotto dei limiti specificati sono definiti nel file di configurazione `/etc/sysconfig/powersave/events`. Le azioni standard dei pulsanti possono essere modificate come descritto nella Sezione 21.5.1, «Configurazione del pacchetto powersave» (p. 296).

```
EVENT_BATTERY_NORMAL="ignore"
EVENT_BATTERY_WARNING="notify"
EVENT_BATTERY_LOW="notify"
EVENT_BATTERY_CRITICAL="wm_shutdown
```

Adattamento del consumo di energia secondo le diverse condizioni

È possibile adattare il comportamento del sistema secondo il tipo di alimentazione. È necessario che il consumo di energia del sistema sia ridotto quando il sistema viene disconnesso dall'alimentazione a elettricità e passa al funzionamento a batteria. Allo stesso modo, è necessario che la prestazione aumenti automaticamente non appena il sistema viene connesso all'alimentazione a elettricità. È possibile modificare la frequenza della CPU, la funzione di risparmio energetico di IDE e alcuni altri parametri.

Le azioni da eseguire quando il computer viene disconnesso da o connesso all'alimentazione a elettricità sono definite in `/etc/sysconfig/powersave/events`. Selezionare gli schemi da utilizzare in `/etc/sysconfig/powersave/common`:

```
AC_SCHEME="performance"
BATTERY_SCHEME="powersave
```

Gli schemi sono memorizzati nei file in `/etc/sysconfig/powersave`. I nomi file sono nel formato `schema_nome-dello-schema`. L'esempio fa riferimento a due schemi: `schema_prestazione` e `schema_powersave`. `prestazione`, `powersave`, `presentazione` e `acustica` sono preconfifurati. Gli schemi esistenti possono essere modificati, creati, eliminati o associati a diversi stati di alimentazione con il modulo power management di YaST descritto nella Sezione 21.6, «Modulo power management di YaST» (p. 304).

21.5.3 Funzionalità aggiuntive di ACPI

Se si utilizza ACPI, è possibile controllare la risposta del sistema ai *pulsanti ACPI* (power, sleep, schermo aperto e schermo abbassato). Configurare l'esecuzione delle azioni in `/etc/sysconfig/powersave/events`. Per la spiegazione delle single opzioni, fare riferimento al file di configurazione.

EVENT_BUTTON_POWER="wm_shutdown"
Alla pressione del pulsante Power, il sistema risponde chiudendo il rispettivo gestore delle finestre (KDE, GNOME, fvwm, e così via.).

EVENT_BUTTON_SLEEP="suspend_to_disk"
Alla pressione del pulsante Sleep, il sistema viene impostato sullo stato sospensione su disco.

EVENT_BUTTON_LID_OPEN="ignore"
Quando si apre lo schermo non avviene nulla.

EVENT_BUTTON_LID_CLOSED="screen_saver"
Quando lo schermo viene abbassato, viene attivato lo screen saver.

È possibile sottoporre ancora a throttling la prestazione della CPU se il carico della CPU non supera il limite specificato per un periodo specificato. Specificare il limite di carico in `PROCESSOR_IDLE_LIMIT` e il time-out in `CPU_IDLE_TIMEOUT`. Se il carico della CPU resta al di sotto del limite per un periodo di tempo superiore al time-out, viene attivato l'evento configurato in `EVENT_PROCESSOR_IDLE`. Se la CPU è di nuovo occupata, viene eseguito `EVENT_PROCESSOR_BUSY`.

21.5.4 Risoluzione dei problemi

Tutti i messaggi e gli avvisi di errore vengono registrati nel file `/var/log/messages`. Nel caso non si riesca a trovare le informazioni necessarie, aumentare la verbosità dei messaggi di powersave utilizzando `DEBUG` nel file `/etc/sysconfig/powersave/common`. Aumentare il valore della variabile a `7` oppure fino a `15` e riavviare il daemon. Gli ulteriori messaggi di errore in `/var/log/messages` sono utili per trovare l'errore. Nella sezione seguente vengono illustrati i problemi più comuni riscontrati con powersave.

ACPI attivato con supporto hardware ma le funzioni non sono attive

Per problemi con ACPI, utilizzare il comando `dmesg|grep -i acpi` per cercare l'output di `dmesg` per messaggi specifici di ACPI. Potrebbe essere necessario aggiornare il BIOS per risolvere il problema. Aprire la pagina iniziale del produttore del computer portatile, cercare la versione aggiornata del BIOS e installarla. Chiedere al produttore la conformità con la specifica ACPI più recente. Se gli errori persistono dopo l'aggiornamento del BIOS, procedere come segue per sostituire la tabella DSDT difettosa del BIOS con quella aggiornata:

1. Scaricare la tabella DSDT per il sistema da http://acpi.sourceforge.net/dsdt/tables. Fare clic se il file è decompresso e compilato come risulta dall'estensione del file .aml (linguaggio macchina ACPI). Se questo è il caso, continuare con il passaggio 3.

2. Se l'estensione del file della tabella scaricata è .asl (linguaggio sorgente ACPI), compilarlo con iasl (pacchetto pmtools). Immettere il comando iasl -sa file.asl . La versione più recente di iasl (compilatore Intel ACPI) è disponibile all'indirizzo http://developer.intel.com/technology/iapc/acpi/downloads.htm.

3. Copiare il file DSDT.aml in una ubicazione qualsiasi (/etc/DSDT.aml consigliata). Modificare /etc/sysconfig/kernel e adattare di conseguenza il percorso del file DSDT. Avviare mkinitrd (pacchetto mkinitrd). Quando si installa il kernel e si utilizza mkinitrd per creare un initrd, la tabella DSDT modificata viene integrata e caricata all'avvio del sistema.

La frequenza della CPU non funziona

Fare riferimento alle origini del kernel (kernel-source) per verificare se il processore è supportato. Per attivare il controllo della frequenza della CPU, potrebbero essere necessari un modulo o opzione di modulo speciale del kernel. Questa informazione è disponibile in /usr/src/linux/Documentation/cpu-freq/*. Nel caso siano necessari un modulo o un'opzione speciale, configurarli nel file /etc/sysconfig/powersave/cpufreq con le variabili CPUFREQD_MODULE e CPUFREQD_MODULE_OPTS.

Gli stati sospensione e stand-by non funzionano

Alcuni problemi relativi al kernel impediscono l'utilizzo degli stati di sospensione e di stand-by nei sistemi ACPI:

- Attualmente, i sistemi con oltre 1 GB di RAM non supportano lo stato di sospensione.

- Attualmente, i sistemi con multiprocessore e i sistemi con processore P4 (con hyperthreading) non supportano lo stato di sospensione.

È possibile che l'errore sia dovuto a un'implementazione (BIOS) difettosa della tabella DSDT. In questo caso, installare un nuova DSDT.

Nei sistemi ACPI e APM: Quando vengono scaricati moduli difettosi, il sistema si arresta oppure l'evento di sospensione non viene attivato. Lo stesso accade se non si scaricano moduli o servizi di arresto che impediscono una sospensione corretta. In entrambi i casi, identificare il modulo difettoso che ha impedito lo stato sleep. I file di log generati dal daemon powersave in `/var/log/sleep mode` sono molti utili a tale proposito. Se il computer non passa allo stato sleep, la causa risiede nell'ultimo modulo scaricato. Manipolare le impostazioni seguenti in `/etc/sysconfig/powersave/sleep` per scaricare i moduli che presentano problemi prima di uno stato di sospensione o stand-by.

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES="
```

Se si utilizza la sospensione o lo stand-by durante la modifica degli ambienti di rete o con file system montati in remoto, quali ad esempio Samba e NIS, utilizzare automounter per montarli o aggiungere i rispettivi servizi, ad esempio, `smbfs` o `nfs`, nella variabile sopra indicata. Se un'applicazione accede al file system montato in remoto prima dello stato di sospensione o di stand-by, non è possibile arrestare il servizio correttamente e il file system non può essere smontato in modo adeguato. Dopo la ripresa del sistema, il file system potrebbe essere corrotto e deve essere rimontato.

Durante l'utilizzo di ACPI, Powersave non riconosce i limiti della batteria

Con ACPI, il sistema operativo può richiedere che BIOS invii un messaggio quando il livello di carica della batteria scende al di sotto di un determinato limite. Il vantaggio di questo metodo è costituito dal fatto che la batteria non deve essere sottoposta a polling costantemente, che potrebbe causare problemi alla prestazione del computer. Tuttavia, è possibile che questa notifica non venga inviata quando il livello di carica scende al di sotto del limite specificato, anche se il BIOS dovrebbe supportare questa funzionalità. In tal caso, impostare la variabile `FORCE_BATTERY_POLLING` nel file `/etc/sysconfig/powersave/battery` su `sì` per eseguire forzatamente il polling della batteria.

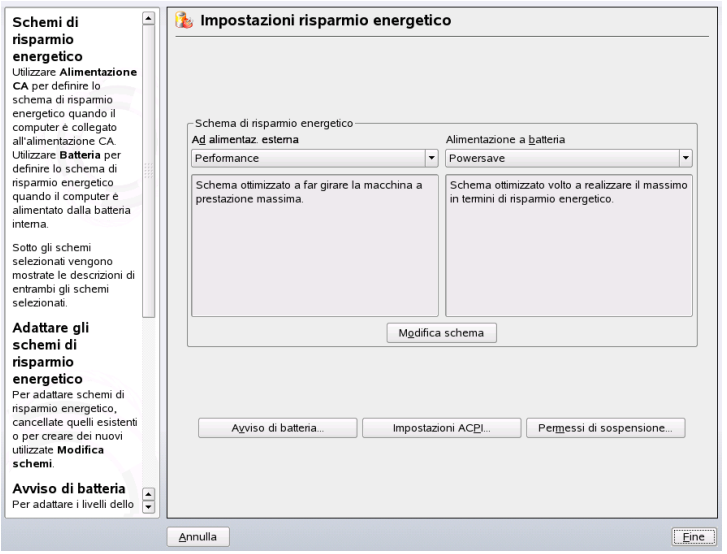
21.5.5 Ulteriori informazioni

Ulteriori informazioni sul pacchetto powersave sono disponibili anche in `/usr/share/doc/packages/powersave`.

21.6 Modulo power management di YaST

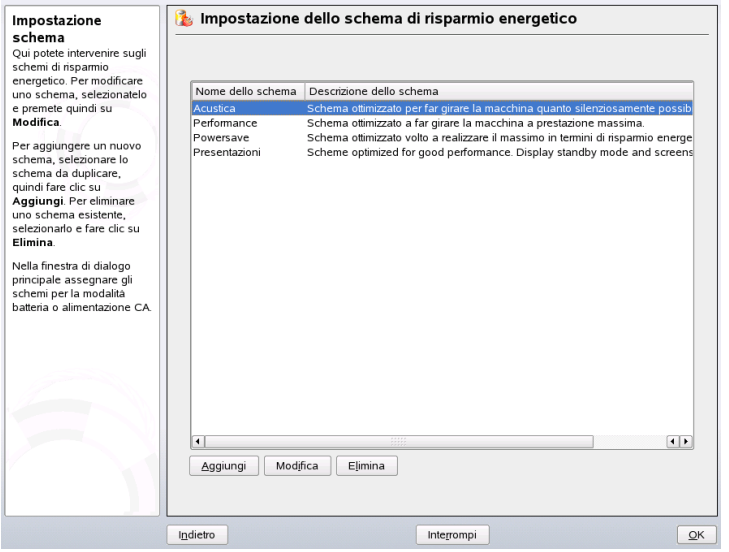
Il modulo power management di YaST consente di configurare tutte le impostazioni di power management già descritte. Quando viene avviato dal Centro di controllo di YaST con *System → Power Management*, si apre la prima finestra di dialogo del modulo. La finestra è mostrata in Figura 21.1, «Selezione dello schema» (p. 304).

Figura 21.1 *Selezione dello schema*



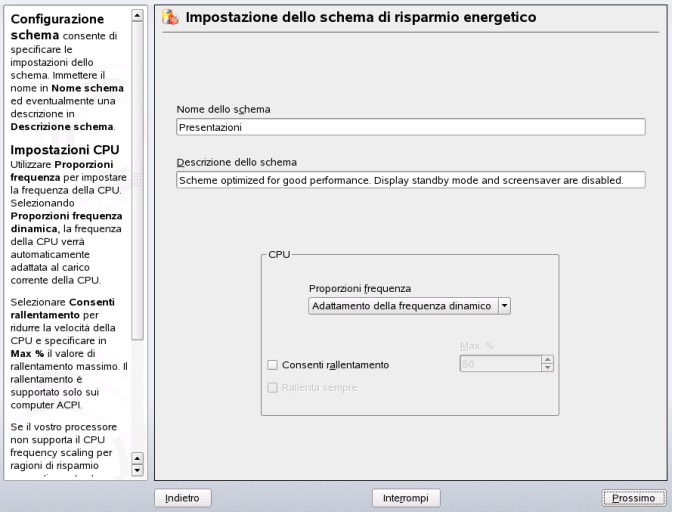
In questa finestra di dialogo, selezionare gli schemi da utilizzare per il funzionamento con alimentazione a batteria e a elettricità. Per aggiungere o modificare gli schemi, fare clic su *Modifica schemi*, viene visualizzata una panoramica degli schemi esistenti come quelli visualizzati in Figura 21.2, «Panoramica degli schemi esistenti» (p. 305).

Figura 21.2 *Panoramica degli schemi esistenti*



Nella panoramica degli schemi, selezionare lo schema da modificare quindi fare clic su *Modifica*. Per creare un nuovo schema, fare clic su *Aggiungi*. In entrambi i casi si apre la stessa finestra di dialogo che viene visualizzata in Figura 21.3, «Configurazione dello schema» (p. 306).

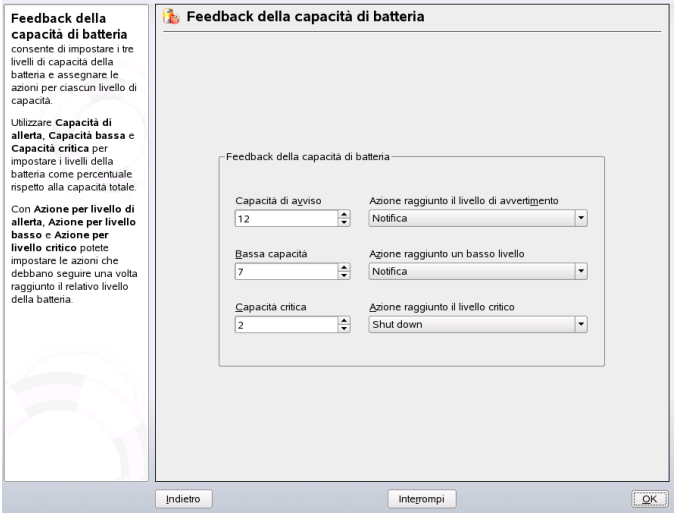
Figura 21.3 *Configurazione dello schema*



Immettere un nome e una descrizione adatti per lo schema nuovo o modificato. Stabilire se è necessario controllare le prestazioni della CPU per questo schema e le modalità di tale controllo. Decidere se e in che misura utilizzare il frequency scaling e il throttling. Nella finestra di dialogo seguente per il disco rigido, definire una *Politica di stand-by* per la prestazione massima o per il risparmio energetico. La *Strategia acustica* consente di controllare il livello di rumore del disco rigido (non supportata da tutti i dischi rigidi). La *Politica del raffreddamento* stabilisce il metodo di raffreddamento da utilizzare. Tuttavia, questo tipo di controllo termico è supportato raramente dal BIOS. Consultare `/usr/share/doc/packages/powersave/README.thermal` per informazioni sull'utilizzo dei metodi di raffreddamento attivo e passivo.

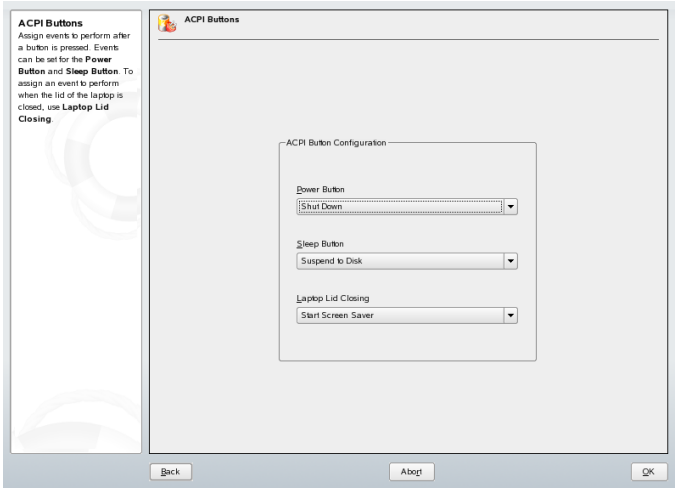
È possibile eseguire le impostazioni generali di power management dalla finestra di dialogo iniziale mediante *Avviso di batteria*, *Impostazioni ACPI*, o *Abilita sospensione*. Fare clic su *Avviso di batteria* per accedere alla finestra di dialogo per il livello di carica della batteria, visualizzata in Figura 21.4, «Livello di carica della batteria» (p. 307).

Figura 21.4 *Livello di carica della batteria*



Se il livello di carica scende sotto determinati limiti configurabili, il BIOS lo notifica al sistema operativo. Definire tre limiti in questa finestra di dialogo: *Capacità di allerta*, *Bassa capacità* e *Capacità critica*. Vengono attivate azioni specifiche quando il livello di carica scende sotto questi limiti. Di norma, i primi due stati si attivano solo per avvisare l'utente. Il terzo livello critico attiva la chiusura poiché l'energia rimanente non è sufficiente per il funzionamento continuativo del sistema. Selezionare i livelli di carica appropriati e le azioni desiderate, quindi fare clic su *OK* per tornare alla finestra di dialogo di avvio.

Figura 21.5 *Impostazioni ACPI*



Per la configurazione dei pulsanti di ACPI, accedere alla finestra di dialogo mediante *Impostazioni ACPI*. La finestra è mostrata in Figura 21.5, «Impostazioni ACPI» (p. 308). Le impostazioni dei pulsanti di ACPI determinano le modalità di risposta del sistema a determinate azioni relative all'alimentazione. Configurare la risposta del sistema alla pressione del pulsante Power, alla pressione del pulsante sleep e alla chiusura dello schermo del portatile. Fare clic su *OK* per completare la configurazione e tornare alla finestra di dialogo iniziale.

Fare clic su *Abilita sospensione* per aprire una finestra di dialogo e stabilire possibilità e modalità di utilizzo della funzionalità di sospensione o di stand-by da parte degli utenti del sistema. Fare clic su *OK* per tornare alla finestra di dialogo principale. Fare clic su *OK* una seconda volta per uscire dal modulo e confermare le impostazioni di power management specificate.

22 Comunicazione wireless

Esistono numerose possibilità per collegare il sistema Linux ad altri computer, cellulari o dispositivi periferici. Il sistema WLAN (wireless LAN) può essere usato per collegare i computer portatili in rete. Il sistema Bluetooth può essere usato per collegare singoli componenti (mouse, tastiera), periferiche, cellulari, PDA e singoli computer gli uni agli altri. Il sistema a infrarossi IrDA è usato per lo più con PDA o cellulari. Il presente capitolo introduce queste tre tecnologie e ne descrive la configurazione.

22.1 LAN wireless

Nell'informatica mobile le LAN wireless sono diventate ormai indispensabili. Oggi, nella maggior parte dei computer portatili sono inserite schede WLAN. Lo standard 802.11 per la comunicazione wireless delle schede WLAN è stato preparato da IEEE. In origine, questo standard forniva una velocità massima di trasmissione di 2 MBit/secondo. Nel frattempo sono state aggiunte varie integrazioni per aumentare la velocità dei dati. Queste integrazioni consentono di definire particolari quali la modulazione, l'output e le velocità di trasmissione:

Tabella 22.1 *Panoramica dei vari standard WLAN*

Nome	Band (GHz)	Velocità massima di trasmissione (MBit/s)	Nota
802.11	2.4	2	Obsoleto; nessun dispositivo finale disponibile
802.11b	2.4	11	Diffuso
802.11a	5	54	Meno comune
802.11g	2.4	54	Compatibile con versioni precedenti con 11b

Esistono inoltre standard proprietari, come la variazione 802.11b di Texas Instruments con una velocità massima di trasmissione di 22 MBit/s (questo standard viene a volte chiamato 802.11b+). In ogni caso la diffusione delle schede che supportano questo standard è limitata.

22.1.1 Hardware

Le schede 802.11 non sono supportate da SUSE Linux. La maggior parte delle schede che utilizzano 802.11a, 802.11b e 802.11g sono comunque supportate. Di solito le nuove schede sono conformi allo standard 802.11g, ma sono ancora disponibili quelle che utilizzano lo standard 802.11b. Le schede con i seguenti chip sono normalmente supportate:

- Aironet 4500, 4800
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Intel PRO/Wireless 2100, 2200BG, 2915ABG
- Intersil Prism2/2.5/3

- Intersil PrismGT
- Lucent/Agere Hermes
- Ralink RT2400, RT2500
- Texas Instruments ACX100, ACX111
- ZyDAS zd1201

Sono inoltre supportate diverse altre schede più obsolete che sono raramente utilizzate e non più disponibili. Una lista esauriente delle schede WLAN e dei relativi chip è disponibile sul sito di *AbsoluteValue Systems* at `http://www.linux-wlan.org/docs/wlan_adapters.html.gz`. `http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz` e fornisce una panoramica dei diversi chip WLAN.

Per alcune schede è necessaria un'immagine firmware che deve essere caricata al momento dell'inizializzazione del driver. È il caso diIntersil PrismGT, Atmel, TI ACX100 e ACX111. Il firmware può essere facilmente installato con l'aggiornamento online YaST. Il firmware per le schede Intel PRO/Wireless viene fornito con SUSE Linux e viene installato automaticamente da YaST non appena viene rilevato questo tipo di scheda. Ulteriori informazioni su questo argomento sono disponibili nel sistema installato in `/usr/share/doc/packages/wireless-tools/README.firmware`.

Le schede che non hanno un supporto Linux nativo possono essere utilizzate eseguendo l'applicazione ndiswrapper che utilizza i driver di Windows consegnati con la maggior parte delle schede WLAN. Una descrizione di ndiswrapper è reperibile in `/usr/share/doc/packages/ndiswrapper/README.SUSE`quando viene installato il pacchetto `ndiswrapper`. Per informazioni più approfondite relative a ndiswrapper, fare riferimento al sito Web del progetto in`http://ndiswrapper.sourceforge.net/support.html`.

22.1.2 Funzione

Nel networking wireless, per garantire connessioni veloci, sicure e di qualità elevata vengono utilizzate varie tecniche e configurazioni. Tipologie operative differenti sono

adatte a configurazioni differenti. La scelta del giusto metodo di autenticazione potrebbe essere difficile. I metodi di cifratura disponibili presentano vantaggi e insidie.

Modalità operativa

In pratica, le reti wireless possono essere classificate come reti gestite e reti ad hoc. Le reti gestite hanno un elemento di gestione: il punto di accesso. Con questa modalità (definita anche modalità infrastruttura), tutte le connessioni delle stazioni WLAN nella rete vengono eseguite tramite il punto di accesso che può anche servire da connessione a una ethernet. Le reti ad hoc non hanno un punto di accesso. Le stazioni comunicano reciprocamente in modo diretto. Nelle reti ad hoc, l'intervallo di trasmissione e il numero di stazioni partecipanti sono molto limitati. Un punto di accesso è di solito più efficiente. È anche possibile utilizzare una scheda WLAN come punto di accesso. La maggior parte delle schede supporta questa funzione.

Siccome è molto più facile intercettare e compromettere una rete wireless rispetto a una rete cablata, i vari standard comprendono metodi di autenticazione e cifratura. Nella versione originale dello standard IEEE 802.11 sono riportati sotto la voce WEP. Comunque, siccome WEP si è rivelato non sicuro (vedere la sezione chiamata «Sicurezza» (p. 318)), il settore delle WLAN (associato con il nome di*Wi-Fi Alliance*) ha definito una nuova estensione chiamata WPA, che si pensa sia in grado di eliminare i punti deboli di WEP. L'ultimo standard IEEE 802.11i (chiamato anche WPA2, perchè WPA è basato su una versione bozza 802.11i) comprende il WPA e altri metodi di autenticazione e cifratura.

Autenticazione

Per essere sicuri che solo le stazioni autorizzate possono connettersi, nelle reti gestite vengono utilizzati vari meccanismi di autenticazione:

Aperto
: Un sistema aperto è un sistema che non richiede autenticazione. Qualsiasi stazione può collegarsi alla rete. Tuttavia è possibile utilizzare la cifratura WEP (vedere la sezione chiamata «Cifratura» (p. 314)).

Chiave condivisa (in base allo standard IEEE 802.11)
: In questa procedura, per l'autenticazione, viene utilizzata la chiave WEP, Non è comunque una procedura consigliata, in quanto rende la chiave WEP più soggetta agli attacchi. Un aggressore deve semplicemente ascoltare per un periodo di tempo

sufficientemente lungo la comunicazione tra la stazione e il punto di accesso. Durante il processo di autenticazione, entrambi i lati scambiano le stesse informazioni una volta in formato cifrato e una volta in formato non cifrato. Questo consente di ricostruire la chiave con strumenti adatti. Siccome con questo metodo viene utilizzata la chiave WEP per l'autenticazione e per la cifratura, questo non migliora la sicurezza della rete. Una stazione con la giusta chiave WEP è in grado di autenticare, cifrare e decifrare. Una stazione che non ha la chiave, non è in grado di decifrare i pacchetti ricevuti. Di conseguenza, non è in grado di comunicare, indipendentemente dal fatto che debba autenticarsi.

WPA-PSK (in base allo standard IEEE 802.1x)

La procedura WPA-PSK (PSK è l'acronimo di chiave precondivisa) opera in modo analogo alla procedura Chiave condivisa. Tutte le stazioni partecipanti e il punto di accesso devono avere la stessa chiave. La chiave ha una lunghezza di 256 bit e viene di solito immessa come stringa di cifratura. Il sistema non necessita di una gestione chiavi complessa come WPA-EAP ed è più adatto all'utilizzo privato. Tuttavia, WPA-PSK viene a volte chiamato WPA «Home».

WPA-EAP (in base allo standard IEEE 802.1x)

In realtà, WPA-EAP non è un sistema di autenticazione, ma un protocollo per il trasporto delle informazioni di autenticazione. WPA-EAP è utilizzato per proteggere le reti wireless nelle aziende. Nelle reti private, è poco diffuso. Per questo motivo, WPA-EAP viene a volte chiamato WPA «Enterprise».

Per l'autenticazione degli utenti, WPA-EAP necessita di un server Radius. EAP offre tre metodi diversi per la connessione al server e l'autenticazione. TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) e PEAP (Protected Extensible Authentication Protocol). In sintesi, queste opzioni funzionano in questo modo:

EAP-TLS

L'autenticazione TLS conta sullo scambio reciproco di certificati sia per il server, sia per il client. In primo luogo, il server presenta il suo certificato al client dove viene valutato. Se il certificato è ritenuto valido, il client a sua volta presenta il suo certificato al server. Anche se TLS è sicuro, richiede un'infrastruttura di gestione delle certificazioni operativa all'interno della rete. Questa infrastruttura si trova raramente nelle reti private.

EAP-TTLS e PEAP
Sia TTLS, sia PEAP, sono protocolli a due stadi. Nel primo stadio viene definito un'autenticazione sicura e, nel secondo, vengono scambiati i dati di autenticazione del client. Richiedono un overhead di gestione delle certificazioni molto inferiore rispetto a TLS.

Cifratura

Esistono vari metodi di cifratura per garantire che nessuna persona non autorizzata possa leggere i pacchetti di dati scambiati su una rete wireless o accedere alla rete:

WEP (definito nello standard IEEE 802.11)
Questo standard utilizza l'algoritmo di cifratura RC4, originariamente con una chiave avente una lunghezza di 40 bit, in seguito anche con 104 bit. Spesso, viene dichiarata una lunghezza di 64 o 128 bit, se sono inclusi i 24 bit del vettore di inizializzazione o meno. Questo standard ha comunque alcuni punti deboli. Gli attacchi contro le chiavi generati da questo sistema possono avere esito positivo. È quindi meglio utilizzare WEP che rinunciare del tutto alla cifratura della rete.

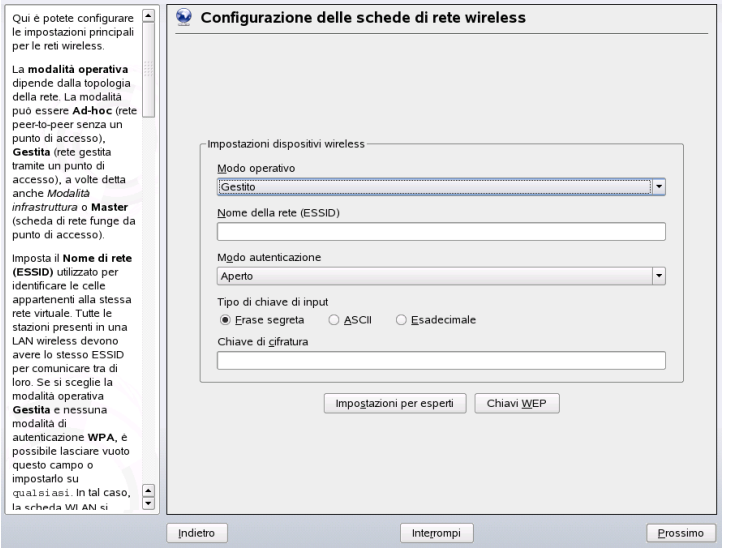
TKIP (definito nello standard WPA/IEEE 802.11i)
Questo protocollo di gestione delle chiavi definito nello standard WPA utilizza lo stesso algoritmo di cifratura di WEP, eliminandone i punti deboli. Poichè per ogni pacchetto viene generata una nuova chiave, gli attacchi nei confronti di queste chiavi non hanno esito positivo. TKIP è utilizzato insieme a WPA-PSK.

CCMP (definito nello standard IEEE 802.11i)
In CCMP è descritta la gestione delle chiavi. CCMP è di solito utilizzato insieme a WPA-EAP, ma può anche essere utilizzato con WPA-PSK. La cifratura avviene in base allo standard AES ed è più valida rispetto alla RC4 dello standard WEP.

22.1.3 Configurazione con YaST

Per configurare la scheda di rete wireless, avviare il modulo YaST *Network Card*. In *Network Address Setup*, selezionare il tipo di dispositivo *Wireless* e cliccare su *Avanti*. In *Wireless Network Card Configuration*, in Figura 22.1, «YaST: Configurazione della scheda di rete wireless» (p. 315), inserire le impostazioni principali per il funzionamento della WLAN:

Figura 22.1 *YaST: Configurazione della scheda di rete wireless*



Modalità operativa

È possibile integrare una stazione in una WLAN in tre modi diversi. Il modo più adatto dipende dalla rete nella quale comunicare: *Ad-hoc* (rete peer-to-peer senza punto di accesso), *Gestita* (la rete è gestita da un punto di accesso), o*Master* (la scheda di rete viene utilizzata come punto di accesso). Per utilizzare una qualsiasi delle modalità WPA-PSK o WPA-EAP, la modalità operativa deve essere impostata su*gestito*.

Nome di rete (ESSID)

Tutte le stazioni presenti in una rete wireless devono avere lo stesso ESSID per comunicare tra di loro. Se non viene indicato nulla, il punto di accesso viene automaticamente selezionato dalla scheda di rete e potrebbe anche non essere quello che si intendeva utilizzare.

Modalità di autenticazione

Selezionare un metodo di autenticazione adatto alla propria rete: *Aprire*, *Chiave condivisa*, *WPA-PSK*, o *WPA-EAP*. Se si seleziona l'autenticazione WPA, si deve impostare un nome di rete.

Impostazioni avanzate

Questo pulsante consente di aprire una finestra di dialogo per configurare in modo dettagliato la connessione WLAN. La descrizione dettagliata di questa finestra di dialogo è riportata in seguito.

Una volta terminate le impostazioni principali, la stazione è pronta per la distribuzione all'interno della WLAN.

IMPORTANTE: La sicurezza nelle reti wireless

Per proteggere il traffico di rete, accertarsi di utilizzare uno dei metodi di autenticazione e cifratura supportati. Le connessioni WLAN non cifrate, consentono a terzi di intercettare tutti i dati di rete. Anche una cifratura debole (WEP) è meglio di niente. Per informazioni consultare sezione chiamata «Cifratura» (p. 314) e sezione chiamata «Sicurezza» (p. 318).

In base al metodo di autenticazione selezionato, YaST invita a mettere a punto le impostazioni in un'altra finestra di dialogo. Per il meccanismo di autenticazione *Aperto*, non si deve configurare nulla in quanto questa impostazione implementa l'operazione di cifratura senza autenticazione.

Chiavi WEP

Impostare un tipo di input per la chiave. Scegliere tra *Stringa di cifratura*, *ASCII*, o *Esadecimale*. Per la cifratura dei dati trasmessi è possibile tenere fino a un massimo di quattro chiavi diverse. Cliccare su *Chiavi multiple* per entrare nella finestra di configurazione delle chiavi. Impostare la lunghezza della chiave: *128 bit* o *64 bit*. L'impostazione predefinita è *128 bit*. Nell'area di elencazione in basso nella finestra di dialogo, è possibile indicare fino a un massimo di quattro chiavi diverse da utilizzare per la cifratura della stazione. Premere *Imposta come predefinito* per indicarne una come chiave predefinita. A meno che non venga modificata, YaST utilizza come chiave predefinita la prima chiave immessa. Se la chiave standard viene cancellata, una delle altre chiavi deve essere contrassegnata manualmente come predefinita. Cliccare su*Modifica* per modificare le voci della lista o creare nuove chiavi. In questo caso, una finestra di pop-up invita a selezionare un tipo di input (*Stringa di cifratura*, *ASCII*, o*Esadecimale*). Se si seleziona *Stringa di cifratura*, immettere una parola o una stringa di caratteri dalla quale viene generata la chiave secondo la lunghezza precedentemente indicata. Per *ASCII* è richiesto un input di 5 caratteri per una chiave a 64 bit e di 13 caratteri per una chiave a 128 bit. Per *Esadecimale*, immettere 10 caratteri per una chiave a 64 bit e di 26 caratteri per una chiave a 128 bit.

WPA-PSK

Per immettere una chiave per WPA-PSK, selezionare il metodo di input*Stringa di cifratura* o *Esadecimale*. Nella modalità*Stringa di cifratura*, l'input deve essere da 8 a 63 caratteri. Nella modalità*Esadecimale*, immettere 64 caratteri.

WPA-EAP

Immettere le credenziali fornite dall'amministratore di rete. Per TLS, fornire il *Certificato del client* e il *Certificato del server*. TTLS e PEAP richiedono *Identità* e *Parola d'ordine*. Il *Certificato del server* è facoltativo. In YaST i certificati vengono cercati in`/etc/cert`, salvarli quindi in questa posizione e limitare l'accesso ai file a `0600` (proprietario lettura e scrittura).

Cliccare su*Impostazioni avanzate* per uscire dalla finestra di dialogo della configurazione di base della connessione WLAN e immettere la configurazione avanzata. In questa finestra, sono disponibili le seguenti opzioni:

Canale

Solo nelle modalità *Ad-hoc* e *Master* si deve indicare un canale sul quale la stazione WLAN deve lavorare. Nella modalità*Gestito*, la scheda cerca automaticamente i canali disponibili per i punti di accesso. In modalità*Ad-hoc*, selezionare uno dei 12 canali offerti per la comunicazione della propria stazione con le altre stazioni. In modalità*Master*, indicare su quale canale la scheda deve dare la funzionalità al punto di accesso. L'impostazione predefinita è *Auto*.

Velocità dei bit

In base alla prestazione della rete, per la trasmissione da un punto a un altro, è possibile impostare una certa velocità dei bit. Nell'impostazione predefinita*Auto*, all'interno del sistema, si cerca di utilizzare la velocità di trasmissione più alta. Alcune schede WLAN non supportano l'impostazione delle velocità dei bit.

Punto di accesso

In un ambiente con vari punti di accesso, è possibile selezionarne uno indicando l'indirizzo MAC.

Utilizzo di Power Management

Quando si è in viaggio, si utilizzano tecnologie per risparmiare energia e aumentare al massimo il tempo di funzionamento della batteria. Ulteriori informazioni relative a power management sono disponibili in Capitolo 21, *Risparmio energetico* (p. 283).

22.1.4 Utility

hostap (pacchetto `hostap`) è utilizzato per eseguire una scheda WLAN come punto di accesso. Ulteriori informazioni su questo pacchetto sono disponibili alla home page del progetto (`http://hostap.epitest.fi/`).

kismet (pacchetto `kismet`) è uno strumento di diagnosi della rete con il quale è possibile ascoltare il traffico del pacchetto WLAN. In questo modo è anche possibile rilevare tentativi di intrusione nella rete. Per ulteriori informazioni vedere `http://www.kismetwireless.net/` e la pagina man.

22.1.5 Suggerimenti e consigli per impostare una WLAN

Questi suggerimenti aiutano a migliorare la velocità, la stabilità e gli aspetti legati alla sicurezza della WLAN.

Stabilità e velocità

La prestazione e l'affidabilità di una rete wireless dipendono soprattutto dal fatto che le stazioni che vi partecipano ricevano o meno un segnale pulito dalle altre stazioni. Ostacoli come ad esempio i muri, indeboliscono notevolmente il segnale. Più cala la forza del segnale, più la trasmissione rallenta. Durante il funzionamento, controllare la forza del segnale con la utility iwconfig sulla riga di comando (campo `Link Quality`), o con KInternet in KDE. Se ci sono problemi per quanto riguarda la qualità del segnale, cercare di impostare i dispositivi altrove o regolare la posizione delle antenne dei punti di accesso. Per molte schede PCMCIA WLAN sono disponibili antenne aggiuntive che migliorano notevolmente la ricezione. La velocità indicata dal fabbricante, ad esempio 54 MBit/s, è un valore nominale che rappresenta il massimo teorico. In pratica, la velocità massima effettiva dei dati non è superiore alla metà di questo valore.

Sicurezza

Se si vuole impostare una rete wireless, è importante ricordare che chiunque nel raggio di trasmissione può facilmente accedervi se non vengono implementate misure di

sicurezza. Accertarsi quindi di attivare un metodo di cifratura. Tutte le schede WLAN e i punti di accesso supportano la cifratura WEP. Sebbene non sia del tutto sicura, è comunque un ostacolo per un potenziale aggressore. La cifratura WEP è adatta soprattutto all'utilizzo privato. Sarebbe meglio utilizzare la WPA-PSK, ma non è implementata nei vecchi punti di accesso o negli instradatori con la funzionalità WLAN. Su alcuni dispositivi, è possibile implementare WPA con un aggiornamento firmware. Inoltre la WPA non è supportata su tutti i componenti hardware Linux. Quando è stata preparata questa documentazione, WPA funzionava solo con le schede utilizzando chip Atheros, Intel PRO/Wireless, o Prism2/2.5/3. Su Prism2/2.5/3, la WPA funziona solo se viene utilizzato il driver hostap (vedere la sezione chiamata «Problemi con le schede Prism2» (p. 319)). Se la WPA non è disponibile, la cifratura WEP è meglio che niente. In aziende con esigenze di sicurezza avanzate, le reti wireless dovrebbero essere cifrate solo con WPA.

22.1.6 Soluzione dei problemi

Se la scheda WLAN non risponde, controllare se è stato scaricato il firmware necessario. Consultare la Sezione 22.1.1, «Hardware» (p. 310). I paragrafi riportati qui di seguito trattano alcuni problemi noti.

Dispositivi di rete multipli

I computer portatili moderni generalmente hanno una scheda di rete e una scheda WLAN. Se entrambi i dispositivi sono stati configurati con DHCP (assegnazione automatica dell'indirizzo) potrebbero esserci dei problemi con la risoluzione del nome e il gateway predefinito. Questo risulta evidente per il fatto che è possibile effettuare il ping con l'instradatore, ma non navigare in Internet. Il database di supporto in `http://portal.suse.com` riporta un articolo su questo argomento. Per trovare l'articolo, entrare in «DHCP» nella finestra di ricerca.

Problemi con le schede Prism2

Per i dispositivi con i chip Prism2, sono disponibili vari driver. Le diverse schede funzionano più o meno bene con i vari driver. Con queste schede, la cifratura WPA è possibile solo con il driver hostap. Se questa scheda non funziona correttamente o non funziona del tutto, o si vuole utilizzare la WPA, leggere `/usr/share/doc/packages/wireless-tools/README.prism2`.

WPA

Per SUSE Linux il supporto WPA è abbastanza nuovo e ancora in fase di sviluppo. In YaST non è quindi supportata la configurazione di tutti i metodi di autenticazione WPA. Non tutte le schede LAN wireless e i driver supportano WPA. Per abilitare WPA su alcune schede è necessario un aggiornamento firmware. Se si vuole utilizzare WPA, leggere `/usr/share/doc/packages/wireless-tools/README.wpa`.

22.1.7 Per ulteriori informazioni

Le pagine Internet di Jean Tourrilhes, che ha sviluppato gli *Strumenti wireless* per Linux, contengono molte informazioni utili sulle reti wireless. Vedere`http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`.

22.2 Bluetooth

Bluetooth è una tecnologia wireless per la connessione di dispositivi diversi, quali ad esempio cellulari, PDA, periferiche, computer portatili o componenti di sistema quali tastiera o mouse. Il nome deriva dal re danese Harold Bluetooth, che riunì diverse fazioni in guerra in Scandinavia. Il logo Bluetooth è basato sulle rune che corrispondono alla lettera «H» (assomiglia a una stella) e alla lettera «B».

Bluetooth si distingue da IrDA sotto molti aspetti importanti. Innanzitutto, non è necessario che i singoli dispositivi si «riconoscano» direttamente e, in secondo luogo, è possibile connettere diversi dispositivi alla rete. La velocità massima dei dati è 720 Kbps (nella versione corrente 1.2). In teoria, Bluetooth è in grado di comunicare persino attraverso le pareti. Nella pratica, tuttavia, la comunicazione dipende dalle proprietà della parete e dalla classe del dispositivo. Esistono tre classi di dispositivi con intervalli di trasmissione compresi tra dieci e cento metri.

22.2.1 Nozioni di base

Nelle sezioni seguenti vengono definiti i principi fondamentali del funzionamento di Bluetooth. Vengono fornite informazioni sui requisiti software necessari, sull'interazione di Bluetooth con il sistema e sul funzionamento dei profili Bluetooth.

Software

Per utilizzare Bluetooth, è necessario un adattatore Bluetooth (integrato o esterno), i driver e uno stack del protocollo Bluetooth. Il kernel di Linux contiene già i driver principali per l'utilizzo di Bluetooth. Il sistema Bluez viene utilizzato come stack di protocollo. Per assicurarsi che le applicazioni funzionino con Bluetooth, è necessario installare i pacchetti di base `bluez-libs` e `bluez-utils`. Questi pacchetti forniscono diversi servizi e utilità necessari. Alcuni adattatori, quali ad es.Broadcom o AVM BlueFritz!, richiedono inoltre l'installazione del pacchetto `bluez-firmware`. Il pacchetto `bluez-cups` consente la stampa tramite connessioni Bluetooth.

Interazione generale

Un sistema Bluetooth è composto da quattro strati interconnessi che forniscono la funzionalità desiderata:

Hardware
: L'adattatore e il driver adeguato per il supporto del kernel di Linux.

File di configurazione
: Utilizzati per il controllo del sistema Bluetooth.

Daemon
: Servizi che sono controllati dai file di configurazione e che forniscono la funzionalità.

Applicazioni
: Le applicazioni consentono la funzionalità fornita dai daemon che devono essere utilizzati e controllati dall'utente.

Quando si inserisce un adattatore Bluetooth, il sistema hotplug carica il relativo driver. Dopo aver caricato il driver, il sistema verifica i file di configurazione per controllare se è possibile avviare Bluetooth. In questo caso, stabilisce i servizi da avviare. Sulla base di queste informazioni, vengono avviati i rispettivi daemon. Gli adattatori Bluetooth vengono controllati dopo l'installazione. Quando ne viene rilevato uno o più di uno, Bluetooth viene abilitato. In caso contrario il sistema Bluetooth viene disattivato. Eventuali dispositivi Bluetooth aggiunti successivamente devono essere abilitati manualmente.

Profili

In Bluetooth, i servizi vengono definiti tramite i profili, quali ad es. il profilo di trasferimento dei file, il profilo principale di stampa e il profilo di rete personale PAN (personal area network). Per abilitare un dispositivo all'utilizzo dei servizi di un altro dispositivo, entrambi devono essere in grado di capire lo stesso profilo; questa parte di informazione di solito manca nel pacchetto e nel manuale del dispositivo. Purtroppo alcuni produttori non si uniformano rigorosamente alle definizioni dei singoli profili. Nonostante ciò, la comunicazione tra i dispositivi di norma funziona correttamente.

Nel testo seguente, i dispositivi locali sono quelli fisicamente connessi al computer. Tutti gli altri dispositivi ai quali è possibile accedere tramite connessioni wireless sono denominati dispositivi remoti.

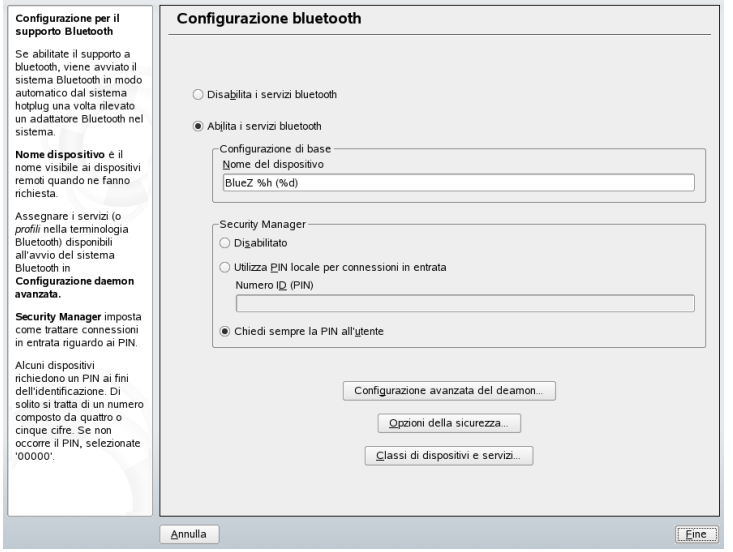
22.2.2 Configurazione

In questa sezione viene descritta la configurazione di Bluetooth. Vengono fornite informazioni sui file di configurazione utilizzati, gli strumenti necessari e le modalità di configurazione di Bluetooth tramite YaST oppure manualmente.

Configurazione di Bluetooth con YaST

Utilizzare il modulo Bluetooth di YaST, mostrato in Figura 22.2, «Configurazione di Bluetooth con YaST» (p. 323), per configurare il supporto Bluetooth nel sistema. Dopo che hotplug ha rilevato un adattatore Bluetooth nel sistema (ad es. durante l'avvio oppure all'inserimento dell'adattatore), Bluetooth viene avviato automaticamente con le impostazioni configurate in questo modulo.

Figura 22.2 *Configurazione di Bluetooth con YaST*



Stabilire nella prima fase di configurazione se i servizi Bluetooth debbano essere avviati nel sistema. Se sono stati abilitati i servizi Bluetooth, è necessario eseguire due configurazioni. Innanzitutto il *Nome dispositivo*. Questo è il nome visualizzato da altri dispositivi quando viene individuato il computer. Sono disponibili due segnaposto: `%h` che indica il nome host del sistema (utile, ad esempio, se viene assegnato in modo dinamico dal server DHCP) e `%d` che inserisce il numero dell'interfaccia (utile solo se è presente più di un adattatore Bluetooth nel computer). Ad esempio, se si immette `computer portatile %h` nel campo e il DHCP assegna il nome `unit123` al computer, gli altri dispositivi remoti lo risconosceranno come `computer portatile unit123`.

Il parametro *Security Manager* si riferisce al comportamento del sistema locale durante il tentativo di connessione di un dispositivo remoto. La differenza è nella gestione del numero PIN. È possibile consentire la connessione di qualsiasi dispositivo senza il PIN oppure stabilire le modalità di scelta del PIN corretto se viene richiesto. Immettere il PIN (memorizzato nel file di configurazione) nell'apposito campo di input. Quando un dispositivo si connette deve utilizzare prima di tutto questo PIN. Se non riesce, tenta di nuovo senza alcun PIN. Per ottenere la sicurezza ottimale, si consiglia di scegliere l'opzione *Always Ask User for PIN*. Questa opzione consente di utilizzare PIN diversi per dispositivi (remoti) diversi.

Fare clic su *Configurazione avanzata del daemon* per aprire la finestra di dialogo per la selezione e la configurazione dei servizi disponibili (denominati *profili* in Bluetooth). Tutti i servizi disponibili vengono visualizzati in un elenco; per attivarli o disattivarli fare clic su *Activate* oppure *Deactivate*. Fare clic su *Modifica* per aprire la finestra di dialogo in cui specificare argomenti aggiuntivi per il servizio selezionato (daemon). Si consiglia di non apportare nessuna modifica fino a quando non si è ascquistata familiarità con il servizio. Una volta completata la configurazione dei daemon, per uscire dalla finestra di dialogo fare clic su *OK*.

Nella finestra di dialogo principale, fare clic su *Opzioni di sicurezza* per aprire la finestra di dialogo della sicurezza e specificare le impostazioni di cifratura, di autenticazione e di scansione. Quindi uscire dalla finestra di dialogo della sicurezza e tornare alla finestra di dialogo principale. Dopo aver chiuso la finestra di dialogo principale con *Finish*, il sistema Bluetooth è pronto per l'utilizzo.

Dalla finestra di dialogo principale, è possibile anche aprire la finestra di dialogo *Classi di dispositivi e servizi*. I servizi Bluetooth sono raggruppati in varie classi di dispositivi. In questa finestra di dialogo, scegliere la classe corretta per il proprio computer, quale ad es.*Desktop* o *Laptop*. La classe di dispositivo non è molto importante, a differenza della classe di servizio, anche questa impostata in questa sede. A volte i dispositivi remoti Bluetooth, quali ad esempio i cellulari, consentono soltanto determinate funzioni se sono in grado di rilevare la classe di servizio corretta nel sistema. Ciò avviene spesso per i cellulari che prevedono una classe denominata *Transfer oggetto* prima di consentire il trasferimento di file dal o al computer. È possibile scegliere più classi. Non risulta utile selezionare tutte le classi «senza motivo.» Nella maggior parte dei casi la selezione di default si rivela appropriata.

Per utilizzare Bluetooth per la configurazione di una rete, attivare *PAND* nella finestra di dialogo *Configurazione avanzata del daemon* e impostare la modalità del daemon con *Modifica*. Per una connessione di rete Bluetooth funzionale, un PAND deve funzionare nella modalità *Listen* e il peer nella modalità *Search*. Per default, la modalità *Listen* è preimpostata. Adattare il comportamento del PAND locale. Configurare inoltre l'interfaccia `bnepX` (`X` indica il numero del dispositivo nel sistema) nel modulo *Scheda di rete* di YaST.

Configurazione manuale di Bluetooth

I file di configurazione dei singoli componenti del sistema Bluez si trovano nella directory `/etc/bluetooth`. Con la sola eccezione del file `/etc/sysconfig/bluetooth` per l'avvio dei componenti, che è modificato dal modulo di YaST.

I file di configurazione descritti di seguito possono essere modificati soltanto dall'utente `radice`. Attualmente, non esiste alcuna interfaccia utente grafica per la modifica di tutte le impostazioni. Le più importanti possono essere configurate mediante il modulo Bluetooth di YaST, descritto nella sezione chiamata «Configurazione di Bluetooth con YaST» (p. 322). Tutte le altre impostazioni sono rilevanti soltanto per gli utenti esperti che devono affrontare casi speciali. Di norma, le impostazioni di default risultano adeguate.

Un numero PIN fornisce la protezione di base contro connessioni indesiderate. I cellulari in genere chiedono il PIN al momento di stabilire il primo contatto (o quando viene configurato un contatto del dispositivo sul telefono). Perché due dispositivi siano in grado di comunicare, entrambi devono identificarsi con lo stesso PIN. Sul computer, il PIN si trova nel file `/etc/bluetooth/pin`.

IMPORTANTE: Sicurezza delle connessioni Bluetooth

Nonostante i numeri PIN, la trasmissione tra due dispositivi potrebbe non essere completamente sicura. Per default, l'autenticazione e la cifratura delle connessioni Bluetooth è disattivata. L'attivazione dell'autenticazione e della cifratura possono causare problemi di comunicazione con alcuni dispositivi Bluetooth.

Diverse impostazioni, quali ad esempio i nomi dei dispositivi e la modalità di sicurezza, possono essere modificate nel file di configurazione `/etc/bluetooth/hcid.conf`. Di norma, le impostazioni di default risultano adeguate. Il file contiene commenti che descrivono le opzioni delle diverse impostazioni.

Due sezioni nel file incluso sono definite come `opzioni` e `dispositivo`. La prima contiene informazioni generali che il file hcid utilizza per l'avvio. La seconda contiene impostazioni per i singoli dispositivi locali Bluetooth.

Una delle impostazioni più importanti della sezione `opzioni` è `sicurezza automatica;`. Se viene impostata su `auto`, il file hcid utilizzerà il PIN locale per le connessioni successive. Se non riesce, passa a `nessuna` e stabilisce comunque la

connessione. Per maggiore sicurezza, si consiglia di configurare questa impostazione di default su `utente` per assicurarsi che all'utente venga richiesto di immettere il PIN ogni volta che viene stabilita una connessione.

Impostare il nome da visualizzare sull'altro computer nella sezione `dispositivo`. La classe di dispositivo, quale ad esempio `Desktop`, `Laptop`, o `Server`, viene definita in questa sezione. È inoltre possibile abilitare o disabilitare l'autenticazione o la cifratura.

22.2.3 Componenti e utilità del sistema

L'operabilità di Bluetooth dipende dall'interazione dei diversi servizi. Sono necessari almeno due daemon di background: hcid (host controller interface daemon), che funge da interfaccia per il dispositivo Bluetooth e lo controlla, e sdpd (service discovery protocol daemon), che consente al dispositivo di individuare quali servizi sono resi disponibili dall'host. Se non vengono attivati automaticamente all'avvio del sistema, è possibile attivare sia hcid che sdpd con il comando `rcbluetooth start`. Questo comando può essere eseguito come utente `radice`.

Nei paragrafi seguenti vengono descritti in breve i maggiori strumenti shell da utilizzare con Bluetooth. Sebbene siano disponibili diversi componenti grafici per il controllo di Bluetooth, può risultare utile verificare questi programmi.

Alcuni dei comandi possono essere eseguiti solo come utente `radice`. Tra questi vi è il comando `l2ping` *`indirizzo_dispositivo`* per la verifica della connessione al dispositivo remoto.

hcitool

È possibile utilizzare hcitool per stabilire se sono stati rilevati dispositivi locali e remoti. Il comando `hcitool dev` elenca i dispositivi locali. L'output genera una riga nel formato *`nome_interfaccia indirizzo_dispositivo`* per ciascun dispositivo locale rilevato.

È possibile cercare i dispositivi remoti con il comando `hcitool inq`. Per ciascun dispositivo rilevato vengono restituiti tre valori: l'indirizzo del dispositivo, l'impostazione dell'orologio e la classe di dispositivo. L'indirizzo del dispositivo è importante poiché viene utilizzato dagli altri comandi per identificare il dispositivo di destinazione.

L'impostazione dell'orologio serve principalmente per motivi tecnici. La classe specifica il tipo di dispositivo e il tipo di servizio come valore esadecimale.

Il comando `hcitool nome` *`indirizzo-dispositivo`* può essere utilizzato per stabilire il nome del dispositivo di un dispositivo remoto. In caso di computer remoto, la classe e il nome del dispositivo corrispondono alle informazioni contenute in `/etc/bluetooth/hcid.conf`. Gli indirizzi dei dispositivi locali generano un output di errore.

hciconfig

Il comando `/usr/sbin/hciconfig` fornisce ulteriori informazioni sul dispositivo locale. Se `hciconfig` viene eseguito senza argomenti, l'output mostra le informazioni sul dispositivo, quali ad esempio il nome del dispositivo (`hciX`), l'indirizzo fisico del dispositivo (un numero a 12 cifre nel formato `00:12:34:56:78`) e le informazioni sulla quantità di dati da trasmettere.

`hciconfig nome hci0` visualizza il nome che viene restituito dal computer quando riceve delle richieste dai dispositivi remoti. Come per le richieste di impostazioni del dispositivo locale, `hciconfig` può essere utilizzato per modificare tali impostazioni. Ad esempio, `hciconfig PROVA nome hci0` imposta il nome su `PROVA`.

sdptool

È possibile utilizzare il programma sdptool per verificare quali servizi sono resi disponibili da un dispositivo specifico. Il comando `sdptool sfoglia` *`indirizzo_dispositivo`* restituisce tutti i servizi di un dispositivo. Utilizzare il comando `sdptool cerca` *`codice_servizio`* per cercare un servizio specifico. Questo comando esegue la scansione dei dispositivi accessibili per il servizio richiesto. Se uno dei dispositivi offre il servizio, il programma stampa il nome del servizio completo restituito dal dispositivo con una breve descrizione. Per visualizzare l'elenco di tutti i possibili codici di servizio, immettere `sdptool` senza parametri.

22.2.4 Applicazioni grafiche

In Konqueror, immettere l'URL `bluetooth:/` per elencare i dispositivi Bluetooth remoti. Fare doppio clic su un dispositivo per ottenere una panoramica dei servizi da esso forniti. Spostandosi su uno dei servizi specificati con il mouse, la barra di stato

del browser visualizza il profilo utilizzato dal servizio. Facendo clic sul servizio, si apre una finestra di dialogo dove specificare le operazioni da eseguire: salvare, utilizzare il servizio (è necessario avviare un'applicazione per farlo), oppure annullare l'azione. Contrassegnare la casella di controllo se non si desidera visualizzare di nuovo la finestra di dialogo ma si desidera che sia eseguita l'azione selezionata. Per alcuni servizi non è ancora disponibile il relativo supporto. Per altri è invece necessario installare pacchetti aggiuntivi.

22.2.5 Esempi

In questa sezione vengono forniti due esempi tipici di possibili scenari Bluetooth. Nel primo esempio viene mostrato come stabilire una connessione di rete tra due host tramite Bluetooth. Nel secondo viene mostrata la connessione tra un computer e un cellulare.

Connessione di rete tra due host

Nel primo esempio, viene stabilita una connessione di rete tra gli host *H1* e *H2*. I due host hanno gli indirizzi del dispositivo Bluetooth *baddr1* e *baddr2* (stabiliti su entrambi gli host con il comando `hcitool dev` come descritto sopra). È necessario identificare gli host con gli indirizzi IP `192.168.1.3` (*H1*) e `192.168.1.4` (*H2*).

La connessione Bluetooth viene stabilita utilizzando il pand (personal area networking daemon). I comandi seguenti devono essere eseguiti dall'utente `radice`. La descrizione concerne le azioni specifiche di Bluetooth e non fornisce una spiegazione dettagliata del comando di rete `ip`.

Immettere `pand -s` per avviare il pand nell'host *H1*. Successivamente, è possibile stabilire una connessione nell'host *H2* con il comando `pand -c` *`baddr1`*. Se si immette `ip link show` in uno degli host per elencare le interface di rete disponibili, l'output deve contenere una voce del tipo seguente:

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
 link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

Invece di `00:12:34:56:89:90`, l'output deve contenere l'indirizzo del dispositivo locale *baddr1* oppure *baddr2*. Ora è necessario assegnare un indirizzo IP a questa interfaccia e attivarla. In *H1*, l'operazione può essere eseguita con i due comandi seguenti:

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

In *H2*:

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Ora è possibile accedere a *H1* da *H2* tramite l'IP `192.168.1.3`. Utilizzare il comando `ssh 192.168.1.4` per accedere a *H2* da *H1*, premesso che *H2* esegua sshd, che in SUSE Linux è attivato per default. Il comando `ssh 192.168.1.4` può essere eseguito anche da un normale utente.

Trasferimento di dati da cellulare a computer

Nel secondo esempio viene mostrata la modalità di trasferimento di una fotografia creata con un cellulare con fotocamera digitale integrata a un computer (senza costi aggiuntivi per la trasmissione di un messaggio multimediale). Anche se la struttura dei menu può variare da cellulare a cellulare, in genere la procedura è piuttosto simile. Fare riferimento al manuale del cellulare, se necessario. In questo esempio viene descritto il trasferimento di una fotografia da un cellulare Sony Ericsson a un computer portatile. È necessario che il computer disponga del servizio Obex-Push e consenta l'accesso al cellulare. Nella prima fase, viene reso disponibile il servizio sul computer portatile. L'operazione viene eseguita con il daemon opd dal pacchetto `bluez-utils`. Avviare il daemon con il comando seguente:

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

Vengono utilizzati due parametri importanti: `--sdp` registra il servizio con sdpd e `--path /tmp` indica al programma dove salvare i dati ricevuti, in questo caso in `/tmp`. È anche possibile specificare qualsiasi altra directory per la quale si dispone di accesso in scrittura.

Ora il cellulare deve riconoscere il computer. Per eseguire questa operazione, aprire il menu *Connect* sul cellulare e selezionare *Bluetooth*. Se necessario, fare clic su *Turn On* prima di selezionare *My devices*. Selezionare *New device* e attendere che il cellulare cerchi il computer portatile. Quando viene rilevato un dispositivo, sul display ne viene visualizzato il nome. Selezionare il dispositivo associato al computer portatile. Se viene richiesto il PIN, immettere il PIN specificato in `/etc/bluetooth/pin`. A questo punto il cellulare riconosce il computer portatile ed è in grado di scambiare i dati con esso. Uscire dal menu corrente e passare al menu dell'immagine. Selezionare l'immagine da trasferire e premere *More*. Nel menu successivo, premere *Send* per selezionare una modalità di trasmissione. Selezionare *Via Bluetooth*. Nell'elenco deve essere visualizzato il computer portatile come dispositivo di destinazione. Selezionare il computer portatile

per avviare la trasmissione. L'immagine viene quindi salvata nella directory specificata con il comando `opd`. Con la stessa procedura è possibile trasferire sul computer portatile anche le tracce audio.

22.2.6 Risoluzione dei problemi

Nel caso si incontrino difficoltà per stabilire la connessione, si consiglia di procedere come descritto nell'elenco seguente. Tenere presente che l'errore può essere presente sia da una sola parte che da entrambe le parti. Identificare possibilmente il problema con un altro dispositivo Bluetooth per verificare che il dispositivo non sia difettoso.

Verificare che il dispositivo locale sia elencato nell'output di `hcitool dev`.
Nel caso non sia elencato in questo output, hcid non viene avviato oppure il dispositivo non viene riconosciuto come dispositivo Bluetooth. Le cause possono essere diverse. Il dispositivo potrebbe essere difettoso oppure potrebbe mancare il driver corretto. I computer portatili con Bluetooth integrato in genere dispongono di un comando di accensione e spegnimento per i dispositivi wireless, quali ad esempio WLAN e Bluetooth. Controllare nel manuale del computer portatile se questo comando è presente. Riavviare il sistema Bluetooth con il comando `rcbluetooth restart` e verificare la presenza di eventuali errori in `/var/log/messages`.

Verificare se l'adattatore Bluetooth necessita di un file firmware.
In caso positivo, installare `bluez-bluefw` e riavviare il sistema Bluetooth con il comando `rcbluetooth restart`.

Verificare se l'output di `hcitool inq` restituisce altri dispositivi.
Ripetere questo comando più di una volta. Potrebbero esserci interferenze nella connessione poiché la banda di frequenza di Bluetooth viene utilizzata anche da altri dispositivi.

Verificare che i PIN corrispondano.
Verificare che il numero PIN del computer (in `/etc/bluetooth/pin`) corrisponda a quello del dispositivo di destinazione.

Verificare se il dispositivo remoto«riconosce» il computer.
Stabilire la connessione dal dispositivo remoto. Verificare se questo dispositivo riconosce il computer.

Verificare se è possibile stabilire una connessione di rete (vedere la sezione chiamata «Connessione di rete tra due host» (p. 328)).

È possibile che la configurazione descritta nella sezione chiamata «Connessione di rete tra due host» (p. 328) non funzioni per diversi motivi. Ad esempio, è possibile che uno dei due computer non supporti il protocollo ssh. Provare il `ping 192.168.1.3` oppure il `ping 192.168.1.4`. Se funziona, verificare che sshd sia attivo. Un altro possibile problema è che uno dei due dispositivi dispone già di impostazioni di rete che sono in conflitto con l'indirizzo `192.168.1.X` dell'esempio. In questo caso, provare indirizzi diversi, quali ad esempio `10.123.1.2` e `10.123.1.3`.

Verificare che il computer portatile sia visualizzato come dispositivo di destinazione (vedere sezione chiamata «Trasferimento di dati da cellulare a computer» (p. 329)).

Verificare che il dispositivo mobile riconosca il servizio Obex-Push del computer portatile.

In *My devices*, selezionare il dispositivo rispettivo e visualizzare l'elenco dei *Services*. Nel caso Obex-Push non sia visualizzato (anche dopo l'aggiornamento dell'elenco), il problema è dovuto a opd sul computer portatile. Verificare che opd si attivo. Verificare se si dispone dell'accesso in scrittura nella directory specificata.

Verificare che lo scenario descritto nella sezione chiamata «Trasferimento di dati da cellulare a computer» (p. 329) funzioni anche nell'altro senso.

Se è installato il pacchetto `obexftp`, su alcuni dispositivi è possibile utilizzare il comando `obexftp -b` *`indirizzo_dispositivo`* `-B 10 -p` *`immagine`*. Su alcuni modelli di cellulari Siemens e Sony Ericsson è stata eseguita la prova con risultati positivi. Per ulteriori informazioni, fare riferimento alla documentazione in `/usr/share/doc/packages/obexftp`.

22.2.7 Per ulteriori informazioni

Per una panoramica completa delle varie istruzioni per l'uso e la configurazione di Bluetooth, visitare il sito `http://www.holtmann.org/linux/bluetooth/`. Per ulteriori informazioni e istruzioni, vedere:

- HOWTO ufficiale dello stack del protocollo Bluetooth integrato nel kernel: `http://bluez.sourceforge.net/howto/index.html`
- Connessione a PDA PalmOS: `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`

22.3 Trasmissione dati a infrarossi

IrDA (Infrared Data Association) è uno standard industriale per la comunicazione wireless a raggi infrarossi. Molti computer portatili attualmente in commercio sono dotati di ricetrasmettitori compatibili IrDA che consentono la comunicazione con altri dispositivi quali ad es. stampanti, modem, LAN o altri computer portatili. La velocità di trasferimento va da 2400 bps a 4 Mbps.

Esistono due modalità di funzionamento IrDA. La modalità standard, SIR, accede alla porta infrarossi tramite interfaccia seriale. Questa modalità funziona su quasi tutti i sistemi ed è sufficiente per la maggior parte dei requisiti. La modalità più veloce, FIR, richiede un driver speciale per il chip IrDA. Non tutti i tipi di chip sono supportati nella modalità FIR poiché mancano driver appropriati. Impostare la modalità IrDA desiderata nel BIOS del computer. Il BIOS indica anche l'interfaccia seriale utilizzata nella modalità SIR.

Ulteriori informazioni su IrDA sono disponibili nel documento IrDA HOWTO di Werner all'indirizzo `http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html`. Fare inoltre riferimento al sito del progetto Linux IrDA all'indirizzo `http://irda.sourceforge.net/`.

22.3.1 Software

I moduli necessari per il kernel sono inclusi nel pacchetto del kernel. Il pacchetto `irda` fornisce applicazioni helper per il supporto dell'interfaccia a infrarossi. È possibile consultare la documentazione in `/usr/share/doc/packages/irda/README` dopo aver installato il pacchetto.

22.3.2 Configurazione

Il servizio del sistema IrDA non viene avviato automaticamente all'avvio del sistema. Utilizzare il modulo IrDA di YaST per l'attivazione. In questo modulo è possibile modificare soltanto un'impostazione: l'interfaccia seriale del dispositivo a infrarossi. La finestra di verifica indica due output. Uno è l'output di `irdadump`, che registra tutti i pacchetti IrDA inviati e ricevuti. Questo output deve contenere il nome del computer e i nomi di tutti i dispositivi a infrarossi nell'intervallo di trasmissione. Un esempio di questi messaggi viene mostrato in Sezione 22.3.4, «Risoluzione dei problemi» (p. 334).

Tutti i dispositivi per i quali esiste una connessione IrDA sono elencati nella parte inferiore della finestra.

La connessione IrDA consuma una notevole quantità di alimentazione a batteria poiché ogni pochi secondi viene inviato un pacchetto di rilevamento per rilevare altri dispositivi periferici. Perciò, è necessario avviare la connessione IrDA solo se necessario nel caso si utilizzi l'alimentazione a batteria. Immettere il comando `rcirda start` per avviarla oppure `rcirda stop` per disattivarla. Quando si attiva l'interfaccia, vengono caricati automaticamente tutti i moduli del kernel necessari.

È possibile eseguire la configurazione manuale nel file `/etc/sysconfig/irda`. Questo file contiene una sola variabile, `IRDA_PORT`, che stabilisce l'interfaccia da utilizzare nella modalità SIR.

22.3.3 Utilizzo

I dati possono essere inviati al file di dispositivo `/dev/irlpt0` per la stampa. Il file di dispositivo `/dev/irlpt0` funge come la normale interfaccia cablata `/dev/lp0`, a meno che i dati di stampa siano inviati wireless a raggi infrarossi. Per la stampa, assicurarsi che la stampante si trovi nell'intervallo di visualizzazione dell'interfaccia a infrarossi del computer e che il supporto a infrarossi sia avviato.

Una stampante gestita tramite interfaccia a infrarossi può essere configurata con il modulo stampante di YaST. Poiché non viene rilevata automaticamente, è possibile configurarla facendo clic su *Altro (non rilevato)*. Nella finestra di dialogo seguente, selezionare *IrDA printer*. In genere, `irlpt0` è la connessione giusta. Informazioni dettagliate sul funzionamento delle stampanti in Linux sono disponibili in Capitolo 31, *Uso della stampante* (p. 501).

La comunicazione con altri host e con i cellulari o con altri dispositivi simili viene effettuata tramite il file dispositivo `/dev/ircomm0`. I cellulari Siemens S25 e Nokia 6210, ad esempio, possono eseguire la connessione a Internet con l'applicazione wvdial utilizzando l'interfaccia a infrarossi. È anche possibile la sincronizzazione dei dati con un Palm Pilot, a condizione che l'impostazione del dispositivo dell'applicazione corrispondente sia stata configurata su `/dev/ircomm0`.

Se lo si desidera, è possibile indicare soltanto dispositivi che supportano la stampante o i protocolli IrCOMM. È possibile accedere con applicazioni speciali, quali ad esempio irobexpalm e irobexreceive, a dispositivi che supportano il protocollo IROBEX, quali

ad esempio il Palm Pilot di 3Com. Per ulteriori informazioni, fare riferimento a *IR-HOWTO* (http://tldp.org/HOWTO/Infrared-HOWTO/). I protocolli supportati dal dispositivo sono elencati in parentesi dopo il nome del dispositivo nell'output di `irdadump`. Il supporto del protocollo IrLAN è ancora «in fase di sviluppo.»

22.3.4 Risoluzione dei problemi

Se i dispositivi connessi alla porta a infrarossi non rispondono, utilizzare il comando `irdadump` (come `radice`) verificare se l'altro dispositivo viene riconosciuto dal computer. Viene visualizzato regolarmente un messaggio simile a Esempio 22.1, «Output di irdadump» (p. 334) quando nell'intervallo di visualizzazione è presente la stampante Canon BJC-80:

Esempio 22.1 *Output di irdadump*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* earth
                        hint=0500 [ PnP Computer ] (21)
```

Verificare che nella configurazione dell'interfaccia non vi sia alcun output o che l'altro dispositivo non risponda. Verificare che sia utilizzata l'interfaccia corretta. L'interfaccia a infrarossi viene ubicata talvolta in `/dev/ttyS2` oppure in `/dev/ttyS3` e a volte viene utilizzata un'interruzione diversa da IRQ 3. Queste impostazioni possono essere verificate e modificate nel menu di configurazione del BIOS di quasi tutti i computer portatili.

Per stabilire se le luci della spia a infrarossi si accendono può essere sufficiente anche una semplice videocamera. La maggior parte delle videocamere sono in grado di vedere la luce a infrarossi che sfugge all'occhio umano.

Parte VII. Amministrazione

23 Sicurezza in Linux

Mascheramento e firewall assicurano un flusso di dati e scambio di dati monitorato. SSH (secure shell) permette di eseguire il log in su host remoti per via di una connessione cifrata. Cifrando dei file o intere partizioni mette a riparo i vostri dati anche nel caso in cui delle persone inautorizzate riuscissero ad accedere al vostro sistema. Insieme alle istruzioni tecniche sono disponibili informazioni sugli aspetti della sicurezza delle reti Linux.

23.1 Mascheramento e firewall

Quando Linux viene utilizzato in un ambiente di rete, vengono rese disponibili le funzioni del kernel che consentono la manipolazione dei pacchetti di rete per mantenere separate le aree interne ed esterne della rete. Il framework netfilter di Linux è il mezzo mediante il quale creare un firewall di rete efficace per mantenere separate le varie reti. Unitamente a iptables, una struttura di tabella generica per la definizione di set di regole, consente di controllare quali pacchetti sono consentiti attraverso un'interfaccia di rete. Questo filtro di pacchetti può essere impostato molto facilmente mediante SuSEfirewall2 e il modulo YaST corrispondente.

23.1.1 Filtro di pacchetti con iptables

I componenti netfilter e iptables vengono utilizzati per filtrare e manipolare i pacchetti di rete e per la conversione degli indirizzi di rete (NAT). I criteri di filtro e le eventuali azioni ad essi associate sono memorizzati in concatenamenti, ai quali devono corrispondere in sequenza i singoli pacchetti di rete all'arrivo. Tali concatenamenti sono

memorizzati in tabelle che possono essere modificate, insieme ai set di regole, mediante il comando `iptables`.

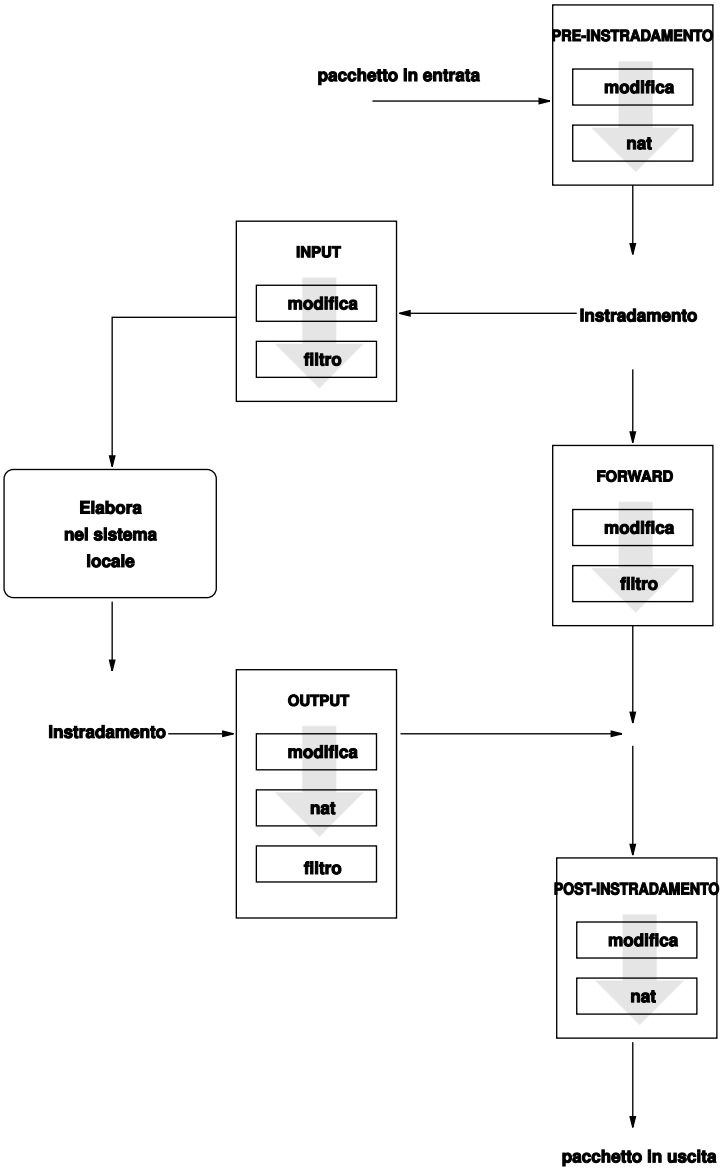
Nel kernel Linux vengono gestite tre tabelle, ognuna per una particolare categoria di funzioni del filtro di pacchetti:

filtro
: In questa tabella è memorizzata la maggior parte delle regole del filtro poiché implementa il meccanismo di *filtro di pacchetti* nel senso più stretto del termine e determina, ad esempio, se i pacchetti vengono accettati (`ACCEPT`) o scartati (`DROP`).

nat
: In questa tabella vengono definite le eventuali modifiche agli indirizzi di origine e di destinazione dei pacchetti. L'uso di queste funzioni consente inoltre di implementare il *mascheramento*, un tipo speciale di NAT utilizzato per collegare una rete privata a Internet.

mangle
: Le regole contenute in questa tabella consentono di manipolare i valori memorizzati nelle intestazioni IP, ad esempio il tipo di servizio.

Figura 23.1 *iptables: possibili percorsi di un pacchetto*



In queste tabelle sono presenti diversi concatenamenti predefiniti per la corrispondenza dei pacchetti:

PREROUTING
Questo concatenamento viene applicato ai pacchetti in entrata.

INPUT
Questo concatenamento viene applicato ai pacchetti destinati ai processi interni del sistema.

FORWARD
Questo concatenamento viene applicato ai pacchetti che sono solo instradati attraverso il sistema.

OUTPUT
Questo concatenamento viene applicato ai pacchetti che hanno origine dal sistema stesso.

POSTROUTING
Questo concatenamento viene applicato a tutti i pacchetti in uscita.

Nella Figura 23.1, «iptables: possibili percorsi di un pacchetto» (p. 339) vengono illustrati i possibili percorsi di un pacchetto di rete in un dato sistema. Ai fini della semplicità, nella figura le tabelle sono elencate come parti di concatenamenti, ma in realtà questi concatenamenti si trovano all'interno delle tabelle stesse.

Nel caso più semplice possibile un pacchetto in entrata destinato al sistema viene ricevuto dall'interfaccia `eth0`. Il pacchetto viene assegnato prima al concatenamento `PREROUTING` della tabella `mangle`, quindi al concatenamento `PREROUTING` della tabella `nat`. Il passaggio seguente, che si riferisce all'instradamento del pacchetto, determina che la destinazione effettiva del pacchetto è un processo del sistema stesso. Dopo il passaggio dei concatenamenti `INPUT` delle tabelle `mangle` e `filter`, il pacchetto raggiunge la destinazione finale, a condizione che vi sia una corrispondenza effettiva con le regole della tabella `filter`.

23.1.2 Nozioni di base sul mascheramento

Il mascheramento è il formato di NAT (Network Address Translation) specifico di Linux. Può essere utilizzato per la connessione di una piccola LAN, in cui gli host utilizzano indirizzi IP dall'intervallo privato (vedere la Sezione 38.1.2, «Maschere di rete e instradamento» (p. 599)), a Internet dove vengono utilizzati indirizzi IP ufficiali. Per consentire agli host della LAN di connettersi a Internet, i relativi indirizzi privati

vengono convertiti in indirizzi ufficiali mediante il router che funge da gateway tra la LAN e Internet. Il principio sottostante è semplice poiché il router dispone di più interfacce di rete, di solito una scheda di rete e un'interfaccia separata per la connessione a Internet. Mentre quest'ultima collega il router alla rete mondiale esterna, una o più ulteriori interfacce lo collegano agli host della LAN. Il collegamento di tali host nella rete locale alla scheda di rete del router, ad esempio `eth0`, consente di inviare al relativo gateway o router di default qualsiasi pacchetto non destinato alla rete locale.

IMPORTANTE: uso della maschera di rete corretta

Durante la configurazione della rete verificare che l'indirizzo di diffusione e la maschera di rete siano gli stessi per tutti gli host locali. In caso contrario, i pacchetti non potranno essere instradati nel modo corretto.

Come accennato in precedenza, ogni volta che un host della LAN invia pacchetti destinati a un indirizzo Internet, questi vengono instradati al router di default il quale deve essere configurato prima che tali pacchetti possano essere inoltrati. Per motivi di sicurezza, questa funzionalità non è abilitata in un'installazione di default di SUSE Linux. Per abilitare l'inoltro di pacchetti, impostare la variabile `IP_FORWARD` nel file `/etc/sysconfig/sysctl` su `IP_FORWARD=yes`.

Il router è visibile all'host di destinazione della connessione che tuttavia non dispone di alcun tipo di informazioni sull'host residente nella rete interna dalla quale hanno avuto origine i pacchetti. Questa tecnica viene infatti definita mascheramento. A causa della conversione degli indirizzi, il router è la prima destinazione di tutti i pacchetti di risposta. Affinché i pacchetti in entrata possano essere inoltrati all'host corretto nella rete locale, è necessario che il router li identifichi e converta i relativi indirizzi di destinazione.

Poiché il traffico in entrata dipende dalla tabella di mascheramento, non è assolutamente possibile aprire una connessione a un host interno dalla rete esterna, in quanto nella tabella non sono presenti voci per una connessione di questo tipo. Per qualsiasi connessione già stabilita, nella tabella è inoltre assegnata una voce relativa allo stato, quindi tale voce non può essere utilizzata da un'altra connessione.

È dunque possibile che si verifichino problemi con alcuni protocolli applicativi, ad esempio ICQ, cucme, IRC (DCC, CTCP) e FTP (in modalità PORT). Netscape, il programma FTP standard, e molti altri utilizzano PASV, una modalità passiva molto meno problematica per quanto riguarda il filtro di pacchetti e il mascheramento.

23.1.3 Nozioni di base sui firewall

Firewall è probabilmente il termine più ampiamente utilizzato per descrivere un meccanismo per la creazione e la gestione di un collegamento tra reti, oltre che per il controllo del flusso di dati tra di esse. Più precisamente, il meccanismo descritto in questa sezione è definito *filtro di pacchetti*. Un filtro di pacchetti è preposto alla regolazione del flusso di dati in base a determinati criteri, ad esempio protocolli, porte e indirizzi IP, e consente di bloccare i pacchetti che, secondo i relativi indirizzi, non dovrebbero presumibilmente raggiungere la rete. Per consentire, ad esempio, l'accesso pubblico al server Web in uso, aprire la porta corrispondente in maniera esplicita. Un filtro di pacchetti non effettua tuttavia la scansione del contenuto di pacchetti con indirizzi validi come quelli destinati al server Web. Se, ad esempio, i pacchetti in entrata avessero lo scopo di compromettere un programma CGI sul server Web, il filtro di pacchetti ne consentirebbe comunque l'ingresso.

Un meccanismo più efficace, ma più complesso, consiste nel combinare più tipi di sistemi in modo da ottenere, ad esempio, l'interazione tra un filtro di pacchetti e un gateway applicativo o un proxy, nel qual caso il filtro di pacchetti rifiuta tutti i pacchetti destinati alle porte disabilitate e accetta solo i pacchetti indirizzati al gateway applicativo. Questo gateway o proxy funge da client del server effettivo e, in un certo senso, il proxy può essere considerato un host di mascheramento al livello del protocollo utilizzato dall'applicazione. Il proxy Squid, un server proxy HTTP, ne è un esempio. Per utilizzare Squid, è necessario configurare la comunicazione del browser tramite il proxy. Tutte le pagine HTTP richieste vengono fornite dalla cache del proxy e le pagine non disponibili nella cache vengono recuperate da Internet mediante il proxy. Per fare un altro esempio, SUSE Proxy Suite (`proxy-suite`) include un proxy per il protocollo FTP.

Nella sezione seguente viene descritto il filtro di pacchetti fornito con SUSE Linux. Per ulteriori informazioni sul filtro di pacchetti e sui firewall, leggere la documentazione HOWTO di Linux su Firewall inclusa nel pacchetto `howto`. Se il pacchetto è installato, utilizzare `less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz` per accedere a tale documentazione.

23.1.4 SuSEfirewall2

SuSEfirewall2 è uno script utilizzato per leggere le variabili impostate nel file `/etc/sysconfig/SuSEfirewall2` e generare un set di regole di iptables. Consente di

definire tre zone di sicurezza, tuttavia nella configurazione di esempio seguente vengono considerate solo la prima e la seconda:

Zona esterna
Poiché non vi è modo di esercitare alcun controllo sulla rete esterna, è necessario impedire l'accesso all'host dall'esterno. Nella maggior parte dei casi la rete esterna si identifica con Internet, ma potrebbe trattarsi di un'altra rete non sicura, ad esempio una WLAN.

Zona interna
Identifica la rete privata, quasi sempre la LAN. Se gli host in questa rete utilizzano indirizzi IP dall'intervallo privato (vedere la Sezione 38.1.2, «Maschere di rete e instradamento» (p. 599)), abilitare la conversione degli indirizzi di rete (NAT) in modo che gli host della rete interna possano accedere alla rete esterna.

Demilitarized Zone (DMZ)
Gli host che si trovano in questa zona possono essere raggiunti sia dalla rete esterna che dalla rete interna, ma non possono accedere alla rete interna. Questa configurazione consente di aggiungere un'ulteriore linea di difesa alla rete interna, essendo i sistemi DMZ isolati da questa rete.

Qualsiasi tipo di traffico di rete non esplicitamente consentito dalla regola di filtraggio viene soppresso da iptables, pertanto ogni interfaccia con traffico in entrata deve essere inserita in una delle tre zone. Definire per ogni zona i protocolli o i servizi consentiti. La regola impostata viene applicata solo ai pacchetti che hanno origine dagli host remoti, mentre i pacchetti generati localmente non vengono catturati dal firewall.

La configurazione può essere eseguita mediante YaST (vedere la sezione chiamata «Configurazione con YaST» (p. 343)) oppure manualmente tramite il file `/etc/sysconfig/SuSEfirewall2` che è commentato in modo chiaro. Nel file `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES` sono inoltre disponibili numerosi scenari di esempio.

Configurazione con YaST

IMPORTANTE: configurazione automatica del firewall

Dopo l'installazione viene avviato automaticamente un firewall da parte di YaST su tutte le interfacce configurate. Se nel sistema è configurato e attivato un

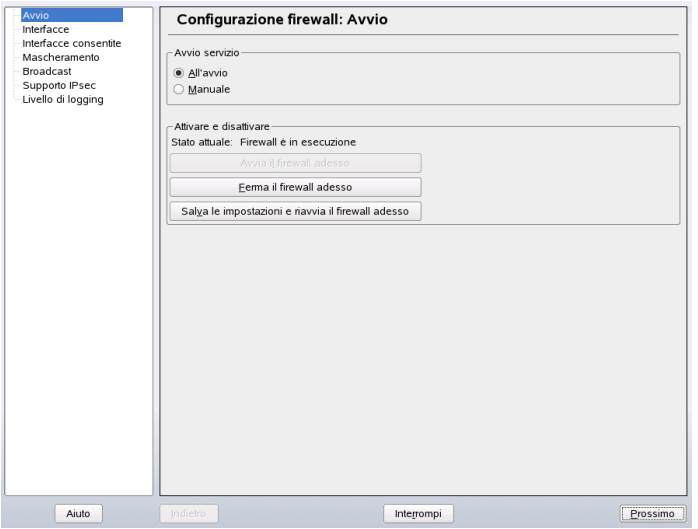
server, YaST è in grado di modificare la configurazione del firewall generata automaticamente mediante l'opzione *Apri il firewall per l'interfaccia selezionata* o *Porta aperta nel firewall* nei moduli di configurazione del server. In alcune finestre di dialogo dei moduli del server è presente il pulsante *Dettagli firewall* che consente l'attivazione di ulteriori servizi e porte. È possibile utilizzare il modulo di configurazione del firewall di YaST per attivare, disattivare o riconfigurare il firewall.

Le finestre di dialogo di YaST per la configurazione grafica sono accessibili dal centro controllo YaST. Selezionare *Sicurezza e utenti* → *Firewall*. La configurazione è suddivisa in sette sezioni a cui è possibile accedere direttamente dalla struttura dell'albero sul lato sinistro.

Avvio

In questa finestra di dialogo è possibile impostare il comportamento all'avvio. In un'installazione di default SuSEfirewall2 viene avviato automaticamente, tuttavia è possibile impostarne l'avvio e l'interruzione tramite questa finestra. Per implementare le nuove impostazioni in un firewall in esecuzione, utilizzare *Salva le impostazioni e riavvia il firewall adesso*.

Figura 23.2 *Configurazione del firewall con YaST*



Interfacce

In questa finestra di dialogo sono elencate tutte le interfacce di rete conosciute. Per rimuovere un'interfaccia da una zona, selezionare l'interfaccia, fare clic su *Modifica*, quindi scegliere *Non è stata assegnata alcuna zona*. Per aggiungere un'interfaccia a una zona, selezionare l'interfaccia, fare clic su *Modifica*, quindi scegliere una delle zone disponibili. È inoltre possibile scegliere *Personalizza* per creare un'interfaccia speciale con impostazioni personalizzate.

Servizi consentiti

È necessario impostare questa opzione per offrire servizi dal sistema in uso a una zona dalla quale è protetto. Per default, il sistema è protetto solo dalle zone esterne. Consentire esplicitamente i servizi che dovranno essere accessibili agli host esterni. Attivare i servizi dopo aver selezionato la zona desiderata in *Servizi consentiti per la zona selezionata*.

Mascheramento

Il mascheramento consente di nascondere la rete interna dalle reti esterne, ad esempio Internet, mentre consente agli host nella rete interna di accedere in maniera trasparente alla rete esterna. Le richieste dalla rete esterna a quella interna vengono bloccate, mentre le richieste dalla rete interna vengono viste dall'esterno come se fossero generate dal server di mascheramento. Se è necessario che servizi speciali in un computer interno siano disponibili alla rete esterna, aggiungere regole di reindirizzamento speciali per i servizi desiderati.

Diffusione

In questa finestra di dialogo è possibile configurare le porte UDP che consentono le diffusioni. Aggiungere i numeri di porta o i servizi necessari alla zona appropriata separati da spazi. Vedere anche il file `/etc/services`.

In questa finestra è possibile abilitare la registrazione delle diffusioni non accettate. Questo aspetto potrebbe risultare problematico, in quanto gli host Windows utilizzano diffusioni per il riconoscimento reciproco e di conseguenza generano molti pacchetti che non vengono accettati.

Supporto IPsec

In questa finestra di dialogo è possibile configurare la disponibilità del servizio IPsec per la rete esterna. Specificare quali pacchetti sono considerati sicuri in *Dettagli*.

Livello di log
: Per la registrazione è possibile utilizzare due regole, ovvero pacchetti accettati e pacchetti non accettati. I pacchetti non accettati sono identificati mediante DROPPED o REJECTED. Selezionare *Protocolla tutto*, *Protocolla solo pacchetti cruciali* oppure *Non protocollare niente* per entrambi.

Dopo aver completato la configurazione del firewall, scegliere *Avanti* per chiudere la finestra di dialogo. Viene aperto un riepilogo basato sulle zone della configurazione del firewall. Controllare tutte le impostazioni. Tutti i servizi, le porte e i protocolli consentiti sono elencati in questo riepilogo. Per modificare la configurazione, scegliere *Indietro*. Per salvare la configurazione, fare clic su *Accetta*.

Configurazione manuale

Nei paragrafi seguenti vengono fornite istruzioni dettagliate per una corretta configurazione. Per ogni voce della configurazione è indicato se si riferisce al firewall o al mascheramento. Non sono invece trattati gli aspetti che riguardano DMZ (Demilitarized Zone) descritti nel file di configurazione, in quanto sono applicabili solo a infrastrutture di rete più complesse di grandi organizzazioni (reti aziendali), che richiedono una configurazione più vasta e una conoscenza approfondita dell'argomento.

Utilizzare innanzitutto il modulo YaST relativo ai servizi di sistema (Runlevel) per abilitare SuSEfirewall2 nel runlevel in uso (3 o più probabilmente 5) e impostare i collegamenti simbolici per gli script SuSEfirewall2_* nelle directory `/etc/init.d/rc?.d/`.

`FW_DEV_EXT` (firewall, mascheramento)
: Il dispositivo collegato a Internet. Per una connessione via modem immettere `ppp0`. Per un collegamento ISDN utilizzare `ippp0`. Per le connessioni DSL utilizzare `dsl0`. Specificare `auto` per utilizzare l'interfaccia corrispondente all'instradamento di default.

`FW_DEV_INT` (firewall, mascheramento)
: Il dispositivo collegato alla rete privata interna (ad esempio `eth0`). Lasciare vuota questa voce se non esiste una rete interna e il firewall viene utilizzato solo per proteggere l'host sul quale è in esecuzione.

FW_ROUTE (firewall, mascheramento)
Se è necessario utilizzare la funzione di mascheramento, impostare questa voce su `yes`. Gli host interni non saranno visibili all'esterno, poiché i relativi indirizzi di rete privata (ad esempio, `192.168.x.x`) vengono ignorati dai router su Internet.

Per un firewall senza mascheramento impostare questa voce su `yes` solo se si desidera consentire l'accesso alla rete interna. In questo caso gli host interni dovranno utilizzare indirizzi IP registrati ufficialmente. Normalmente l'accesso dall'esterno alla rete interna *non* dovrebbe essere consentito.

FW_MASQUERADE (mascheramento)
Impostare questa voce su `yes` se è necessario utilizzare la funzione di mascheramento. In questo modo si ottiene una connessione virtualmente diretta a Internet per gli host interni. Tra gli host della rete interna e Internet è tuttavia più sicuro utilizzare un server proxy. Il mascheramento non è necessario per i servizi forniti da un server proxy.

FW_MASQ_NETS (mascheramento)
Specificare gli host o le reti da mascherare lasciando uno spazio tra le singole voci. Ad esempio:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (firewall)
Impostare questa voce su `yes` per proteggere l'host firewall da attacchi che hanno origine nella rete interna. I servizi sono disponibili per la rete interna solo se vengono abilitati esplicitamente. Vedere anche `FW_SERVICES_INT_TCP` e `FW_SERVICES_INT_UDP`.

FW_SERVICES_EXT_TCP (firewall)
Immettere le porte TCP che dovranno essere disponibili. Lasciare vuota questa voce per una normale workstation in una configurazione domestica che non offre alcun servizio.

FW_SERVICES_EXT_UDP (firewall)
Lasciare vuota questa voce, a meno che sia in esecuzione un servizio UDP e si desideri renderlo disponibile all'esterno. Tra i servizi che utilizzano UDP vi sono server DNS, IPSec, TFTP, DHCP e altri. In tal caso immettere le porte UDP da utilizzare.

FW_SERVICES_INT_TCP (firewall)
Definire tramite questa variabile i servizi disponibili per la rete interna La notazione è la stessa di FW_SERVICES_EXT_TCP, tuttavia le impostazioni vengono applicate alla rete *interna*. È necessario impostare questa variabile solo se FW_PROTECT_FROM_INT è impostata su yes.

FW_SERVICES_INT_UDP (firewall)
Vedere FW_SERVICES_INT_TCP.

Dopo aver completato la configurazione del firewall, eseguirne il test. Per creare set di regole del firewall immettere SuSEfirewall2 start come root. Utilizzare quindi telnet, ad esempio, da un host esterno per verificare che la connessione sia effettivamente rifiutata. Esaminare successivamente /var/log/messages il cui contenuto dovrebbe essere analogo a quanto segue:

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEBC0000000001030300)
```

Per il test della configurazione del firewall è consigliabile utilizzare anche il pacchetto nmap o nessus. La documentazione relativa a nmap è disponibile in /usr/share/doc/packages/nmap, mentre la documentazione di nessus si trova nella directory /usr/share/doc/packages/nessus-core dopo l'installazione del rispettivo pacchetto.

23.1.5 Ulteriori informazioni

Le informazioni più aggiornate e altra documentazione relativa al pacchetto SuSEfirewall2 sono disponibili in /usr/share/doc/packages/SuSEfirewall2. Tramite la home page del progetto netfilter e iptables, http://www.netfilter.org, è possibile consultare un'ampia raccolta di documenti in molte lingue.

23.2 SSH: lavorare in tutta sicurezza su host remoti

Lavorare in rete spesso comporta dover accedere ad host remoti. L'utente deve autenticarsi tramite il proprio nome di login e password. Se questi dati non vengono cifrati possono venir intercettati da terzi e utilizzati per eseguire il login all'insaputa dell'utente. A parte il fatto che in tal modo verrebbe violata la privacy dell'utente, l'intrusore può utilizzare l'accesso per sferrare degli attacchi contro altri sistemi oppure conferirsi i diritti dell'amministratore o dell'utente `root` del relativo sistema. In passato per collegare due host remoti si usava Telnet sprovvisto di qualsiasi meccanismo di cifratura o di sicurezza contro tentativi di intrusione; offrono poca sicurezza anche i semplici collegamenti FTP o alcuni programmi che permettono di copiare dei dati da un host all'altro.

Il software SSH offre la protezione necessaria. Le stringhe di autenticazione, di solito il nome utente e la password, ed anche il processo di comunicazione avvengono in forma cifrata; anche qui è possibile intercettare dei dati trasmessi ma senza la chiave di cifratura non è possibile decifrare il flusso di dati. Quindi si realizza una comunicazione sicura attraverso una rete insicura come Internet. SUSE Linux offre il pacchetto OpenSSH.

23.2.1 Il pacchetto OpenSSH

Con SUSE Linux viene installato di default il pacchetto OpenSSH. Avrete a vostra disposizione i programmi ssh, scp e sftp, come alternativa a telnet, rlogin, rsh, rcp e ftp. Nella configurazione di default, si potrà accedere ad un sistema SUSE Linux solo tramite utility OpenSSH e solo se il firewall consente l'accesso.

23.2.2 Il programma ssh

Con il programma ssh, potete stabilire un collegamento ad un sistema remoto e lavorarci interattivamente. Questo programma sostituisce quindi sia telnet che rlogin. Il programma slogin è solo un link simbolico che rimanda a ssh. Per fare un esempio: con il comando `ssh sun`, si può accedere al sistema sun che vi chiederà la vostra password.

Dopo l'autenticazione, potrete lavorare sia dalla riga di comando che interattivamente, p.es. con YaST. Se il nome utente locale e quello sul sistema remoto differiscono, potete indicare un nome differente p.es. `ssh -l augusto sun` o `ssh augusto@sun`.

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 sun e creata una directory con il nome `tmp`. L'output del programma viene visualizzato sul terminale locale del sistema earth.

```
ssh  altropianeta "uptime; mkdir tmp"
tux@password_di_altropianeta:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

Le virgolette servono qui per riunire le due istruzioni in un comando; solo così verrà eseguito anche il secondo comando sul sistema sun.

23.2.3 scp – copiare in modo sicuro

Per mezzo di scp potete copiare dei file su un host remoto. scp è il sostituto cifrato e sicuro di rcp. Per esempio, `scp miotesto.tex sun:` copia il file `miotesto.tex` dal sistema earth sul sistema sun. Se il nome utente su earth differisce da quello su sun, potete impostare quest'ultimo con `nomeutente@nomehost`. Non esiste un'opzione `-l` per questo comando.

Dopo aver immesso la password, scp inizia con la trasmissione dei dati e ne indica lo stato di avanzamento con una barra formata da asterischi che cresce da sinistra a destra. Inoltre, sul margine destro viene mostrato il tempo rimanente (stimato) per la trasmissione (ingl. estimated time of arrival). Ogni output può venire soppresso con l'opzione `-q`.

scp consente non solo di copiare singoli file ma offre anche una funzionalità di copiatura ricorsiva per poter copiare intere directory: `scp -r src/ sun:backup/` copia l'intero contenuto della directory `src/` sottodirectory incluse su sun e lì nella sottodirectory `backup/`. Se questa sottodirectory non dovesse ancora esistere, viene generata automaticamente.

Per mezzo dell'opzione `-p`, scp non modifica la datazione dei file. `-C` provvede ad una trasmissione compressa. In questo modo, viene ridotto al minimo il volume dei dati da trasmettere, anche se questo processo comporta un considerevole carico di lavoro per il processore.

23.2.4 sftp - trasmissione più sicura

Al posto di scp si può usare sftp. Una sessione sftp offre molti dei comandi noti di ftp. Rispetto a scp si rivela vantaggioso soprattutto quando si trasmettono dati di cui si ignorano i nomi dei file.

23.2.5 Il demone SSH (sshd): lato server

Affinché possano venire utilizzati i programmi client del pacchetto SSH, ossia ssh e scp, un server, in questo caso il demone di SSH, deve girare in sottofondo, e mettersi in ascolto su `TCP/IP port 22`. Durante il primo avvio, il demone genera tre paia di chiavi composte da una parte privata e da una pubblica. Per questo si usa definire questo approccio come procedimento basato su chiave pubblica. Per garantire una comunicazione sicura tramite SSH, solo l'amministratore deve poter accedere ai file delle chiavi private. A questo scopo, i permessi dei file vengono impostati (preimpostati) in modo molto restrittivo durante l'installazione di default. Le chiavi private sono richiese localmente solo dal demone SSH e non devono venir trasmesse a nessun altro. Le chiavi pubbliche (riconoscibili dall'estensione `.pub`), invece, vengono trasmesse al client che chiede di collegarsi e sono quindi leggibili per tutti gli utenti.

Il client SSH cerca di stabilire una connessione. Il demone SSH in attesa e il client SSH richiedente scambiamo i dati di identificazione per confrontare la versione di protocollo e di software ed escludere la connessione ad una porta errata. Dato che è un processo figlio del demone SSH a replicare, sono possibili una serie di connessioni SSH contemporanee.

OpenSSH supporta ai fini della comunicazione tra server SSH e client SSH il protocollo SSH nella versione 1 e 2. Se eseguite una nuova installazione di SUSE Linux verrà installato automaticamente la versione 2 del protocollo. Se dopo un aggiornamento volete continuare ad utilizzare SSH 1, seguite le istruzioni riportate in `/usr/share/doc/packages/openssh/README.SuSE`. Lì viene anche descritto come convertire in pochi passaggi un ambiente SSH 1 in un ambiente SSH 2.

Con il protocollo SSH versione 1, il server inivia la sua chiave host (ingl. host key) pubblica ed una chiave server (ingl. server key) che viene rigenerata dal demone di SSH ogni ora. Per mezzo delle due chiavi, il client SSH crea una chiave di sessione (ingl.session key) cifrata e la invia al server SSH. Il client ssh comunica inoltre al server quale metodo di cifratura utilizzare (ingl. cipher).

Il protocollo SSH versione 2 non prevede l'uso della chiave server, ricorre invece all'algoritmo secondo Diffie-Hellman per lo scambio delle chiavi.

Le chiavi host e server private, assolutamente necessarie per decifrare la chiave di sessione, non possono venire dedotte dalle chiavi pubbliche. In questo modo, solo il demone SSH contattato è in grado di decifrare la chiave di sessione grazie alla sua chiave privata (si veda `man /usr/share/doc/packages/openssh/RFC.nroff`). Questa fase iniziale del collegamento si lascia seguire da vicino ricorrendo all'opzione `-v` preposta alla ricerca di errori (debugging).

Di default viene utilizzato il protocollo SSH versione 2; con il parametro `-1` potete tuttavia forzare l'uso della versione 1 del protocollo SSH. Il client archivia tutte le chiavi host pubbliche in `~/.ssh/known_hosts` dopo la prima presa di contatto con l'host remoto. In tal modo è possibile respingere tentativi di attacchi del tipo man-in-the-middle con server SSH che utilizzano nomi ed indirizzi IP contraffatti. Questi tentativi verranno smascherati a causa di una chiave host non inclusa in `~/.ssh/known_hosts` oppure vista l'impossibilità del server di decifrare la chiave di sessione dal momento che manca la controparte privata.

É consigliabile archiviare su di un supporto esterno ed in un luogo sicuro le chiavi private e pubbliche di `/etc/ssh/`. In questo modo, accertate eventuali manipolazione delle chiavi, potrete ripristinare le vecchie chiavi reinstallandole. Così risparmiate agli utenti l'avvertimenti pochi rassicuranti. Una volta accertato che, nonostante l'avviso, si tratta del server SSH giusto, eliminate la registrazione relativa a questo sistema da `~/.ssh/known_hosts`.

23.2.6 Meccanismi di autenticazione SSH

Ora segue l'autenticazione vera e propria, che, nella variante più semplice prevede l'immissione di una password, così come negli esempi sopra citati. Con SSH si è voluto introdurre un software sicuro e al contempo facile da usare, con un metodo di autenticazione semplice come quello dei programmi che intende sostituire (rsh e rlogin). Con SSH vi è un ulteriore paio di chiavi generato dall'utente. A questo scopo il pacchetto SSH contiene il tool ssh-keygen. Immettendo `ssh-keygen -t rsa` o `ssh-keygen -t dsa` viene generato il paio di chiavi e vi verrà chiesto il nome del file nel quale archiviare le chiavi:

Confermate il valore di default e indicate la passphrase. Anche se il software vi consiglia di non indicare una passphrase, consigliamo di inserire comunque una stringa lunga da 10 a 30 caratteri. Non utilizzate parole o frasi semplici o brevi. Il programma vi chiederà di inserire la frase una seconda volta. Infine, vi mostrerà dove le chiavi pubbliche e private siano state archiviate, ovvero, nel nostro esempio, nei file `id_rsa` e `id_rsa.pub`.

Usate `ssh-keygen -p -t rsa` o rispettivamente `ssh-keygen -p -t dsa` per modificare la vostra passphrase. Copiate la parte pubblica della chiave (nel nostro esempio `id_rsa.pub`) sul sistema remoto, dove la salvate sotto `~/.ssh/authorized_keys`. Ogni volta che vi connetterete, vi verrà chiesta la passphrase. In caso contrario, verificate la locazione ed il contenuto dei file summenzionati.

A lungo andare, questo procedimento è più laborioso dell'inserimento di una password. Quindi, il pacchetto SSH fornisce un altro tool: ssh-agent che tiene pronte le chiavi private per la durata di una X session; a questo scopo, l'intera X session viene avviata come processo figlio di ssh-agent. Potete realizzare ciò semplicemente impostando la variabile `usessh` all'inizio del file `.xsession` su `yes`, ed eseguire il login tramite un display manager (p.es.KDM o XDM). Alternativamente potete usare `ssh-agent startx`.

Ora potete utilizzare ssh o scp. Se avete distribuito la vostra chiave pubblica come descritto sopra, non dovreste più ricevere la richiesta d'inserimento della password. Quando uscite dal vostro sistema, fate attenzione a terminare la vostra X session o a non permettere a nessuno di accedervi ad es. impostando una applicazione per bloccare lo schermo protetta da una password, p.es. xlock.

Tutte le principali modifiche con l'introduzione della seconda versione del protocollo SSH, sono riportate nel file `/usr/share/doc/packages/openssh/README.SuSE`.

23.2.7 X: inoltro e autenticazione

Oltre ai miglioramenti in termini di sicurezza finora descritti, ssh facilita anche l'uso di applicazioni X remote. Se inserite `ssh` con l'opzione `-X`, sul sistema remoto viene automaticamente impostata la variabile DISPLAY e tutte le emissioni di X vengono reindirizzate, tramite il collegamento ssh, sul sistema di partenza. Questa comoda funzione previene contemporaneamente la possibilità d'intercettazione esistente finora

nelle applicazioni X lanciate su un sistema remoto e con visualizzazione sul sistema locale.

Tramite l'opzione `-A`, viene il meccanismo di autenticazione di ssh-agent viene passato al prossimo sistema. In tal modo è possibile passare da un sistema all'altro senza dover inserire una password; questo però solo se prima sono state distribuite e archiviate correttamente le chiavi pubbliche sui sistema meta interessati.

Per precauzione, entrambi i meccanismi non sono attivi di default. Per attivarli permanentemente, andate nel file di configurazione del sistema, `/etc/ssh/ssh_config` o in quello dell'utente `~/.ssh/config`.

Potete utilizzare ssh anche per reindirizzare un collegamento TCP/IP. Come esempio riportiamo l'inoltro della porta SMTP e POP3:

```
ssh -L 25:sun:25 earth
```

Con questo comando ogni collegamento indirizzato a *earth port 25* (SMTP) viene reindirizzato alla porta SMTP di sun tramite un canale cifrato. Ciò è utile specialmente per gli utenti di server SMTP senza supporto per le funzionalità SMTP-AUTH o POP-before-SMTP. Le e-mail possono in tal maniera venir inviate da una postazione qualsiasi con un collegamento di rete per essere consegnate al proprio server di posta (ingl.«home» mail server). In modo analogo con il seguente comando le richieste POP3 (porta 110) di earth possono essere inoltrate alla porta POP3 di sun.

```
ssh -L 110:sun:110 earth
```

Questi comandi vanno eseguiti come utente `root`, poiché vengono indirizzate porte locali privilegiate. Con un collegamento SSH esistente, la posta viene spedita e ritirata da utente normale. L'host SMTP e l'host POP3 deve venire configurato su `localhost`. Per ulteriori informazioni consultate le pagine di manuale dei singoli programmi e dei file sotto `/usr/share/doc/packages/openssh`.

23.3 Cifratura di partizioni e file

Tutti gli utenti creano o utilizzano dati riservati a cui gli altri utenti non devono avere accesso. La gestione dell'accesso ai dati richiede particolare attenzione nel caso di utenti mobili e connessi. La cifratura di file o intere partizioni è consigliata negli scenari in cui altri utenti hanno accesso fisico diretto oppure tramite una connessione di rete ai file.

AVVERTIMENTO: i supporti cifrati offrono una protezione limitata

Si tenga presente che i metodi descritti in questa sezione non consentono di evitare che il sistema in esecuzione venga compromesso. Dopo che i supporti cifrati sono stati montati, tutti gli utenti che dispongono di autorizzazioni adeguate possono accedervi. I supporti cifrati risultano utili nel caso in cui il computer venga perso o sottratto e individui non autorizzati desiderino leggere dati riservati.

Di seguito vengono elencati alcuni possibili scenari di applicazione.

Computer portatili
Se si utilizza un computer portatile durante i propri viaggi, è consigliabile cifrare le partizioni del disco rigido contenenti dati riservati. In caso di perdita o furto del computer portatile, i dati presenti nel file system cifrato o in un singolo file cifrato non saranno accessibili.

Supporti rimovibili
Le unità flash USB e i dischi rigidi esterni presentano gli stessi rischi di sottrazione dei computer portatili. Un file system cifrato garantisce una protezione contro l'accesso da parte di terzi.

Workstation
Nelle società in cui quasi tutti gli utenti hanno accesso a un computer può essere utile cifrare partizioni o singoli file.

23.3.1 Impostazione di un file system cifrato con YaST

YaST consente di cifrare file o partizioni sia durante l'installazione che in un sistema già installato. Un file cifrato può essere creato in qualsiasi momento perché si adatta perfettamente al layout delle partizioni esistenti. Per cifrare un'intera partizione, riservare una partizione alla cifratura nel layout delle partizioni. Il partizionamento standard proposto da YaST non include per default una partizione cifrata ed è necessario aggiungerla manualmente nella finestra di dialogo per il partizionamento.

Creazione di una partizione cifrata durante l'installazione

AVVERTIMENTO: input della password

Leggere i messaggi di avviso riguardanti la protezione durante l'impostazione della password per partizioni cifrate e memorizzare tale parola. Senza la password non è possibile accedere ai dati cifrati né ripristinarli.

Nella finestra di dialogo avanzata di YaST per il partizionamento, descritta nella Sezione «Partizionamento» (Capitolo 3, *Configurazione di sistema con YaST*, ↑Avvio), sono disponibili le opzioni necessarie per creare una partizione cifrata. Fare clic su *Crea* come quando si crea una normale partizione. Nella finestra di dialogo visualizzata immettere i parametri del partizionamento per la nuova partizione, ad esempio la formattazione desiderata e il punto di montaggio. Fare clic su *File system cifrato* per completare la procedura. Nella finestra di dialogo successiva immettere la password due volte. La nuova partizione cifrata viene creata quando si fa clic su *OK* per chiudere la finestra di dialogo per il partizionamento. Il sistema operativo richiede la password in fase di avvio, prima del montaggio della partizione.

Se non si desidera montare la partizione cifrata durante la fase di avvio, premere Invio quando viene richiesta la password, quindi scegliere di non immettere la password una seconda volta. In questo caso, il file system cifrato non viene montato e il sistema operativo continua la procedura di avvio bloccando l'accesso ai dati. La partizione risulta disponibile a tutti gli utenti dopo che è stata montata.

Se si desidera montare il file system cifrato solo in caso di necessità, abilitare *Non montare durante l'avvio* nella finestra di dialogo *Opzioni*. La partizione corrispondente non verrà montata durante l'avvio del sistema. Per renderla disponibile successivamente, è necessario montarla manualmente tramite il comando `mount` *`nome_partizione punto_montaggio`*. Immettere la password quando richiesto. Dopo avere utilizzato la partizione, smontarla tramite il comando `umount nome_partizione` per impedire l'accesso da parte di altri utenti.

Creazione di una partizione cifrata in un sistema in esecuzione

AVVERTIMENTO: attivazione della cifratura in un sistema in esecuzione

È inoltre possibile creare partizioni cifrate in un sistema in esecuzione seguendo una procedura simile a quella utilizzata durante l'installazione. La cifratura di una partizione esistente, tuttavia, comporta la distruzione di tutti i dati esistenti.

In un sistema in esecuzione selezionare *Sistema → Partizionamento* nel centro controllo YaST. Fare clic su *Sì* per continuare. Anziché selezionare *Crea* come specificato sopra, fare clic su *Modifica*. La restante parte della procedura è identica.

Installazione di file cifrati

Anziché utilizzare una partizione, è possibile creare file system cifrati all'interno di singoli file per la memorizzazione di dati riservati. Questi file system vengono creati nella stessa finestra di dialogo di YaST. Selezionare *File cifrato* e immettere il percorso del file da creare nonché la dimensione prevista. Accettare le impostazioni di formattazione proposte e il tipo di file system. Specificare quindi il punto di montaggio e scegliere se il file system cifrato deve essere montato durante l'avvio del sistema.

I file cifrati offrono il vantaggio di poter essere aggiunti senza ripartizionare il disco rigido. Vengono montati con l'ausilio di un dispositivo con loop e hanno un comportamento analogo a quello delle normali partizioni.

Uso di vi per la cifratura di file

Lo svantaggio derivante dall'uso di partizioni cifrate è che durante il montaggio della partizione i dati sono accessibili almeno dall'utente `root`. Per evitare questo inconveniente, è possibile utilizzare vi in modalità cifrata.

Utilizzare `vi -x` *`nomefile`* per modificare un nuovo file. Verrà chiesto di impostare una password, dopo di che il contenuto del file verrà cifrato. Ogni volta che si accederà a questo file, verrà richiesta la password.

Per aumentare ulteriormente il livello di protezione, è possibile inserire il file di testo cifrato in una partizione cifrata. Poiché la cifratura applicata in vi non è di livello avanzato, è consigliabile adottare questo ulteriore accorgimento.

23.3.2 Cifratura del contenuto di supporti rimovibili

YaST gestisce i supporti rimovibili come dischi rigidi esterni e le unità flash USB come qualsiasi altro disco rigido. I file o le partizioni su tali supporti possono essere cifrati come descritto sopra. Evitare, tuttavia, di montare questi supporti durante l'avvio del sistema perché in genere sono connessi solo mentre il sistema è in esecuzione.

23.4 Sicurezza e riservatezza

Una delle caratteristiche principali di un sistema Linux o UNIX è la capacità di gestire più utenti contemporaneamente (multi-utente) e di consentire agli utenti di eseguire più attività (multitasking) nello stesso computer allo stesso tempo. Il sistema operativo supporta inoltre l'accesso alla rete invisibile all'utente, in modo tale che spesso gli utenti non percepiscono la differenza tra i dati e le applicazioni forniti dal computer in uso o quelli resi disponibili attraverso la rete.

La funzionalità multi-utente richiede la memorizzazione separata dei dati di utenti diversi, pertanto aspetti come la sicurezza e la privacy dei dati devono essere necessariamente garantiti. La sicurezza dei dati ha rappresentato un problema importante ancora prima che i computer venissero connessi attraverso reti informatiche. Allora come oggi l'elemento più importante era la capacità di assicurare la disponibilità dei dati anche in caso di perdita o danno di un supporto fisico, quasi sempre un disco rigido.

In questa sezione vengono descritti soprattutto i problemi di riservatezza e i metodi che è possibile implementare per proteggere la privacy degli utenti. È tuttavia importante sottolineare che un concetto di sicurezza completo dovrà sempre includere procedure che prevedano la disponibilità di un backup aggiornato regolarmente, fruibile e testato. Senza queste premesse, potrebbe risultare estremamente difficile recuperare i dati non solo nel caso di hardware difettoso, ma anche qualora insorga il sospetto che utenti non autorizzati abbiano potuto accedere ai file e manometterli.

23.4.1 Sicurezza locale e di rete

È possibile accedere ai dati in vari modi:

- Mediante la comunicazione personale con utenti che dispongono delle informazioni desiderate o mediante l'accesso ai dati in un computer.
- Direttamente dalla console di un computer (accesso fisico).
- Attraverso una linea seriale.
- Utilizzando un collegamento di rete.

In tutti i casi l'utente dovrà essere autenticato prima di poter accedere alle risorse o ai dati in questione. Un server Web può essere più o meno restrittivo, ma è presumibile che non si desideri rivelare i propri dati personali a chiunque.

Nel primo caso è richiesta una maggiore interazione dell'utente, analogamente a quanto avviene in una transazione bancaria nella quale è necessario provare la propria identità come titolare di un determinato conto bancario, dopodiché viene chiesto di fornire una firma, un PIN o una password per confermare tale identità. In alcuni casi è possibile che le informazioni a conoscenza di una persona vengano carpite semplicemente citando qualche dettaglio noto, in modo da ottenere la fiducia di quella persona con subdole capacità oratorie. La vittima potrebbe essere portata a rivelare maggiori informazioni gradualmente, anche senza rendersene conto. Tra i pirati informatici, la tecnica che sfrutta espedienti psicologici, ad esempio per indurre le vittime a effettuare determinate operazioni, è detta *social engineering*. L'unico modo per contrastare questo tipo di attacco è di mettere in guardia le persone e gestire con consapevolezza il linguaggio e le informazioni. Prima di introdursi nei sistemi informatici, chi effettua l'attacco tenta spesso un approccio con gli addetti alla ricezione, con il personale di servizio o addirittura con i familiari dei dipendenti di una società. In molti casi questo tipo di attacchi che sfruttano la tecnica del social engineering vengono scoperti solo dopo molto tempo.

Coloro che cercano di accedere ai dati senza essere autorizzati utilizzano spesso le tecniche tradizionali di accesso diretto all'hardware. È quindi necessario proteggere il computer da manomissioni, in modo da impedire che i componenti vengano rimossi, sostituiti o danneggiati. Questo concetto si applica anche ai backup, nonché al cavo di rete o di alimentazione. È necessario proteggere anche la procedura di avvio, poiché

esistono combinazioni di tasti note che possono causare un comportamento anomalo. Per proteggersi da tale evenienza, impostare password per il BIOS e per il boot loader.

I terminali seriali connessi alle porte seriali sono ancora diffusi in molti ambienti. A differenza delle interfacce di rete, non utilizzano un protocollo di rete per la comunicazione con l'host, bensì un semplice cavo o una porta a infrarossi per lo scambio di semplici caratteri tra dispositivi. In un sistema di questo tipo il cavo stesso costituisce il punto più debole. Con una vecchia stampante connessa al cavo è estremamente semplice registrare qualsiasi informazione trasmessa sul filo. Ciò che è possibile ottenere con una stampante può essere realizzato anche in altri modi, a seconda dell'impegno prodigato nell'attacco.

La lettura locale di un file in un host richiede altre regole di accesso rispetto all'apertura di una connessione di rete mediante un server in un host diverso. Tra il concetto di sicurezza locale e quello di sicurezza di rete esiste una distinzione, infatti per inviare dati altrove è necessario includerli in pacchetti.

Sicurezza locale

La sicurezza locale inizia dall'ambiente fisico nel quale il computer è in esecuzione. Installare il computer in un ambiente nel quale la sicurezza è in linea con le proprie aspettative ed esigenze. L'obiettivo principale della sicurezza locale è di mantenere separati gli utenti, in modo che nessuno possa assumere le autorizzazioni o l'identità di altri. Questa regola generale è valida in particolare per l'utente `root`, il quale ha il controllo totale del sistema. L'utente `root` può assumere l'identità di qualsiasi altro utente locale senza fornire la password e leggere tutti i file memorizzati localmente.

Password

In un sistema Linux le password non vengono memorizzate come testo normale e la stringa di testo immessa non viene semplicemente confrontata con il modello salvato poiché in tal caso tutti gli account nel sistema verrebbero compromessi se qualcuno riuscisse ad accedere al file corrispondente. La password memorizzata viene al contrario cifrata e cifrata nuovamente a ogni immissione, quindi vengono confrontate le due stringhe cifrate. Questo meccanismo offre maggiore sicurezza solo se la password cifrata non può essere decodificata nella stringa di testo originale.

Questo si ottiene mediante uno speciale tipo di algoritmo, detto anche *algoritmo trapdoor*, che funziona solo in una direzione. Anche se chi effettua l'attacco è riuscito

a ottenere la stringa cifrata, non sarà in grado di rilevare la password semplicemente applicando lo stesso algoritmo una seconda volta. Dovrà invece provare tutte le possibili combinazioni di caratteri finché non troverà una combinazione corrispondente alla password cifrata. Per le password di otto caratteri le combinazioni possibili da calcolare sono numerose.

Negli anni '70 si riteneva che questo metodo sarebbe stato più sicuro rispetto ad altri, a causa della relativa lentezza dell'algoritmo utilizzato che impiegava alcuni secondi per cifrare una sola password. Nel frattempo i PC sono diventati abbastanza potenti da eseguire alcune centinaia di migliaia o addirittura milioni di cifrature al secondo. Per questo motivo le password cifrate non dovrebbero essere visibili ai normali utenti, ovvero `/etc/shadow` non può essere letto dai normali utenti. È ancora più importante ricorrere all'uso di password che non siano facili da individuare qualora il file delle password diventi visibile agli utenti a causa di un errore. Non è quindi molto utile «convertire» una password come «tantalize» in «t@nt@1lz3».

La sostituzione di alcune lettere di una parola in numeri dall'aspetto simile non è un metodo sufficientemente sicuro. Anche i programmi di individuazione delle password che utilizzano dizionari per identificare le parole ricorrono a questo tipo di sostituzioni. Il metodo migliore consiste nel creare una parola priva di significato che abbia senso solo per l'utente, ad esempio le prime lettere di una frase o del titolo di un libro quale «Il nome della rosa» di Umberto Eco, che consente di ottenere la password sicura «INodRdUE9». Al contrario, password come «compagnidiviaggio» o «michela76» sono facilmente individuabili da chi abbia anche solo una conoscenza superficiale dell'utente.

Procedura di avvio

Configurare il sistema in modo che non possa essere avviato da un disco floppy o da un CD. A questo scopo, rimuovere completamente le unità o impostare una password per il BIOS e configurarne l'avvio solo da un disco rigido. Un sistema Linux viene in genere avviato da un boot loader in modo da consentire il passaggio di opzioni aggiuntive al kernel avviato. Per impedire ad altri di utilizzare questi parametri durante l'avvio, impostare una password aggiuntiva in `/boot/grub/menu.lst` (vedere il Capitolo 29, *Boot Loader* (p. 463)). Questa impostazione è fondamentale per la sicurezza del sistema. Non solo lo stesso kernel viene eseguito con autorizzazioni `root`, ma è anche la prima autorità che concede autorizzazioni `root` all'avvio del sistema.

Autorizzazioni dei file

Come regola generale, utilizzare sempre privilegi più restrittivi possibile per una determinata attività. Non è assolutamente necessario, ad esempio, disporre di autorizzazioni `root` per leggere o scrivere messaggi e-mail. Se nel programma di posta elettronica è presente un bug, questo potrebbe essere sfruttato per un attacco utilizzando esattamente le stesse autorizzazioni del programma al momento dell'avvio. L'applicazione della regola sopra descritta consente di limitare al minimo il possibile danno.

Le autorizzazioni per gli oltre 200.000 file inclusi in una distribuzione SUSE vengono scelte con attenzione. In caso di installazione di software o altri file aggiuntivi, l'amministratore di sistema dovrà procedere con la massima precauzione, specialmente per l'impostazione dei bit delle autorizzazioni. Gli amministratori esperti e attenti alla sicurezza utilizzano sempre l'opzione `-l` con il comando `ls` per ottenere un elenco di file esteso, in modo da rilevare immediatamente eventuali autorizzazioni di file non corrette. Un attributo di file non corretto non significa solo che i file potrebbero essere stati danneggiati o eliminati, ma anche che questi file modificati potrebbero essere eseguiti da `root` o, nel caso dei file di configurazione, essere utilizzati da programmi con autorizzazioni `root` con un aumento significativo delle possibilità di attacco. Attacchi di questo genere sono detti cuckoo egg (uova di cuculo), poiché il programma (l'uovo) viene eseguito (covato) da un altro utente (uccello), proprio come il cuculo induce altri uccelli a covare le sue uova.

In un sistema SUSE Linux sono disponibili i file `permissions`, `permissions.easy`, `permissions.secure` e `permissions.paranoid` nella directory `/etc`. Lo scopo di questi file è la definizione di autorizzazioni speciali, ad esempio directory di tipo world-writable oppure, per i file, il bit setuser ID. I programmi con impostato il bit setuser ID non vengono eseguiti con le autorizzazioni dell'utente che li ha avviati, bensì con le autorizzazioni del proprietario del file, nella maggior parte dei casi `root`. Per aggiungere impostazioni personali, l'amministratore può utilizzare il file `/etc/permissions.local`.

Per definire quale dei file sopra indicati viene utilizzato dai programmi di configurazione di SUSE per impostare le autorizzazioni di conseguenza, selezionare *Sicurezza* in YaST. Per ulteriori informazioni sull'argomento, leggere i commenti nel file `/etc/permissions` o consultare la documentazione di `chmod` (`man chmod`).

Overflow del buffer e bug delle stringhe di formato

Quando si prevede che un programma elabori dati che possono o potrebbero essere danneggiati da un utente, è necessario prestare particolare attenzione anche se questo problema riguarda più il programmatore di un'applicazione che i normali utenti. Il programmatore dovrà assicurarsi che l'applicazione interpreti i dati nel modo corretto, evitando che vengano scritti in aree di memoria troppo piccole per contenerli. I dati dovranno inoltre essere trasmessi in maniera coerente, utilizzando le interfacce definite a tale scopo.

Un *overflow del buffer* può verificarsi se la dimensione effettiva di un buffer di memoria non viene considerata durante la scrittura nel buffer. In alcuni casi i dati generati dall'utente utilizzano più spazio di quanto sia disponibile nel buffer e di conseguenza vengono scritti oltre la fine di tale area del buffer. In alcuni casi ciò consente l'esecuzione di sequenze del programma determinate dall'utente (non dal programmatore), anziché la semplice elaborazione dei dati. Un bug di questo genere può avere conseguenze molto serie, specialmente se il programma in questione viene eseguito con privilegi speciali (vedere la sezione chiamata «Autorizzazioni dei file» (p. 362)).

Il funzionamento dei *bug delle stringhe di formato* è leggermente diverso ma, anche in questo caso, l'input dell'utente può influire sul programma. Nella maggior parte dei casi questi errori di programmazione vengono sfruttati mediante programmi eseguiti con autorizzazioni speciali, ad esempio programmi setuid e setgid. Ciò significa che i dati e il sistema possono essere protetti da tali bug eliminando i corrispondenti privilegi di esecuzione dai programmi. Anche in questo caso la procedura migliore consiste nell'applicare un criterio che preveda l'uso del livello di privilegi più basso possibile (vedere la sezione chiamata «Autorizzazioni dei file» (p. 362)).

Considerato che gli overflow del buffer e i bug delle stringe di formato sono correlati alla gestione dei dati utente, essi possono essere sfruttati non solo se è stato consentito l'accesso a un account locale. Molti dei bug segnalati possono infatti essere sfruttati anche tramite un collegamento di rete. Per questo motivo gli overflow del buffer e i bug delle stringhe di formato dovrebbero essere classificati tra i bug che interessano sia la sicurezza locale sia della rete.

Virus

Contrariamente a quanto sostenuti da alcuni, esistono virus eseguibili in ambiente Linux. I virus noti sono comunque stati rilasciati dagli autori come *prova concettuale* del

funzionamento della tecnica secondo le intenzioni. Di nessuno di questi virus è stata riscontrata finora una *diffusione incontrollata*.

I virus non possono sopravvivere e diffondersi senza un host in cui risiedere. In questo caso, l'host potrebbe essere un programma o un'importante area di memorizzazione del sistema, ad esempio il Master Boot Record (MBR), che dovrà essere accessibile in scrittura al codice di programma del virus. In conseguenza della capacità multi-utente di Linux, il sistema è in grado di limitare l'accesso in scrittura a determinati file, specialmente i file di sistema importanti. Per questo motivo, se si svolge la normale attività con autorizzazioni `root`, si aumenta il rischio che il sistema venga infettato da un virus. Se invece si segue il principio di utilizzare il più basso livello possibile di privilegi, come indicato in precedenza, le possibilità di introduzione di virus nel sistema sono estremamente limitate.

Ciò premesso, è opportuno evitare di farsi indurre a eseguire programmi da siti Internet di cui non si ha una conoscenza effettiva. I pacchetti RPM di SUSE sono dotati di una firma di cifratura sotto forma di etichetta digitale per indicare che sono stati creati con attenzione. I virus sono una tipica indicazione che l'amministratore o l'utente non è consapevole dei reali requisiti di sicurezza necessari per evitare di mettere a rischio persino un sistema che, per sua sua stessa natura di progettazione, dovrebbe essere estremamente sicuro.

Evitare di confondere i virus con i worm, che fanno parte del mondo delle reti e non richiedono un host per diffondersi.

Sicurezza di rete

La sicurezza della rete è importante per proteggere il sistema da attacchi avviati dall'esterno. La tipica procedura di login, che prevede l'uso di un nome utente e di una password per l'autenticazione dell'utente, continua a essere un problema di sicurezza locale. Nel caso particolare del login in rete, è necessario distinguere i due aspetti della sicurezza. Tutto ciò che accade fino all'effettiva autenticazione riguarda la sicurezza di rete, mentre tutto ciò che accade successivamente riguarda la sicurezza locale.

X Window System e autenticazione X

Come accennato all'inizio, la trasparenza della rete costituisce una delle caratteristiche principali di un sistema UNIX. X è il sistema a finestre dei sistemi operativi UNIX in grado di utilizzare questa funzionalità in maniera ottimale. Con X non è un problema

accedere a un host remoto e avviare un programma grafico, che viene quindi inviato attraverso la rete per essere visualizzato nel computer in uso.

Quando è necessario visualizzare un client X remoto su un server X, quest'ultimo dovrà proteggere la risorsa gestita (il display) dall'accesso non autorizzato. In termini più concreti, al programma client dovranno essere concesse determinate autorizzazioni. In X Window System è possibile eseguire questa operazione in due modi, ovvero mediante il controllo dell'accesso basato sull'host e il controllo dell'accesso basato su cookie. Il primo si basa sull'indirizzo IP dell'host nel quale dovrà essere eseguito il client. A questo scopo è disponibile il programma xhost, che immette l'indirizzo IP di un client valido in un piccolo database appartenente al server X. L'uso di indirizzi IP per l'autenticazione non è tuttavia un metodo sicuro. Se, ad esempio, un secondo utente dell'host invia il programma client, anche questo utente potrà accedere al server X, come chiunque si impossessi dell'indirizzo IP. A causa di questi inconvenienti, questa procedura di autenticazione non viene descritta più dettagliatamente in questa sezione. Per ulteriori informazioni è tuttavia possibile utilizzare il comando `man xhost`.

Nel caso di controllo dell'accesso basato su cookie viene generata una stringa di caratteri, nota solo al server X e all'utente legittimo, che funge da scheda di identificazione. Il cookie (il termine inglese, che significa biscotto, non si riferisce in questo caso ai biscotti comuni, bensì ai biscotti cinesi che contengono una massima) viene memorizzato al login nel file `.Xauthority` nella home directory dell'utente ed è disponibile a tutti i client X che richiedono l'uso del server X per visualizzare una finestra. Il file `.Xauthority` può essere esaminato dall'utente mediante lo strumento xauth. Se il file `.Xauthority` viene rinominato o eliminato accidentalmente dalla home directory, non sarà possibile aprire nuove finestre o client X. Per ulteriori informazioni sui meccanismi di sicurezza di X Window System, vedere la documentazione di Xsecurity (`man Xsecurity`).

È possibile utilizzare SSH (Secure Shell) per cifrare completamente una connessione di rete e inoltrarla a un server X in maniera trasparente, senza che il meccanismo di cifratura venga percepito dall'utente. Questo metodo, definito inoltro X, si ottiene mediante la simulazione di un server X sul lato server e l'impostazione di una variabile DISPLAY per la shell nell'host remoto. Per ulteriori informazioni su SSH, vedere la Sezione 23.2, «SSH: lavorare in tutta sicurezza su host remoti» (p. 349).

AVVERTIMENTO

Se l'host nel quale si esegue il login non è considerato sicuro, non utilizzare il metodo di inoltro X. Quando è abilitato l'inoltro X, un utente malintenzionato

potrebbe effettuare l'autenticazione attraverso la connessione SSH e introdursi nel server X, ad esempio, per rilevare l'input dalla tastiera.

Overflow del buffer e bug delle stringhe di formato

Come descritto nella sezione chiamata «Overflow del buffer e bug delle stringhe di formato» (p. 363), gli overflow del buffer e i bug delle stringhe di formato dovrebbero essere classificati come problemi che interessano sia la sicurezza locale che la sicurezza della rete. Come avviene con le varianti locali di tali bug, gli overflow del buffer nei programmi di rete, se sfruttati per un attacco, vengono principalmente utilizzati per ottenere le autorizzazioni `root`. Sebbene non sia questo il caso, il bug potrebbe consentire l'accesso a un account locale senza privilegi per sfruttare eventuali altre vulnerabilità esistenti nel sistema.

Lo sfruttamento degli overflow del buffer e dei bug delle stringhe di formato attraverso un collegamento di rete è certamente la forma più frequente di attacchi remoti in generale. I programmi che consentono di sfruttare queste nuove falle nel sistema di sicurezza vengono spesso pubblicati nelle mailing list sulla sicurezza e possono essere utilizzati per attaccare la vulnerabilità del sistema senza conoscere i dettagli del codice. Nel corso degli anni l'esperienza ha dimostrato che la disponibilità dei codici di tali programmi ha contribuito a rendere più sicuri i sistemi operativi perché i produttori sono stati costretti a correggere i problemi presenti nel software. Con il software libero chiunque può accedere al codice sorgente (SUSE Linux viene fornito con tutti i codici sorgente disponibili) e chiunque individui una vulnerabilità e il codice per sfruttarla può inviare una patch per correggere il bug corrispondente.

Denial of Service (DoS)

Lo scopo di un attacco Denial Of Service (DoS) consiste nel bloccare un programma server o un intero sistema utilizzando vari mezzi, ad esempio sovraccaricando il server, tenendolo occupato con pacchetti inutili oppure sfruttando l'overflow di un buffer remoto. Un attacco DoS ha spesso il solo obiettivo di far scomparire un servizio tuttavia, quando un dato servizio non è più disponibile, le comunicazioni possono diventare vulnerabili ad *attacchi di tipo man-in-the-middle* (sniffing, hijacking della connessione TCP, spoofing) e DNS poisoning.

Man-in-the-middle: sniffing, hijacking, spoofing

In generale, qualsiasi attacco remoto da parte di un utente che si inserisce nelle comunicazioni tra gli host è detto *attacco di tipo man-in-the-middle*. L'elemento comune di questi tipi di attacchi è che in genere la vittima non è consapevole di ciò che sta accadendo. Le varianti possibili sono molte, ad esempio il pirata informatico potrebbe rilevare una richiesta di connessione e inoltrarla al computer di destinazione. In questo caso la vittima avrà inconsapevolmente stabilito una connessione con l'host non corretto, in quanto l'altra estremità della connessione si presenta come un computer di destinazione valido.

La forma più semplice di attacco man-in-the-middle è detta *sniffer*, ovvero il pirata informatico rimane «semplicemente» in ascolto del traffico di rete in transito. Una forma più complessa di attacco «man-in-the-middle» può essere il tentativo di assumere il controllo di una connessione già stabilita (hijacking). Per fare ciò, il pirata informatico deve analizzare i pacchetti per un certo intervallo di tempo per poter determinare i numeri della sequenza TCP appartenenti alla connessione. Quando il pirata informatico è finalmente in grado di assumere il ruolo di host di destinazione, la vittima viene informata mediante un messaggio di errore nel quale è indicato che la connessione è stata terminata a causa di un errore. Alcuni protocolli, tuttavia, non sono protetti da hijacking mediante la cifratura, ma eseguono solo una semplice procedura di autenticazione al momento in cui viene stabilita la connessione rendendo più facili gli attacchi.

Lo *spoofing* è un tipo di attacco in cui i pacchetti vengono modificati mediante l'immissione di dati di origine contraffatti, in genere l'indirizzo IP. Le forme di attacco più attive si basano sull'invio di tali pacchetti contraffatti, un'operazione che in un computer Linux può essere eseguita solo dal superutente (`root`).

Molti degli attacchi descritti vengono portati a termine in combinazione con DoS. Se un pirata informatico rileva l'opportunità di rendere improvvisamente inattivo un determinato host, anche solo per un breve intervallo, potrà portare avanti più facilmente l'attacco attivo, in quando l'host non sarà in grado di interferire per un dato periodo.

DNS poisoning

DNS poisoning è una tecnica che consente di danneggiare la cache di un server DNS mediante l'invio di pacchetti di risposta DNS contraffatti per fare in modo che il server invii dati particolari a una vittima che richiede informazioni da quel server. Molti server

mantengono una relazione di fiducia con altri host basate su indirizzi IP e nomi host. Per assumere l'identità di uno degli host sicuri, il pirata informatico deve avere una buona conoscenza della struttura effettiva delle relazioni di fiducia. Di solito analizza alcuni pacchetti ricevuti dal server per ottenere le informazioni necessarie e spesso deve prevedere contemporaneamente un attacco DoS con la giusta temporizzazione al server dei nomi. Per proteggersi da questo tipo di attacchi, utilizzare connessioni cifrate in grado di verificare l'identità degli host ai quali si stabilisce la connessione.

Worm

I worm vengono spesso confusi con i virus, benché vi sia una chiara differenza. Diversamente dai virus, l'esistenza dei worm non è legata all'infezione di un programma host. Sono invece specializzati nel diffondersi il più velocemente possibile attraverso le strutture di rete. I worm che si sono diffusi in passato, ad esempio Ramen, Lion o Adore, sfruttano le falle conosciute nel sistema di sicurezza dei programmi server come bind8 o lprNG. La protezione dai worm è relativamente semplice. Poiché tra la scoperta di una falla nel sistema di sicurezza e il momento in cui il worm penetra nel server trascorre un pò di tempo, è molto probabile che sia già disponibile una versione aggiornata del programma interessato. Questo aspetto è utile solo se l'amministratore installa effettivamente gli aggiornamenti di sicurezza nei sistemi in questione.

23.4.2 Alcuni suggerimenti generali sulla sicurezza

Per gestire la sicurezza in maniera competente, è importante tenersi aggiornati sui nuovi sviluppi e informati sui più recenti problemi di sicurezza. Un ottimo metodo per proteggere i sistemi da qualsiasi tipo di problema consiste nell'ottenere e installare al più presto possibile i pacchetti aggiornati suggeriti dagli annunci relativi alla sicurezza. Gli annunci relativi alla sicurezza di SUSE vengono pubblicati in una mailing list che è possibile sottoscrivere all'indirizzo `http://www.novell.com/linux/security/securitysupport.html` (in lingua inglese). La mailing list `suse-security-announce@suse.de` costituisce una pratica fonte di informazioni sui pacchetti aggiornati e, tra i collaboratori attivi, include i membri del team di sicurezza di SUSE.

La mailing list suse-security@suse.de è un'ottima area di discussione per qualsiasi argomento riguardante problemi di sicurezza specifici. È possibile sottoscrivere la mailing list nella stessa pagina Web.

bugtraq@securityfocus.com è una delle mailing list sulla sicurezza più conosciute al mondo, nella quale vengono inseriti tra 15 e 20 messaggi ogni giorno, di cui si consiglia la lettura. Ulteriori informazioni sono disponibili all'indirizzo http://www.securityfocus.com (in lingua inglese).

Di seguito è riportato un elenco di regole utili per la gestione delle problematiche di base relative alla sicurezza:

- In base alla regola di utilizzare il set di autorizzazioni più restrittivo possibile per ogni lavoro, evitare di svolgere la normale attività come `root`. In questo modo si riduce la vulnerabilità agli attacchi di tipo cuckoo egg o ai virus, proteggendosi inoltre dai propri errori.

- Utilizzare sempre, se possibile, connessioni cifrate quando si accede a un computer remoto. L'uso di `ssh` (Secure Shell) in sostituzione di `telnet`, `ftp`, `rsh`e `rlogin` dovrebbe costituire una regola abituale.

- Evitare di utilizzare metodi di autenticazione basati solo su indirizzi IP.

- Mantenere aggiornati i più importanti pacchetti relativi alla rete e sottoscrivere le mailing list corrispondenti per ricevere gli annunci riguardanti nuove versioni di tali programmi (bind, sendmail, ssh e così via). Lo stesso concetto è valido per il software relativo alla sicurezza locale.

- Modificare il file `/etc/permissions` per ottimizzare le autorizzazioni dei file fondamentali per la sicurezza del sistema. Se si rimuove il bit setuid da un programma, è possibile che non possa più essere utilizzato nel modo previsto. D'altra parte, si consideri che nella maggior parte dei casi il programma non costituirà più un rischio potenziale per la sicurezza. Questo tipo di approccio può essere adottato per i file e per le directory di tipo world-writable.

- Disattivare tutti i servizi di rete che non sono assolutamente necessari per il corretto funzionamento del server, il sistema risulterà più sicuro. Le porte aperte con lo stato del socket LISTEN possono essere individuate con il programma netstat. Si consiglia di utilizzare l'opzione `netstat -ap` o `netstat -anp`. L'opzione `-p` consente di vedere quale processo occupa una porta e con quale nome.

Confrontare i risultati di netstat con quelli di una scansione completa delle porte eseguita dall'esterno dell'host. Un ottimo programma a questo scopo è nmap, poiché oltre al controllo delle porte nel computer in uso consente di trarre alcune conclusioni sui servizi in attesa su tali porte. La scansione delle porte può tuttavia essere interpretata come un'azione aggressiva, è quindi opportuno evitare di eseguirla in un host senza l'esplicita approvazione dell'amministratore. Ricordare infine che oltre alla scansione delle porte TCP è importante anche la scansione delle porte UDP (opzioni `-sS` e `-sU`).

- Per un monitoraggio efficiente dell'integrità dei file del sistema, utilizzare il programma AIDE (Advanced Intrusion Detection Environment) disponibile in SUSE Linux. Per impedirne la manomissione, cifrare il database creato da AIDE. Conservare inoltre una copia di backup di questo database all'esterno del computer in uso, memorizzandola in un supporto fisico non collegato al computer mediante un collegamento di rete.

- Installare programmi software di terze parti con cautela. Si sono verificati casi in cui un pirata informatico ha introdotto un trojan horse nell'archivio tar di un pacchetto software di sicurezza che è stato fortunatamente scoperto con tempestività. Se si installa un pacchetto di dati binari, verificare l'affidabilità del sito dal quale è stato scaricato.

  I pacchetti RPM di SUSE sono firmati con GPG. La chiave utilizzata da SUSE per la firma è la seguente:

  ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>

  Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

  Il comando `rpm --checksig package.rpm` consente di verificare se il valore checksum e la firma di un pacchetto non installato sono corretti. Cercare la chiave nel primo CD della distribuzione e nella maggior parte dei server delle chiavi disponibili nel mondo.

- Verificare regolarmente i backup dei file utente e di sistema. Se il funzionamento dei backup non viene verificato, è possibile che questi siano inservibili.

- Controllare i file di log. Quando possibile, creare un piccolo script per la ricerca di voci sospette. In effetti non si tratta di un'attività semplice poiché solo l'utente può sapere quali sono le voci insolite e quelle normali.

- Utilizzare `tcp_wrapper` per limitare l'accesso ai singoli servizi in esecuzione nel computer in uso, in modo da controllare esplicitamente quali indirizzi IP si connettono a un servizio. Per ulteriori informazioni su `tcp_wrapper`, consultare la documentazione di tcpd e hosts_access (`man 8 tcpd`, `man hosts_access`).
- Per migliorare la sicurezza fornita da tcpd (tcp_wrapper), utilizzare SuSEfirewall.
- Progettare misure di sicurezza ridondanti poiché è preferibile visualizzare due volte un messaggio piuttosto che non visualizzarne nessuno.

23.4.3 Indirizzo per l'invio di rapporti al centro di sicurezza

Se si individua un problema legato alla sicurezza, dopo aver controllato i pacchetti di aggiornamento disponibili inviare una e-mail a `security@suse.de`. Includere una descrizione dettagliata del problema e il numero di versione del pacchetto in questione. SUSE tenterà di fornire una risposta al più presto. Si consiglia di cifrare i messaggi e-mail con pgp. La chiave pgp di SUSE è la seguente:

```
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
```

Questa chiave può essere scaricata anche all'indirizzo `http://www.novell.com/linux/security/securitysupport.html` (in lingua inglese).

Elenchi di controllo dell'accesso in Linux

24

In questo capitolo vengono brevemente riepilogate le caratteristiche generali e le funzioni degli ACL POSIX (Elenchi di controllo dell'accesso) per file system Linux. Gli ACL possono essere utilizzati come un'estensione del concetto tradizionale di autorizzazione per oggetti file system. Tramite gli ACL è possibile definire le autorizzazioni in modo più flessibile rispetto al meccanismo convenzionale.

Il termine *ACL POSIX* indica che si tratta di uno standard POSIX (*Portable Operating System Interface*). Nonostante le relative proposte di standard POSIX 1003.1e e POSIX 1003.2c siano state revocate per vari motivi, gli ACL utilizzati in molti sistemi della famiglia UNIX si basano su tali proposte e l'implementazione degli ACL per file system illustrata in questo capitolo segue questi due standard. Il testo di questi standard è disponibile all'indirizzo `http://wt.xpilot.org/publications/posix.1e/` (in lingua inglese).

24.1 Vantaggi degli ACL

Per ogni oggetto file in un sistema Linux tradizionalmente vengono definiti tre set di autorizzazioni. Questi set includono le autorizzazioni di lettura (`r`), scrittura (`w`) ed esecuzione (`x`) per tre diversi tipi di utenti, ovvero il proprietario del file, il gruppo e gli altri utenti. È inoltre possibile impostare il bit *set user id*, *set group id* e *sticky*. Questo semplice concetto si adatta perfettamente alla maggior parte degli impieghi pratici. Tuttavia, per scenari più complessi o applicazioni avanzate, gli amministratori di sistema in precedenza dovevano ricorrere a una serie di espedienti per ovviare alle limitazioni del concetto tradizionale di autorizzazione.

Gli ACL possono essere utilizzati per situazioni che richiedono un'estensione del concetto tradizionale di autorizzazione per file. Consentono di assegnare autorizzazioni a singoli utenti o gruppi che non corrispondono al proprietario originale o al gruppo proprietario. Gli elenchi di controllo dell'accesso sono una funzionalità del kernel di Linux e attualmente sono supportati da ReiserFS, Ext2, Ext3, JFS e XFS. Tramite gli ACL è possibile creare scenari complessi senza implementare modelli di autorizzazione intricati a livello di applicazione.

I vantaggi offerti dagli ACL sono immediatamente evidenti in una situazione quale la sostituzione di un server Windows con un server Linux. Dopo il processo di migrazione, è possibile che alcune delle workstation connesse continuino a utilizzare Windows. Il sistema Linux offre servizi di stampa e file ai client Windows tramite Samba. Poiché Samba supporta gli elenchi di controllo dell'accesso, è possibile configurare autorizzazioni utente sia nel server Linux che in Windows tramite un'interfaccia utente grafica (solo in Windows NT e versione successiva). Con winbindd è inoltre possibile assegnare autorizzazioni a utenti che esistono solo nel dominio Windows e non dispongono di alcun account nel server Linux.

24.2 Definizioni

classe di utenti
: Il concetto tradizionale di autorizzazione POSIX prevede l'utilizzo di tre *classi* di utenti per l'assegnazione delle autorizzazioni nel file system, ovvero il proprietario, il gruppo proprietario e gli altri utenti. Per ogni classe di utenti è possibile impostare tre bit di autorizzazione per consentire a tali utenti di eseguire operazioni di lettura (`r`), scrittura (`w`) ed esecuzione (`x`).

ACL di accesso
: Le autorizzazioni di accesso di utenti e gruppi vengono determinate per tutti i tipi di oggetti file system (file e directory) tramite gli ACL di accesso.

ACL di default

: Gli ACL di default possono essere applicati solo alle directory. Determinano le autorizzazioni che un oggetto file system eredita dalla directory superiore quando viene creato.

voce ACL
Ogni ACL è costituito da un set di voci ACL. Una voce ACL contiene un tipo (vedere la Tabella 24.1, «Tipi di voci ACL» (p. 376)), un qualificatore dell'utente o del gruppo a cui la voce si riferisce e un set di autorizzazioni. Per alcuni tipi di voci, il qualificatore del gruppo o degli utenti non viene definito.

24.3 Gestione degli ACL

Nella Tabella 24.1, «Tipi di voci ACL» (p. 376) vengono riepilogati i sei possibili tipi di voci ACL, ognuno dei quali definisce le autorizzazioni di un utente o un gruppo di utenti. La voce *proprietario* definisce le autorizzazioni dell'utente proprietario del file o della directory. La voce *gruppo proprietario* definisce le autorizzazioni del gruppo proprietario del file. Il superuser può modificare il proprietario o il gruppo proprietario tramite il comando `chown` o `chgrp`, nel quale caso le voci del proprietario e del gruppo proprietario faranno riferimento al nuovo proprietario e al nuovo gruppo proprietario. Ogni voce *utente denominato* definisce le autorizzazioni dell'utente specificato nel campo del qualificatore della voce, ovvero il campo centrale nel formato testo illustrato nella Tabella 24.1, «Tipi di voci ACL» (p. 376). Ogni voce *gruppo denominato* definisce le autorizzazioni del gruppo specificato nel campo del qualificatore della voce. Il campo del qualificatore contiene un valore solo per le voci dell'utente denominato e del gruppo denominato. La voce *altri* definisce le autorizzazioni di tutti gli altri utenti.

La voce *maschera* limita ulteriormente le autorizzazioni concesse dalle voci *utente denominato*, *gruppo denominato* e *gruppo proprietario* in quanto definisce quali autorizzazioni di tali voci vengono effettivamente applicate e quali vengono mascherate. Se le autorizzazioni esistono sia in una delle voci menzionate che nella maschera, vengono applicate. Le autorizzazioni contenute solo nella maschera o solo nella voce non vengono applicate, il che significa che non vengono assegnate agli utenti. Tutte le autorizzazioni definite nelle voci *proprietario* e *gruppo proprietario* vengono sempre applicate. L'esempio riportato nella Tabella 24.2, «Mascheramento delle autorizzazioni di accesso» (p. 376) illustra il funzionamento di questo meccanismo.

Esistono due classi di ACL di base. Un ACL *minimo* contiene solo le voci per i tipi *proprietario*, *gruppo proprietario* e *altri*, che corrispondono ai bit di autorizzazione tradizionali per i file e le directory. Un ACL *esteso* include anche altri dati. Deve contenere una voce *maschera* e può contenere varie voci di tipo *utente denominato* e *gruppo denominato*.

Tabella 24.1 *Tipi di voci ACL*

Tipo	Formato testo
Proprietario	`user::rwx`
Utente denominato	`user:name:rwx`
Gruppo proprietario	`group::rwx`
Gruppo denominato	`group:name:rwx`
Maschera	`mask::rwx`
Altri	`other::rwx`

Tabella 24.2 *Mascheramento delle autorizzazioni di accesso*

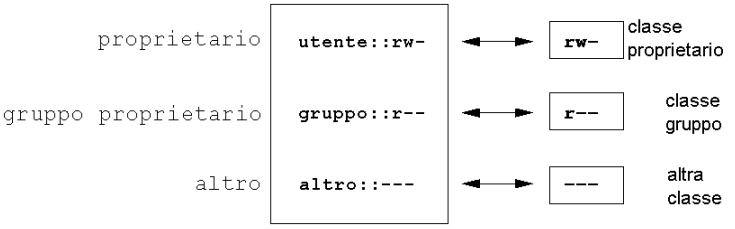
Tipo di voce	Formato testo	Autorizzazioni
Utente denominato	`user:geeko:r-x`	`r-x`
Maschera	`mask::rw-`	`rw-`
	Autorizzazioni effettive:	`r--`

24.3.1 Voci ACL e bit di autorizzazione in modalità file

Nella Figura 24.1, «ACL minimo: voci ACL e bit di autorizzazione» (p. 377) e nella Figura 24.2, «ACL esteso: voci ACL e bit di autorizzazione» (p. 377) vengono illustrati rispettivamente un ACL minimo e un ACL esteso. Queste figure sono suddivise in tre blocchi. Il blocco a sinistra indica il tipo di voce ACL, il blocco centrale contiene un ACL di esempio e il blocco a destra indica i bit di autorizzazione corrispondenti in base al concetto tradizionale di autorizzazione, ad esempio visualizzati da `ls -l`. In entrambi i casi, le autorizzazioni della *classe del proprietario* vengono mappate alla voce ACL *proprietario*. Le autorizzazioni della *classe degli altri utenti* vengono mappate alla voce

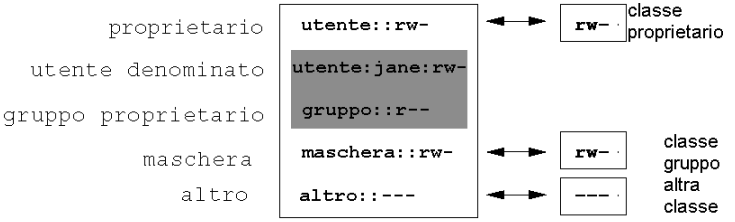
ACL corrispondente. La mappatura delle autorizzazioni della *classe del gruppo* è invece diversa nei due casi.

Figura 24.1 *ACL minimo: voci ACL e bit di autorizzazione*



Nel caso di un ACL minimo, senza la voce *maschera*, le autorizzazioni della *classe del gruppo* vengono mappate alla voce ACL *gruppo proprietario*. Questo meccanismo è illustrato nella Figura 24.1, «ACL minimo: voci ACL e bit di autorizzazione» (p. 377). Nel caso di un ACL esteso, con la voce *maschera*, le autorizzazioni della *classe del gruppo* vengono mappate alla voce *maschera*. Questo meccanismo è illustrato nella Figura 24.2, «ACL esteso: voci ACL e bit di autorizzazione» (p. 377).

Figura 24.2 *ACL esteso: voci ACL e bit di autorizzazione*



Questo tipo di mappatura garantisce un'agevole interazione tra le applicazioni, indipendentemente dal fatto che sia disponibile il supporto ACL. Le autorizzazioni di accesso assegnate tramite i bit di autorizzazione rappresentano il limite superiore per tutte le altre «ottimizzazioni» eseguite con un ACL. Le modifiche apportate ai bit di autorizzazione vengono aggiornate nell'ACL e viceversa.

24.3.2 Directory con un ACL di accesso

Nell'esempio riportato di seguito viene illustrata la gestione degli ACL di accesso.

Prima di creare la directory, utilizzare il comando `umask` per definire le autorizzazioni di accesso da mascherare ogni volta che viene creato un oggetto file. Il comando `umask 027` imposta le autorizzazioni di default assegnando al proprietario l'intera gamma di autorizzazioni (`0`), negando l'accesso in scrittura per il gruppo (`2`) e negando qualsiasi autorizzazione a tutti gli altri utenti (`7`). Il comando `umask` di fatto maschera o disattiva i bit di autorizzazione corrispondenti. Per informazioni, vedere la documentazione corrispondente (`man umask`).

Il comando `mkdir mydir` crea la directory `mydir` con le autorizzazioni di default definite da `umask`. Utilizzare `ls -dl mydir` per verificare che tutte le autorizzazioni siano state assegnate in modo corretto. L'output relativo a questo esempio è il seguente:

```
drwxr-x--- ... tux project3 ... mydir
```

Il comando `getfacl mydir` consente di verificare lo stato iniziale dell'ACL e fornisce informazioni quali:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

L'output del comando `getfacl` riflette con precisione la mappatura dei bit di autorizzazione e delle voci ACL descritta nella Sezione 24.3.1, «Voci ACL e bit di autorizzazione in modalità file» (p. 376). Nelle prime tre righe di output vengono indicati il nome, il proprietario e il gruppo proprietario della directory. Le tre righe successive contengono le tre voci ACL *proprietario*, *gruppo proprietario* e *altri*. Trattandosi di un ACL minimo, il comando `getfacl` non genera le informazioni fornite dal comando `ls`.

Modificare l'ACL per assegnare le autorizzazioni di lettura, scrittura ed esecuzione a un utente aggiuntivo denominato `geeko` e un gruppo aggiuntivo denominato `mascots` con il seguente comando:

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

L'opzione `-m` indica a `setfacl` di modificare l'ACL esistente. L'argomento successivo indica le voci ACL da modificare. Per separare voci multiple viene utilizzata la virgola. La parte finale specifica il nome della directory a cui devono essere applicate queste modifiche. Utilizzare il comando `getfacl` per esaminare l'ACL risultante.

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

Oltre alle voci inizializzate per l'utente `geeko` e il gruppo `mascots`, è stata generata una voce *maschera*. La voce *maschera* viene impostata automaticamente per rendere effettive tutte le autorizzazioni. Il comando `setfacl` adatta automaticamente le voci *maschera* esistenti in base alle impostazioni modificate, a meno che questa funzionalità non venga disattivata tramite l'opzione `-n`. La voce *maschera* definisce le autorizzazioni di accesso massime effettive per tutte le voci della *classe del gruppo*, tra cui *utente denominato*, *gruppo denominato* e *gruppo proprietario*. I bit di autorizzazione della *classe del gruppo* visualizzati dal comando `ls -dl mydir` ora corrispondono alla voce `maschera`.

```
drwxrwx---+ ... tux project3 ... mydir
```

La prima colonna dell'output ora contiene un carattere `+` aggiuntivo che indica la disponibilità di un ACL *esteso* per questo elemento.

In base all'output del comando `ls`, le autorizzazioni per la voce *maschera* includono l'accesso in scrittura. Tali bit di autorizzazione normalmente indicherebbero che il *gruppo proprietario*, in questo caso `project3`, dispone dell'accesso in scrittura alla directory `mydir`. Le autorizzazioni di accesso effettive di cui dispone il *gruppo proprietario*, tuttavia, risultano dalla sovrapposizione delle autorizzazioni definite per il *gruppo proprietario* e per la voce *maschera*, in questo esempio `r-x` (vedere la Tabella 24.2, «Mascheramento delle autorizzazioni di accesso» (p. 376)). Per quanto riguarda le autorizzazioni effettive del *gruppo proprietario* in questo esempio, nulla è cambiato dopo l'aggiunta delle voci ACL.

Modificare la voce *maschera* tramite il comando `setfacl` o `chmod`. Utilizzare ad esempio `chmod g-w mydir` . Il comando `ls -dl mydir` visualizzerà quindi le seguenti informazioni:

```
drwxr-x---+ ... tux project3 ... mydir
```

Il comando `getfacl mydir` fornisce il seguente output:

```
# file: mydir
# owner: tux
```

```
# group: project3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascots:rwx       # effective: r-x
mask::r-x
other::---
```

Dopo l'esecuzione del comando `chmod` per la rimozione dell'autorizzazione di scrittura dai bit della *classe del gruppo*, le informazioni contenute nell'output del comando `ls` sono sufficienti per capire che i bit della voce *maschera* sono stati modificati di conseguenza: l'autorizzazione di scrittura risulta di nuovo assegnata solo al proprietario di `mydir`. Questa situazione è confermata dall'output del comando `getfacl`. Questo output include un commento per tutte le voci in cui i bit di autorizzazione effettivi non corrispondono alle autorizzazioni originali perché vengono filtrati in base alla voce *maschera*. Le autorizzazioni originali possono essere ripristinate in qualsiasi momento tramite il comando `chmod g+w mydir .`

24.3.3 Directory con un ACL di default

Alle directory è possibile assegnare un ACL di default, ovvero un tipo speciale di ACL che definisce le autorizzazioni di accesso ereditate dagli oggetti creati in tale directory. L'ACL di default ha effetto sia sulle sottodirectory che sui file.

Effetti di un ACL di default

Le autorizzazioni dell'ACL di default di una directory possono essere passate ai file e alle sottodirectory in essa contenuti in due diversi modi:

- Una sottodirectory eredita l'ACL di default della directory superiore sia come ACL di default che come ACL di accesso.
- Un file eredita l'ACL di default come ACL di accesso.

Tutte le chiamate di sistema che creano oggetti file system utilizzano un parametro `mode` che definisce le autorizzazioni di accesso del nuovo oggetto file system creato. Se la directory superiore non dispone di un ACL di default, i bit di autorizzazione definiti dal comando `umask` vengono sottratti dalle autorizzazioni passate dal parametro `mode` e il risultato viene assegnato al nuovo oggetto. Se la directory superiore dispone di un ACL di default, i bit di autorizzazione assegnati al nuovo oggetto sono determinati

dalla sovrapposizione delle autorizzazioni del parametro `mode` e di quelle definite nell'ACL di default. Il comando `umask` in questo caso viene ignorato.

Applicazione di ACL di default

Nei tre esempi riportati di seguito vengono illustrate le operazioni principali da eseguire per le directory e gli ACL di default:

1. Aggiungere un ACL di default alla directory esistente `mydir` con il seguente comando:

   ```
   setfacl -d -m group:mascots:r-x mydir
   ```

   L'opzione `-d` del comando `setfacl` indica a `setfacl` di apportare nell'ACL di default le modifiche indicate dall'opzione `-m` successiva.

   Di seguito viene riportato il risultato di questo comando:

   ```
   getfacl mydir

   # file: mydir
   # owner: tux
   # group: project3
   user::rwx
   user:geeko:rwx
   group::r-x
   group:mascots:rwx
   mask::rwx
   other::---
   default:user::rwx
   default:group::r-x
   default:group:mascots:r-x
   default:mask::r-x
   default:other::---
   ```

   Il comando `getfacl` restituisce sia l'ACL di accesso che l'ACL di default. L'ACL di default comprende tutte le righe che iniziano con `default`. Anche se il comando `setfacl` è stato eseguito con una sola voce relativa al gruppo `mascots` per l'ACL di default, sono state copiate automaticamente tutte le altre voci dell'ACL di accesso per creare un ACL di default valido. Gli ACL di default non hanno un effetto immediato sulle autorizzazioni di accesso. Vengono utilizzati solo quando viene creato un oggetto file system. Questi nuovi oggetti ereditano le autorizzazioni solo dall'ACL di default della directory superiore.

2. Nell'esempio successivo viene utilizzato il comando `mkdir` per creare una sottodirectory di `mydir` che eredita l'ACL di default.

```
mkdir mydir/mysubdir

getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: project3
user::rwx
group::r-x
group:mascots:r-x
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

   Come previsto, la nuova sottodirectory creata `mysubdir` dispone delle autorizzazioni dell'ACL di default della directory superiore. L'ACL di accesso di `mysubdir` corrisponde esattamente all'ACL di default di `mydir`. Lo stesso dicasi per l'ACL di default che questa directory passerà agli oggetti subordinati.

3. Utilizzare il comando `touch` per creare un file nella directory `mydir`, ad esempio `touch mydir/myfile` . Il comando `ls -l mydir/myfile` visualizzerà quindi le seguenti informazioni:

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

   L'output del comando `getfacl mydir/myfile` è il seguente:

```
# file: mydir/myfile
# owner: tux
# group: project3
user::rw-
group::r-x          # effective:r--
group:mascots:r-x   # effective:r--
mask::r--
other::---
```

   Il comando `touch` utilizza un parametro `mode` con il valore `0666` per la creazione di nuovi file, il che significa che i file vengono creati con autorizzazioni di lettura e scrittura per tutte le classi di utenti, a condizione che non vengano imposte altre restrizioni nel comando `umask` o nell'ACL di default (vedere la sezione chiamata «Effetti di un ACL di default» (p. 380)). Questo in pratica

significa che tutte le autorizzazioni di accesso non specificate nel valore di `mode` vengono rimosse dalle voci ACL corrispondenti. Nonostante dalla voce ACL della *classe del gruppo* non sia stata rimossa alcuna autorizzazione, la voce *maschera* è stata modificata per mascherare le autorizzazioni non impostate in `mode`.

Questo approccio garantisce un'agevole interazione tra le applicazioni, ad esempio i compilatori, tramite gli ACL. È possibile creare file con autorizzazioni di accesso limitate e successivamente contrassegnarli come eseguibili. Grazie al meccanismo del comando `mask`, questi file potranno essere eseguiti come desiderato dagli utenti e dai gruppi corretti.

24.3.4 Algoritmo di controllo dell'ACL

Prima di consentire a un processo o un'applicazione di accedere a un oggetto file system protetto da un ACL, viene applicato un algoritmo di controllo. In genere, le voci ACL vengono esaminate nella seguente sequenza: *proprietario*, *utente denominato*, *gruppo proprietario* o *gruppo denominato* e *altri*. L'accesso viene gestito in base alla voce più adatta al processo. Le autorizzazioni non sono cumulative.

Se un processo appartiene a più gruppi ed è potenzialmente appropriato per più voci *gruppo*, la situazione diventa più complessa. Viene selezionata casualmente una voce tra quelle adatte contenenti le autorizzazioni necessarie. La voce che genera il risultato finale di «concessione dell'accesso» è irrilevante. In modo analogo, se nessuna delle voci *gruppo* adatte contiene le autorizzazioni necessarie, una voce selezionata casualmente genererà il risultato finale di «negazione dell'accesso».

24.4 Supporto ACL nelle applicazioni

Gli ACL possono essere utilizzati per implementare scenari di autorizzazione estremamente complessi in grado di soddisfare i requisiti delle moderne applicazioni. È possibile utilizzare il concetto tradizionale di autorizzazione in combinazione con gli ACL in modo da ottenere un sistema di protezione efficiente. I comandi di base per i file (`cp`, `mv`, `ls` e così via) supportano gli ACL, così come Samba.

Il supporto ACL, tuttavia, non è ancora disponibile in molti editor e strumenti di gestione dei file. Quando si copiano file con Konqueror, ad esempio, gli ACL di questi file

vengono persi. Quando si modificano file con un editor, gli ACL dei file vengono mantenuti solo se la modalità di backup dell'editor utilizzato lo consente. Se l'editor scrive le modifiche nel file originale, l'ACL di accesso viene mantenuto. Se l'editor salva il contenuto aggiornato in un nuovo file a cui successivamente viene assegnato il nome del file precedente, è possibile che gli ACL vengano persi se non sono supportati dall'editor. Fatta eccezione per star archiver, attualmente nessuna applicazione di backup mantiene gli ACL.

24.5 Ulteriori informazioni

Informazioni dettagliate sugli ACL sono disponibili all'indirizzo `http://acl.bestbits.at/` (in lingua inglese). Vedere inoltre la documentazione di `getfacl(1)`, `acl(5)` e `setfacl(1)`.

25 Utility di monitoraggio del sistema

In questo capitolo vengono illustrati alcuni dei numerosi programmi e meccanismi che è possibile utilizzare per esaminare lo stato del sistema. Vengono inoltre descritte alcune utility che semplificano l'esecuzione di operazioni ripetitive con i relativi principali parametri.

Per ogni comando vengono forniti esempi degli output rilevanti. In tali esempi la prima riga contiene il comando vero e proprio, preceduto dal prompt con il segno di dollaro. I commenti sono racchiusi tra parentesi quadre (`[...]`) e le righe lunghe dove necessario vengono riportate a capo. Le interruzioni di riga sono indicate da una barra rovesciata (\).

```
$ command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

Al fine di poter presentare il maggior numero di utility possibile, la lunghezza delle descrizioni è stata volutamente limitata. Per ulteriori informazioni su tutti questi comandi, vedere le rispettive documentazioni. La maggior parte di questi comandi supporta inoltre l'opzione `--help`, che consente di visualizzare un breve elenco dei parametri utilizzabili.

25.1 Elenco dei file aperti: lsof

Per visualizzare un elenco di tutti i file aperti per un processo con l'ID di processo *PID*, utilizzare `-p`. Ad esempio, per visualizzare tutti i file utilizzati dalla shell attuale, immettere:

```
$ lsof -p $$
COMMAND  PID USER   FD   TYPE DEVICE    SIZE     NODE NAME
zsh     4694   jj  cwd    DIR   0,18     144 25487368 /suse/jj/t
(totan:/real-home/jj)
zsh     4694   jj  rtd    DIR    3,2     608        2 /
zsh     4694   jj  txt    REG    3,2  441296    20414 /bin/zsh
zsh     4694   jj  mem    REG    3,2  104484    10882 /lib/ld-2.3.3.so
zsh     4694   jj  mem    REG    3,2   11648    20610
/usr/lib/zsh/4.2.0/zsh/rlimits.so
[...]
zsh     4694   jj  mem    REG    3,2   13647    10891 /lib/libdl.so.2
zsh     4694   jj  mem    REG    3,2   88036    10894 /lib/libnsl.so.1
zsh     4694   jj  mem    REG    3,2  316410   147725 /lib/libncurses.so.5.4
zsh     4694   jj  mem    REG    3,2  170563    10909 /lib/tls/libm.so.6
zsh     4694   jj  mem    REG    3,2 1349081    10908 /lib/tls/libc.so.6
zsh     4694   jj  mem    REG    3,2      56    12410
/usr/lib/locale/de_DE.utf8/LC_TELEPHONE
[...]
zsh     4694   jj  mem    REG    3,2      59    14393
/usr/lib/locale/en_US/LC_NUMERIC
zsh     4694   jj  mem    REG    3,2  178476    14565
/usr/lib/locale/en_US/LC_CTYPE
zsh     4694   jj  mem    REG    3,2   56444    20598
/usr/lib/zsh/4.2.0/zsh/computil.so
zsh     4694   jj    0u   CHR 136,48              50 /dev/pts/48
zsh     4694   jj    1u   CHR 136,48              50 /dev/pts/48
zsh     4694   jj    2u   CHR 136,48              50 /dev/pts/48
zsh     4694   jj   10u   CHR 136,48              50 /dev/pts/48
```

In questo esempio è stata utilizzata la variabile di shell speciale `$$`, il cui valore corrisponde all'ID di processo della shell.

Se viene utilizzato senza specificare alcun parametro, il comando `lsof` consente di generare un elenco di tutti i file attualmente aperti. Poiché i file aperti sono spesso nell'ordine delle migliaia, un elenco completo risulta utile solo in rari casi. Per generare elenchi utili, è possibile utilizzare l'elenco di tutti i file in combinazione con apposite funzioni di ricerca. È ad esempio possibile visualizzare un elenco di tutti i dispositivi a caratteri utilizzati:

```
$ lsof | grep CHR
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
```

```
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
zsh        4694      jj    0u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    1u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    2u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj   10u   CHR 136,48               50 /dev/pts/48
X          6476    root  mem    CHR    1,1             38042 /dev/mem
lsof      13478      jj    0u   CHR 136,48               50 /dev/pts/48
lsof      13478      jj    2u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    1u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    2u   CHR 136,48               50 /dev/pts/48
```

25.2 Utente che accede ai file: fuser

Questo comando consente di individuare i processi o gli utenti che attualmente utilizzano determinati file. Si supponga, ad esempio, di voler smontare un file system montato in `/mnt`. Quando si tenta di eseguire il comando `umount`, viene segnalato che il dispositivo è occupato. In tal caso, è possibile utilizzare il comando `fuser` per individuare i processi che stanno utilizzando il dispositivo:

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt
                     jj        26597 f....  less
```

Dopo l'interruzione del processo `less`, in esecuzione su un altro terminale, è possibile smontare il file system.

25.3 Proprietà dei file: stat

Il comando `stat` consente di visualizzare le proprietà dei file:

```
$ stat xml-doc.txt
  File: `xml-doc.txt'
  Size: 632             Blocks: 8          IO Block: 4096   regular file
Device: eh/14d  Inode: 5938009     Links: 1
Access: (0644/-rw-r--r--)  Uid: (11994/      jj)   Gid: (   50/    suse)
Access: 2004-04-27 20:08:58.000000000 +0200
Modify: 2003-06-03 15:29:34.000000000 +0200
Change: 2003-07-23 17:48:27.000000000 +0200
```

Il parametro `--filesystem` consente di visualizzare i dettagli delle proprietà del file system in cui si trova il file specificato:

```
$ stat  . --filesystem File: "." ID: 0       Namelen: 255     Type: ext2/ext3

 $ stat  . --filesystem
  File: "."
    ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388   Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

Se si utilizza la shell z (`zsh`), è necessario immettere `/usr/bin/stat` poiché tale shell include un comando `stat` incorporato che prevede sia opzioni che un formato di output diversi:

```
% type stat
stat is a shell builtin
% stat .
device  769
inode   4554808
mode    16877
nlink   12
uid     11994
gid     50
rdev    0
size    4096
atime   1091536882
mtime   1091535740
ctime   1091535740
blksize 4096
blocks  8
link
```

25.4 Dispositivi USB: lsusb

Il comando `lsusb` consente di elencare tutti i dispositivi USB. È possibile utilizzare l'opzione `-v` per visualizzare ulteriori dettagli, che vengono recuperati dalla directory `/proc/bus/usb/`. Di seguito viene riportato l'output visualizzato dal comando `lsusb` dopo il collegamento di uno stick di memoria USB. Nell'ultima riga viene segnalata la presenza del nuovo dispositivo.

```
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 001: ID 0000:0000
Bus 001 Device 018: ID 0402:5634 ALi Corp.
```

25.5 Informazioni su un dispositivo SCSI: scsiinfo

Il comando `scsiinfo` consente di visualizzare le informazioni relative a un dispositivo SCSI. È possibile utilizzare l'opzione `-l` per generare un elenco di tutti i dispositivi SCSI rilevati dal sistema. Informazioni analoghe possono essere ottenute anche tramite il comando `lsscsi`. Di seguito viene riportato l'output visualizzato dal comando `scsiinfo -i /dev/sda`, che restituisce informazioni relative a un disco rigido. L'opzione `-a` consente di ottenere maggiori dettagli.

```
Inquiry command
---------------
Relative Address                  0
Wide bus 32                       0
Wide bus 16                       1
Synchronous neg.                  1
Linked Commands                   1
Command Queueing                  1
SftRe                             0
Device Type                       0
Peripheral Qualifier              0
Removable?                        0
Device Type Modifier              0
ISO Version                       0
ECMA Version                      0
ANSI Version                      3
AENC                              0
TrmIOP                            0
Response Data Format              2
Vendor:                   FUJITSU
Product:                  MAS3367NP
Revision level:           0104A0K7P43002BE
```

È presente un elenco di difetti che include due tabelle di blocchi non validi di un disco rigido: innanzitutto quella fornita dal produttore (tabella Manufacturer) e in secondo luogo l'elenco di blocchi non validi rilevati durante il funzionamento (tabella Grown). Se il numero di voci nella tabella Grown aumenta, potrebbe essere necessario sostituire il disco rigido.

25.6 Processi: top

Il comando `top`, acronimo di "table of processes" (tabella dei processi), consente di visualizzare un elenco dei processi che viene aggiornato ogni due secondi. Per terminare il programma, premere Q. Il parametro `-n 1` consente di terminare il programma dopo una sola visualizzazione dell'elenco dei processi. Di seguito viene riportato un esempio dell'output del comando `top -n 1`:

```
top - 14:19:53 up 62 days,  3:35, 14 users,  load average: 0.01, 0.02, 0.00
Tasks: 102 total,   7 running,  93 sleeping,   0 stopped,   2 zombie
Cpu(s):   0.3% user,   0.1% system,   0.0% nice,  99.6% idle
Mem:    514736k total,   497232k used,    17504k free,    56024k buffers
Swap:  1794736k total,   104544k used,  1690192k free,   235872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  Command
 1426 root      15   0  116m  41m  18m S  1.0  8.2  82:30.34 X
20836 jj        15   0   820  820  612 R  1.0  0.2   0:00.03 top
    1 root      15   0   100   96   72 S  0.0  0.0   0:08.43 init
    2 root      15   0     0    0    0 S  0.0  0.0   0:04.96 keventd
    3 root      34  19     0    0    0 S  0.0  0.0   0:00.99 ksoftirqd_CPU0
    4 root      15   0     0    0    0 S  0.0  0.0   0:33.63 kswapd
    5 root      15   0     0    0    0 S  0.0  0.0   0:00.71 bdflush
       [...]
 1362 root      15   0   488  452  404 S  0.0  0.1   0:00.02 nscd
 1363 root      15   0   488  452  404 S  0.0  0.1   0:00.04 nscd
 1377 root      17   0    56    4    4 S  0.0  0.0   0:00.00 mingetty
 1379 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
 1380 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
```

Se si preme F durante l'esecuzione di `top`, viene visualizzato un menu che consente di apportare sostanziali modifiche al formato dell'output.

Il parametro `-U UID` consente di monitorare solo i processi associati a un particolare utente. Sostituire *`UID`* con l'ID dell'utente. `top -U $(id -u nomeutente)` consente di recuperare l'UID dell'utente in base al nome utente e di visualizzare i relativi processi.

25.7 Elenco dei processi: ps

Il comando `ps` consente di generare un elenco dei processi. Se si aggiunge il parametro `r`, vengono visualizzati solo i processi nei quali sono in corso operazioni di elaborazione:

```
$ ps r
  PID TTY      STAT   TIME COMMAND
```

```
22163 pts/7    R      0:01 -zsh
 3396 pts/3    R      0:03 emacs new-makedoc.txt
20027 pts/7    R      0:25 emacs xml/common/utilities.xml
20974 pts/7    R      0:01 emacs jj.xml
27454 pts/7    R      0:00 ps r
```

Non utilizzare il segno meno davanti a questo parametro. Non tutti i parametri richiedono il segno meno. La documentazione relativa a questa utility può risultare particolarmente complessa per gli utenti comuni. È tuttavia possibile visualizzare una breve pagina di informazioni digitando il comando `ps --help`.

Per controllare il numero di processi `emacs` in esecuzione, utilizzare:

```
$ ps x | grep emacs
 1288 ?        S      0:07 emacs
 3396 pts/3    S      0:04 emacs new-makedoc.txt
 3475 ?        S      0:03 emacs .Xresources
20027 pts/7    S      0:40 emacs xml/common/utilities.xml
20974 pts/7    S      0:02 emacs jj.xml

$ pidof emacs
20974 20027 3475 3396 1288
```

Il parametro `-p` consente di selezionare i processi in base al relativo ID:

```
$ ps www -p $(pidof xterm)
  PID TTY      STAT   TIME COMMAND
 9025 ?        S      0:01 xterm -g 100x45+0+200
 9176 ?        S      0:00 xterm -g 100x45+0+200
29854 ?        S      0:21 xterm -g 100x75+20+0 -fn \
  -B&H-LucidaTypewriter-Medium-R-Normal-Sans-12-120-75-75-M-70-iso10646-1
 4378 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
25543 ?        S      0:02 xterm -g 100x45+0+200
22161 ?        R      0:14 xterm -g 100x45+0+200
16832 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
16912 ?        S      0:00 xterm -g 100x45+0+200
17861 ?        S      0:00 xterm -bg DarkSeaGreen1 -g 120x45+40+300
19930 ?        S      0:13 xterm -bg LightCyan
21686 ?        S      0:04 xterm -g 100x45+0+200 -fn \
lucidasanstypewriter-12
23104 ?        S      0:00 xterm -g 100x45+0+200
26547 ?        S      0:00 xterm -g 100x45+0+200
```

È possibile formattare l'elenco dei processi in base alle proprie esigenze. L'opzione `-L` restituisce un elenco di tutte le parole chiave. Immettere il seguente comando per generare un elenco di tutti i processi ordinato in base all'uso della memoria:

```
$ ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2    0 [ksoftirqd/0]
```

```
    3    0 [events/0]
   17    0 [kblockd/0]
[...]
10164 5260 xterm
31110 5300 xterm
17010 5356 xterm
 3896 29292 /usr/X11R6/bin/X -nolisten tcp -br vt7 -auth
/var/lib/xdm/authdir/au
```

25.8 Albero dei processi: pstree

Il comando `pstree` consente di visualizzare un elenco dei processi sotto forma di albero:

```
$ pstree
init-+-atd
     |-3*[automount]
     |-bdflush
     |-cron
  [...]
     |-usb-storage-1
     |-usb-storage-2
     |-10*[xterm---zsh]
     |-xterm---zsh---mutt
     |-2*[xterm---su---zsh]
     |-xterm---zsh---ssh
     |-xterm---zsh---pstree
     |-ypbind---ypbind---2*[ypbind]
     `-zsh---startx---xinit4-+-X
                             `-ctwm-+-xclock
                                    |-xload
                                    `-xosview.bin
```

Il parametro `-p` consente di aggiungere l'ID di processo a un nome specificato. Per visualizzare anche le righe di comando, utilizzare il parametro `-a`:

```
$ pstree -pa
init,1
  |-atd,1255
[...]
  `-zsh,1404
      `-startx,1407 /usr/X11R6/bin/startx
          `-xinit4,1419 /suse/jj/.xinitrc [...]
              |-X,1426 :0 -auth /suse/jj/.Xauthority
              `-ctwm,1440
                  |-xclock,1449 -d -geometry -0+0 -bg grey
                  |-xload,1450 -scale 2
                  `-xosview.bin,1451 +net -bat +net
```

25.9 Utenti e relative azioni: w

Il comando `w` consente di individuare gli utenti che hanno eseguito il login al sistema e le operazioni attualmente eseguite. Ad esempio:

```
$ w
 15:17:26 up 62 days,  4:33, 14 users,  load average: 0.00, 0.04, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
jj       pts/0     30Mar04  4days  0.50s  0.54s xterm -e su -l
jj       pts/1     23Mar04  5days  0.20s  0.20s -zsh
jj       pts/2     23Mar04  5days  1.28s  1.28s -zsh
jj       pts/3     23Mar04  3:28m  3.21s  0.50s -zsh
[...]
jj       pts/7     07Apr04  0.00s  9.02s  0.01s w
jj       pts/9     25Mar04  3:24m  7.70s  7.38s mutt
[...]
jj       pts/14    12:49   37:34   0.20s  0.13s ssh totan
```

L'ultima riga indica che l'utente jj ha stabilito una connessione di shell sicura (`ssh`) al computer `totan`. Se alcuni utenti di altri sistemi hanno eseguito il login da postazioni remote, il parametro `-f` consente di individuare i computer dai quali è stata stabilita la connessione.

25.10 Uso della memoria: free

L'utility `free` consente di esaminare l'uso della memoria RAM. Vengono visualizzate informazioni dettagliate relative alla memoria disponibile e utilizzata nonché alle aree di swap.

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

L'opzione `-m` consente di visualizzare tutte le dimensioni in megabyte:

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

Un dato particolarmente utile è quello incluso nella seguente riga:

```
-/+ buffers/cache:        191        311
```

Si tratta della quantità di memoria utilizzata dai buffer e dalle cache. Il parametro `-d ritardo` consente di impostare un numero di secondi (*`ritardo`*) per la frequenza di aggiornamento delle informazioni. Ad esempio, `free -d 1.5` esegue l'aggiornamento ogni 1,5 secondi.

25.11 Buffer ad anello del kernel: dmesg

Il kernel di Linux memorizza alcuni messaggi in un buffer ad anello. Per visualizzare questi messaggi, immettere il comando `dmesg`:

```
$ dmesg
[...]
sdc : READ CAPACITY failed.
sdc : status = 1, message = 00, host = 0, driver = 08
Info fld=0xa00 (nonstd), Current sd00:00: sense key Not Ready
sdc : block size assumed to be 512 bytes, disk size 1GB.
sdc: test WP failed, assume Write Enabled
 sdc: I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 unable to read partition table
 I/O error: dev 08:20, sector 0
nfs: server totan not responding, still trying
nfs: server totan OK
```

Nell'ultima riga viene segnalata la presenza di un problema temporaneo nel server NFS `totan`. Le righe precedenti sono generate dal collegamento di un'unità flash USB. Gli eventi meno recenti sono registrati nei file `/var/log/messages` e `/var/log/warn`.

25.12 File system e relativo uso: mount, df e du

Il comando `mount` consente di visualizzare informazioni riguardanti il file system montato (dispositivo e tipo) e il relativo punto di montaggio:

```
$ mount
/dev/hdb2 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /data type ext2 (rw)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
automount(pid1012) on /suse type autofs \
    (rw,fd=5,pgrp=1012,minproto=2,maxproto=3)
totan:/real-home/jj on /suse/jj type nfs \
    (rw,nosuid,rsize=8192,wsize=8192,hard,intr,nolock,addr=10.10.0.1)
```

È possibile visualizzare informazioni sull'uso complessivo dei file system mediante il comando `df`. Il parametro `-h` (o `--human-readable`) consente di ottenere un output in formato comprensibile per gli utenti comuni.

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdb2             7.4G  5.1G  2.0G  73% /
/dev/hda1              74G  5.8G   65G   9% /data
shmfs                 252M     0  252M   0% /dev/shm
totan:/real-home/jj   350G  324G   27G  93% /suse/jj
```

Gli utenti del file server NFS `totan` devono svuotare le rispettive home directory immediatamente. È possibile visualizzare le dimensioni totali di tutti i file presenti in una determinata directory e nelle relative sottodirectory mediante il comando `du`. Il parametro `-s` consente di escludere i dettagli dall'output. Il parametro `-h` consente anche in questo caso di trasformare i dati in un formato comprensibile da chiunque. Il seguente comando:

```
$ du -sh ~
361M    /suse/jj
```

consente di visualizzare la quantità di spazio occupata dalla propria home directory.

25.13 File system /proc

Si tratta diun file system fittizio in cui il kernel memorizza informazioni importanti sotto forma di file virtuali. È ad esempio possibile visualizzare il tipo di CPU con il seguente comando:

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

Il seguente comando consente di recuperare informazioni relative all'allocazione e all'uso degli interrupt:

```
$ cat /proc/interrupts
           CPU0
  0:  537544462          XT-PIC  timer
  1:     820082          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          2          XT-PIC  rtc
  9:          0          XT-PIC  acpi
 10:      13970          XT-PIC  usb-uhci, usb-uhci
 11:  146467509          XT-PIC  ehci_hcd, usb-uhci, eth0
 12:    8061393          XT-PIC  PS/2 Mouse
 14:    2465743          XT-PIC  ide0
 15:       1355          XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

Di seguito viene brevemente descritto il contenuto di alcuni file importanti:

/proc/devices
: Dispositivi disponibili.

/proc/modules
: Moduli del kernel caricati.

/proc/cmdline
Riga di comando del kernel.

/proc/meminfo
Informazioni dettagliate sull'uso della memoria.

/proc/config.gz
File di configurazione, compresso con `gzip`, del kernel attualmente in esecuzione.

Per ulteriori informazioni, vedere il file di testo `/usr/src/linux/Documentation/filesystems/proc.txt`. Le informazioni sui processi in esecuzione sono disponibili nelle directory `/proc/`*`NNN`*, dove *`NNN`* rappresenta l'ID del processo rilevante (PID). Le caratteristiche di ogni processo si trovano in `/proc/self/`:

```
$ ls -l /proc/self
lrwxrwxrwx  1 root root 64 Apr 29 13:52 /proc/self -> 27585

$ ls -l /proc/self/
total 0
dr-xr-xr-x  2 jj suse 0 Apr 29 13:52 attr
-r--------  1 jj suse 0 Apr 29 13:52 auxv
-r--r--r--  1 jj suse 0 Apr 29 13:52 cmdline
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 cwd -> /suse/jj/t
-r--r--r--  1 jj suse 0 Apr 29 13:52 delay
-r--------  1 jj suse 0 Apr 29 13:52 environ
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 exe -> /bin/ls
dr-x------  2 jj suse 0 Apr 29 13:52 fd
-rw-------  1 jj suse 0 Apr 29 13:52 mapped_base
-r--r--r--  1 jj suse 0 Apr 29 13:52 maps
-rw-------  1 jj suse 0 Apr 29 13:52 mem
-r--r--r--  1 jj suse 0 Apr 29 13:52 mounts
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 root -> /
-r--r--r--  1 jj suse 0 Apr 29 13:52 stat
-r--r--r--  1 jj suse 0 Apr 29 13:52 statm
-r--r--r--  1 jj suse 0 Apr 29 13:52 status
dr-xr-xr-x  3 jj suse 0 Apr 29 13:52 task
-r--r--r--  1 jj suse 0 Apr 29 13:52 wchan
```

Le assegnazioni degli indirizzi di file eseguibili e librerie sono riportate nel file `maps`:

```
$ cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:02 22890      /bin/cat
0804c000-0804d000 rw-p 00003000 03:02 22890      /bin/cat
0804d000-0806e000 rwxp 0804d000 00:00 0
40000000-40016000 r-xp 00000000 03:02 10882      /lib/ld-2.3.3.so
40016000-40017000 rw-p 00015000 03:02 10882      /lib/ld-2.3.3.so
40017000-40018000 rw-p 40017000 00:00 0
4002b000-40135000 r-xp 00000000 03:02 10908      /lib/tls/libc.so.6
```

```
40135000-4013d000 rw-p 0010a000 03:02 10908      /lib/tls/libc.so.6
4013d000-40141000 rw-p 4013d000 00:00 0
bfffe000-c0000000 rw-p bfffe000 00:00 0
ffffe000-fffff000 ---p 00000000 00:00 0
```

25.14 vmstat, iostat e mpstat

L'utility `vmstat` consente di visualizzare statistiche relative alla memoria virtuale. Queste informazioni vengono recuperate dai file `/proc/meminfo`, `/proc/stat` e `/proc/*/stat`. Questi dati possono essere utilizzati per individuare colli di bottiglia nelle prestazioni del sistema. Il comando `iostat` consente di visualizzare statistiche relative alla CPU e all'input e all'output di dispositivi e partizioni. I dati visualizzati vengono recuperati dai file `/proc/stat` e `/proc/partitions`. L'output ottenuto può essere utilizzato per ottimizzare il bilanciamento del carico di input e output tra i dischi rigidi. Il comando `mpstat` consente di visualizzare statistiche correlate alla CPU.

25.15 procinfo

Il comando `procinfo` consente di generare un riepilogo contenente informazioni importanti relative al file system `/proc`:

```
$ procinfo
Linux 2.6.4-54.5-default (geeko@buildhost) (gcc 3.3.3 ) #1 1CPU [roth.suse.de]


Memory:      Total        Used        Free      Shared     Buffers
Mem:        516696      513200        3496           0       43284
Swap:       530136        1352      528784

Bootup: Wed Jul  7 14:29:08 2004    Load average: 0.07 0.04 0.01 1/126 5302

user  :       2:42:28.08   1.3%  page in :        0
nice  :       0:31:57.13   0.2%  page out:        0
system:       0:38:32.23   0.3%  swap in :        0
idle  :   3d 19:26:05.93  97.7%  swap out:        0
uptime:   4d  0:22:25.84         context :207939498

irq  0: 776561217 timer                  irq  8:         2 rtc

irq  1:    276048 i8042                  irq  9:     24300 VIA8233

irq  2:         0 cascade [4]          irq 11:  38610118 acpi, eth0, uhci_hcd
```

```
irq  3:          3                          irq 12:   3435071 i8042

irq  4:          3                          irq 14:   2236471 ide0

irq  6:          2                          irq 15:       251 ide1
```

Per visualizzare tutte le informazioni, utilizzare il parametro `-a`. Il parametro `-nN` consente di aggiornare le informazioni ogni *N* secondi. Se si imposta questo parametro, è possibile terminare il programma premendo Q.

Per default, vengono visualizzati valori cumulativi. Il parametro `-d` restituisce i valori differenziali. `procinfo -dn5` consente di visualizzare i valori che hanno subito modifiche negli ultimi 5 secondi.

```
Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:             0           2          -2           0           0           0
Swap:            0           0           0

Bootup: Wed Feb 25 09:44:17 2004    Load average: 0.00 0.00 0.00 1/106 31902

user  :       0:00:00.02   0.4%  page in :        0  disk 1:        0r       0w
nice  :       0:00:00.00   0.0%  page out:        0  disk 2:        0r       0w
system:       0:00:00.00   0.0%  swap in :        0  disk 3:        0r       0w
idle  :       0:00:04.99  99.6%  swap out:        0  disk 4:        0r       0w
uptime:  64d  3:59:12.62         context :     1087

irq  0:       501 timer                 irq 10:         0 usb-uhci, usb-uhci
irq  1:         1 keyboard              irq 11:        32 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]           irq 12:       132 PS/2 Mouse
irq  6:         0                       irq 14:         0 ide0
irq  8:         0 rtc                   irq 15:         0 ide1
irq  9:         0 acpi
```

25.16 Risorse PCI: lspci

Il comando `lspci` consente di visualizzare un elenco delle risorse PCI:

```
$ lspci
00:00.0 Host bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333]
00:01.0 PCI bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333 AGP]
00:0b.0 Ethernet controller: Digital Equipment Corporation \
    DECchip 21140 [FasterNet] (rev 22)
00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)
00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge
```

```
00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B \
    PIPC Bus Master IDE (rev 06)
00:11.5 Multimedia audio controller: VIA Technologies, Inc. \
    VT8233 AC97 Audio Controller (rev 50)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. \
    MGA G550 AGP (rev 01)
```

È possibile utilizzare il parametro `-v` per ottenere un elenco più dettagliato:

```
$ lspci -v
[...]
01:00.0 \
 VGA compatible controller: Matrox Graphics, Inc. MGA G550 AGP (rev 01) \
    (prog-if 00 [VGA])
 Subsystem: Matrox Graphics, Inc. Millennium G550 Dual Head DDR 32Mb
 Flags: bus master, medium devsel, latency 32, IRQ 10
 Memory at d8000000 (32-bit, prefetchable) [size=32M]
 Memory at da000000 (32-bit, non-prefetchable) [size=16K]
 Memory at db000000 (32-bit, non-prefetchable) [size=8M]
 Expansion ROM at <unassigned> [disabled] [size=128K]
 Capabilities: <available only to root>
```

Le informazioni sulla risoluzione dei nomi dei dispositivi vengono recuperate dal file `/usr/share/pci.ids`. Gli ID di PCI non presenti in questo file vengono contrassegnati come «Unknown device» (dispositivo sconosciuto).

Il parametro `-vv` restituisce tutte le informazioni che è stato possibile recuperare mediante il programma. Per visualizzare solo valori numerici, è necessario utilizzare il parametro `-n`.

25.17 Chiamate di sistema di un programma eseguito: strace

L'utility `strace` consente di analizzare tutte le chiamate di sistema di un processo attualmente in esecuzione. Immettere il comando nel modo consueto e aggiungere l'utility `strace` all'inizio della riga:

```
$ strace -e open ls

execve("/bin/ls", ["ls"], [/* 88 vars */]) = 0
uname({sys="Linux", node="edison", ...}) = 0
brk(0)                                  = 0x805b000
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
          = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
```

```
fstat64(3, {st_mode=S_IFREG|0644, st_size=76333, ...}) = 0
old_mmap(NULL, 76333, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
[...]
ioctl(1, SNDCTL_TMR_TIMEBASE or TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=53, ws_col=110, ws_xpixel=897, ws_ypixel=693}) = 0
open(".", O_RDONLY|O_NONBLOCK|O_LARGEFILE|O_DIRECTORY) = 3
fstat64(3, {st_mode=S_IFDIR|0755, st_size=144, ...}) = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
getdents64(3, /* 5 entries */, 4096)    = 160
getdents64(3, /* 0 entries */, 4096)    = 0
close(3)                                = 0
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 48), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
          = 0x40018000
write(1, "ltrace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

Per analizzare ad esempio tutti i tentativi di apertura di un determinato file, utilizzare il seguente comando:

```
$ strace -e open ls myfile.txt

open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/tls/librt.so.1", O_RDONLY)   = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libselinux.so.1", O_RDONLY)  = 3
open("/lib/tls/libc.so.6", O_RDONLY)    = 3
open("/lib/tls/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
open("/proc/mounts", O_RDONLY)          = 3
[...]
open("/proc/filesystems", O_RDONLY)     = 3
open("/proc/self/attr/current", O_RDONLY) = 4
```

Per analizzare tutti i processi secondari, utilizzare il parametro `-f`. Sono disponibili numerose opzioni che consentono di controllare il funzionamento e il formato di output del comando strace. Per informazioni, vedere `man strace`.

25.18 Chiamate di libreria di un programma eseguito: ltrace

L'utility `ltrace` consente di analizzare tutte le chiamate di libreria di un processo. Questo comando viene utilizzato in modo analogo all'utility `strace`. Il parametro `-c` restituisce il numero e la durata delle chiamate di libreria eseguite:

```
$ ltrace -c find /usr/share/doc
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 86.27    1.071814          30     35327           write
 10.15    0.126092          38      3297           getdents64
  2.33    0.028931           3     10208           lstat64
  0.55    0.006861           2      3122         1 chdir
  0.39    0.004890           3      1567         2 open
[...]
  0.00    0.000003           3         1           uname
  0.00    0.000001           1         1           time
------ ----------- ----------- --------- --------- ----------------
100.00    1.242403                 58269         3 total
```

25.19 Impostazione della libreria necessaria: ldd

Il comando `ldd` consente di individuare le librerie che caricheranno il file eseguibile dinamico specificato come argomento:

```
$ ldd /bin/ls
linux-gate.so.1 =>  (0xffffe000)
librt.so.1 => /lib/tls/librt.so.1 (0x4002b000)
libacl.so.1 => /lib/libacl.so.1 (0x40033000)
libselinux.so.1 => /lib/libselinux.so.1 (0x40039000)
libc.so.6 => /lib/tls/libc.so.6 (0x40048000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x4015d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
libattr.so.1 => /lib/libattr.so.1 (0x4016d000)
```

I file binari statici non richiedono librerie dinamiche:

```
$ ldd /bin/sash
        not a dynamic executable
$ file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, statically linked, stripped
```

25.20 Ulteriori informazioni sui file binari ELF

È possibile leggere il contenuto dei file binari mediante l'utility `readelf`. Questo comando può essere utilizzato anche con file ELF creati per architetture hardware diverse:

```
$ readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8049b40
  Start of program headers:          52 (bytes into file)
  Start of section headers:          76192 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           40 (bytes)
  Number of section headers:         29
  Section header string table index: 26
```

25.21 Comunicazione tra processi: ipcs

Il comando `ipcs` restituisce un elenco delle risorse IPC attualmente in uso:

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x000027d9 5734403    toms       660        64528      2
0x00000000 5767172    toms       666        37044      2
0x00000000 5799941    toms       666        37044      2

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x000027d9 0          toms       660        1
```

```
------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

25.22 Calcolo della durata mediante time

È possibile calcolare la durata dell'esecuzione dei comandi mediante l'utility `time`. Sono disponibili due versioni di questo comando, ovvero come componente integrato della shell e come programma (`/usr/bin/time`).

```
$ time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

Parte VIII. Sistema

Applicazioni a 32 e 64 bit in ambienti di sistema a 64 bit

26

SUSE Linux è disponibile per numerose piattaforme a 64 bit. Ciò non significa che tutte le applicazioni incluse siano anch'esse state modificate per le piattaforme a 64 bit. SUSE Linux supporta l'uso di applicazioni a 32 bit in ambienti di sistema a 64 bit. Il presente capitolo offre una breve panoramica sul modo in cui tale supporto è implementato nelle piattaforme SUSE Linux a 64 bit. Vengono descritte la modalità di esecuzione delle applicazioni a 32 bit (supporto di runtime) e la procedura di compilazione che deve essere eseguita per le applicazioni a 32 bit in modo da consentirne l'esecuzione sia negli ambienti a 32 che in quelli a 64 bit. Vengono inoltre fornite informazioni sull'API del kernel nonché una descrizione su come le applicazioni a 32 bit possono essere eseguite in un kernel a 64 bit.

SUSE Linux per le piattaforme AMD64 e EM64T a 64 bit è progettato in modo che le applicazioni a 32 bit possano essere eseguite in ambienti a 64 bit «senza ulteriori modifiche». Mediante questo supporto, è possibile continuare a usare le proprie applicazioni a 32 bit senza dover attendere la disponibilità delle corrispondenti versioni a 64 bit.

26.1 Supporto di runtime

IMPORTANTE: Conflitti tra versioni di un'applicazione

Se un'applicazione è disponibile sia per ambienti a 32 che 64 bit, l'installazione di entrambe le versioni genera dei problemi. In tali casi, scegliere quale delle due versioni installare e usare.

Per un'esecuzione corretta, ogni applicazione richiede una serie di librerie. Purtroppo i nomi delle librerie nelle versioni a 32 e 64 bit sono identici. Per differenziarli, è necessario trovare un altro modo.

Per mantenere la compatibilità con la versione a 32 bit, le librerie vengono memorizzate nel sistema nella stessa ubicazione dell'ambiente a 32 bit. La versione a 32 bit di `libc.so.6` so trova in `/lib/libc.so.6` sia negli ambienti a 32 che in quelli a 64 bit.

Tutte le librerie e i file oggetto a 64 bit si trovano in directory denominate `lib64`. I file oggetto a 64 bit normalmente presenti in `/lib`, `/usr/lib` e `/usr/X11R6/lib` si trovano ora sotto `/lib64`, `/usr/lib64` e `/usr/X11R6/lib64`. Ciò significa che è possibile collocare le librerie a 32 bit sotto `/lib`, `/usr/lib` e `/usr/X11R6/lib` lasciando invariato il nome in entrambe le versioni.

Nessuna delle sottodirectory di oggetti il cui contenuto di dati è svincolato dalla dimensione delle parole è stata spostata. Ad esempio, i font X11 si trovano sempre nella solita ubicazione in `/usr/X11R6/lib/X11/fonts`. Questo schema è conforme con gli standard LSB (Linux Standards Base) e FHS (File System Hierarchy).

26.2 Sviluppo di software

Uno strumento di sviluppo bivalente consente la generazione di oggetti a 32 e 64 bit. Il valore di default è la compilazione di oggetti a 64 bit. Per generare oggetti a 32 bit, è possibile usare dei flag speciali. Per GCC, questo flag speciale è `-m32`.

Tutte i file di intestazione devono essere scritti in un formato indipendente dall'architettura. Le librerie a 32 e 64 bit installate devono disporre di un'API (interfaccia di programmazione dell'applicazione) corrispondente ai file di intestazione installati. L'ambiente SUSE normale è concepito in base a questo principio. Nel caso di librerie aggiornate manualmente, questi problemi devono essere risolti dall'utente stesso.

26.3 Compilazione di software in piattaforme bivalenti

Per sviluppare file binari per l'altra architettura in un'architettura bivalente, è necessario installare anche le rispettive librerie per la seconda architettura. Questi pacchetti sono

chiamati `rpmname-32bit`. Sarà inoltre necessario disporre delle rispettive intestazioni e librerie dei pacchetti `rpmname-devel` e delle librerie di sviluppo per la seconda architettura di `rpmname-devel-32bit`.

La maggior parte dei programmi open source usano configurazioni di programma basate su `autoconf`. Per configurare un programma per la seconda architettura mediante `autoconf`, sovrascrivere le impostazioni normali del linker e del compilatore di `autoconf` eseguendo lo script `configure` con ulteriori variabili d'ambiente.

Il seguente esempio si riferisce a un sistema AMD64 o EM64T con una seconda architettura x86:

1. Impostare `autoconf` per l'uso del compilatore a 32 bit:

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

2. Istruire il linker per l'elaborazione degli oggetti a 32 bit:

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

3. Impostare l'assemblatore per la generazione di oggetti a 32 bit:

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

4. Accertarsi che le librerie per `libtool` e altri pacchetti derivino da `/usr/lib`:

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

5. Accertarsi che le librerie vengano memorizzate nella sottodirectory `lib`:

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

6. Accertarsi che vengano usate le librerie X a 32 bit:

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

Queste variabili non sono tutte necessarie per tutti i programmi; adattarle a seconda del programma.

```
CC="gcc -m64"            \
LDFLAGS="-L/usr/lib64;"  \
        .configure       \
          --prefix=/usr  \
          --libdir=/usr/lib64
```

```
make
make install
```

26.4 Specifiche del kernel

I kernel a 64 bit per AMD64 e EM64T offrono un'ABI (interfaccia binaria dell'applicazione) sia per il kernel a 32 che per quello a 64 bit. L'ABI per il kernel a 64 bit è identica a quella del kernel a 32 bit. Ciò significa che l'applicazione a 32 bit è in grado di comunicare con il kernel a 64 bit nello stesso modo in cui comunica con il kernel a 32 bit.

L'emulazione a 32 bit delle chiamate di sistema al kernel a 64 bit non supporta numerose API usate dai programmi di sistema. Questo fenomeno varia a seconda della piattaforma. Per questo motivo, per funzionare correttamente, alcune applicazioni come `lspci` o i programmi di amministrazione LVM devono essere compilati a 64 bit.

Un kernel a 64-bit è in grado di caricare solo moduli per kernel a 64 bit appositamente compilati per tale kernel. Non è possibile usare moduli per kernel a 32 bit.

SUGGERIMENTO

Alcune applicazioni richiedono moduli caricabili dal kernel separati. Per usare tali applicazioni a 32 bit in ambienti di sistema a 64 bit, contattare il fornitore dell'applicazione e SUSE per verificare la disponibilità, per questo modulo, della versione a 64 bit del modulo caricabile dal kernel e quella della versione a 32 bit compilata dell'API del kernel.

27 Uso della shell

Anche se le interfacce utente grafiche stanno acquistando maggiore importanza per Linux, il mouse non è sempre il metodo migliore per eseguire task ricorrenti. Mediante la riga di comando, è possibile ottenere efficienza e flessibilità elevate. Le applicazioni basate sul testo sono particolarmente importanti per il controllo di computer su collegamenti di rete lenti, oppure se si desidera eseguire attività come `root` sulla riga di comando in xterm. La shell Bash è l'interprete di riga di comando di default in SUSE Linux.

Linux è un sistema multiutente; l'accesso ai file è controllato mediante autorizzazioni. Che si usi la riga di comando o un'interfaccia utente grafica, è utile comprendere il concetto delle autorizzazioni. Nell'utilizzo della riga di comando, sono importanti una serie di comandi. L'editor di testo vi viene spesso utilizzato nella configurazione di un sistema dalla riga di comando. È anche apprezzato da molti amministratori di sistema e sviluppatori.

27.1 Uso della shell bash sulla riga di comando

Nella barra dei task KDE è presente un'icona che raffigura un monitor con una conchiglia. Quando si clicca su questa icona, si apre la finestra di un terminale, nella quale inserire i comandi. Konsole, il programma del terminale, di solito esegue Bash (Bourne again shell), un programma sviluppato come parte del progetto GNU. Sul desktop di GNOME, per avviare un terminale che normalmente esegue Bash, fare clic sull'icona con il monitor di un computer nel riquadro superiore.

Una volta aperta la shell, osservare il prompt sulla prima riga. Di solito il prompt comprende il nome utente, il nome host e il percorso corrente, ma può essere personalizzato. Quando il cursore si trova dopo questo prompt, è possibile inviare comandi direttamente al proprio sistema informatico.

27.1.1 Immissione dei comandi

Un comando è composto da vari elementi. Il primo elemento è sempre il comando effettivo, seguito da parametri od opzioni. I comandi vengono eseguiti premendo Invio. Prima di effettuare questa operazione, modificare la riga di comando, aggiungere opzioni o correggere errori di battitura. Uno dei comandi utilizzati con maggiore frequenza è `ls`, che può essere utilizzato con o senza argomenti. Immettendo semplicemente `ls` il comando mostra i contenuti della directory corrente.

Le opzioni sono precedute da un trattino. Il comando `ls -l` , ad esempio, mostra i contenuti della stessa directory in modo dettagliato (formato listato lungo). Di fianco a ciascun nome di file, appare la data in cui è stato creato il file, la dimensione in byte e ulteriori dettagli descritti in seguito. Un'opzione importante che esiste per molti comandi è `--help`. Immettendo `ls --help` , appaiono tutte le opzioni per il comando `ls`.

È importante scrivere la «citazione» nel modo giusto. Se il nome di un file contiene uno spazio, sostituirlo utilizzando una barra inversa(`\`) o racchiuderlo tra virgolette semplici o doppie. In caso contrario Bash interpreta il nome di un file come `I miei documenti` come il nome di tre file o directory. La differenza tra le virgolette singole e quelle doppie è che l'espansione della variabile avviene con le virgolette doppie. Le virgolette semplici garantiscono che la shell veda la stringa tra virgolette alla lettera.

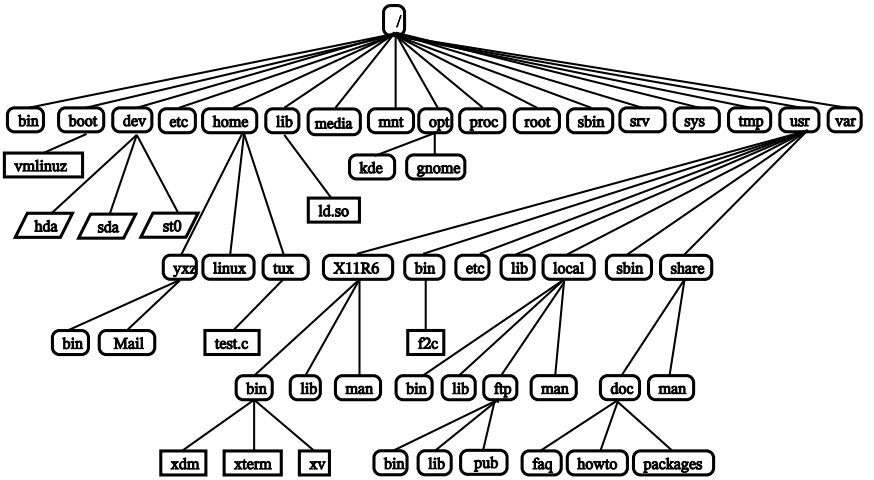
27.1.2 File e directory

Per utilizzare la shell in modo efficace, è molto utile conoscere le strutture dei file e delle directory di un sistema Linux. Si può pensare alle directory come a cartelle elettroniche nelle quali sono memorizzati file, programmi e sottodirectory. La directory di massimo livello nella gerarchia è la directory root menzionata come `/`. Da questa posizione è possibile accedere a tutte le altre directory.

La directory `/home` contiene le directory nelle quali i singoli utenti possono salvare i loro file personali. Figura 27.1, «Estratto da un albero delle directory standard» (p. 413)

mostra l'albero delle directory standard di Linux con le home directory degli utenti di esempio `xyz`, `linux`, e `tux`. L'albero delle directory di un sistema Linux ha una struttura funzionale che segue il*Filesystem Hierarchy Standard* (FHS). La lista qui di seguito riporta una breve descrizione delle directory standard presenti in Linux.

Figura 27.1 *Estratto da un albero delle directory standard*



/
Directory root, punto di inizio dell'albero delle directory

/home
Directory personali degli utenti

/dev
File dei dispositivi che rappresentano i componenti hardware

/etc
File importanti per la configurazione del sistema

/etc/init.d
Script di avvio

/usr/bin
Programmi generalmente accessibili

/bin
Programmi richiesti per primi nel processo di avvio

/usr/sbin
Programmi riservati all'amministratore del sistema

/sbin
Programmi riservati all'amministratore del sistema e necessari per l'avvio

/usr/include
File di intestazione per il compilatore C

/usr/include/g++
File di intestazione per il compilatore C++

/usr/share/doc
File relativi a documentazione varia

/usr/share/man
System manual pages (pagine man)

/usr/src
Codice sorgente del software di sistema

/usr/src/linux
Codice sorgente del kernel

/tmp, /var/tmp
File temporanei

/usr
Tutti i programmi delle applicazioni

/var
File di configurazione (ad esempio quelli collegati da `/usr`)

/var/log
File log di sistema

/var/adm
Dati relativi all'amministrazione del sistema

`/lib`
Librerie condivise (per i programmi collegati in modo dinamico)

`/proc`
File system di processo

`/sys`
File system di sistema nel quale sono riunite tutte le informazioni del dispositivo per il kernel

`/usr/local`
Estensioni locali indipendenti dalla distribuzione

`/opt`
Software facoltativo, pacchetti di programmi aggiuntivi di dimensioni maggiori (come KDE, GNOME, Netscape)

27.1.3 Caratteristiche di Bash

Esistono due caratteristiche importanti della shell che possono facilitare di molto il lavoro:

Cronologia
Per ripetere un comando precedentemente inserito, premere ↑ fino a quando non appare il comando al prompt. Spostarsi avanti nella lista dei comandi precedentemente inseriti premendo ↓. Per modificare la riga di comando, spostare il cursore nella posizione desiderata utilizzando i tasti con le frecce e iniziare la digitazione. Per effettuare una ricerca nella cronologia utilizzare Ctrl + R.

Completamento
Completare un nome di file in tutta la sua lunghezza dopo aver digitato le prime lettere fino a quando non viene individualmente identificato. Per eseguire questa operazione, digitare le prime lettere, quindi premere Tab. Se esistono diversi nomi di file che iniziano con le stesse lettere, è possibile ottenere una lista premendo due volte Tab.

Primo esempio: Gestione di file

Ora che gli utenti sanno come è un comando, quali directory esistono in SUSE Linux e come accelerare le cose quando si utilizza Bash, è importante mettere in pratica queste conoscenze con un piccolo esercizio.

1. Aprire una console dal desktop KDE o GNOME cliccando sull'icona della shell.

2. Immettere il comando`ls` per vedere i contenuti della propria home directory.

3. Utilizzare il comando `mkdir` (che corrisponde a*crea directory*) per creare una nuova sottodirectory chiamata `prova` immettendo `mkdir test`.

4. Ora lanciare un editor premendo Alt + F2 e immettendo`kate` Kate per KDE `gedit` per Gedit in GNOME. Digitare alcune lettere nell'editor, quindi salvare il file come `File di prova` nella propria directory. Linux distingue tra maiuscole e minuscole. Per questo esempio, utilizzare una F maiuscola.

5. Visualizzare di nuovo i contenuti della propria home directory. Anzichè digitare di nuovo `ls` premere semplicemente ↑ due volte; il comando `ls` dovrebbe riapparire al prompt. Per eseguire il comando, premere Invio. La directory `prova` appena creata dovrebbe apparire con lettere in azzurro e `File di prova` in nero. Questo esercizio dimostra come si possono distinguere directory e file in una console.

6. Spostare `File di prova`nella sottodirectory `prova` con il comando `mv`. Per accelerare l'operazione, utilizzare la funzione di espansione: immettere semplicemente `mv F` e premere Tab. Fino a quando, all'interno della directory, non ci sono altri file che iniziano con questa lettera, la shell espande il nome del file e aggiunge la stringa *estfile*. Altrimenti aggiungere una lettera o due e provare con Tab ogni volta per vedere se la shell è in grado di espandere il nome. Infine, digitare uno spazio quindi `prova` dopo il nome del file esteso e premere Invio per eseguire il comando.

7. A questo punto`File di prova` non dovrebbe essere più nella directory. Verificarlo immettendo di nuovo `ls`.

8. Per vedere se lo spostamento del file ha avuto esito positivo, modificare la directory `prova` con il comando`cd test`. Ora immettere di nuovo `ls`. Nel

listato dovrebbe apparire `File di prova`. Tornare di nuovo nella propria home directory in qualsiasi punto immettendo solo `cd`.

9. Per fare una copia del file, utilizzare `cp`. Ad esempio, immettere`cp File di prova Provabackup` per copiare `File di prova` in `Provabackup`. Ancora una volta, è possibile utilizzare il comando `ls` per veder se entrambi i file sono nella directory.

27.1.4 Indicazione dei percorsi

Quando si lavora con i file o con le directory, è importante indicare il percorso corretto. Non è comunque necessario immettere l'intero percorso (assoluto) dalla directory root al rispettivo file. È possibile iniziare dalla directory corrente. Indirizzare la propria home directory direttamente con ~. Questo significa che esistono due modi per elencare il file`File di prova`nella directory `prova`: immettendo il percorso relativo con `ls prova` o specificando il percorso assoluto con `ls ~/prova`.

Per ottenere una lista dei contenuti delle home directory degli altri utenti, immettere `ls ~username`. Nell'albero della directory di esempio, uno degli utenti campione è `tux`. In questo caso, `ls ~tux` dovrebbe elencare i contenuti della home directory di `tux`.

Rappresentare la directory corrente con un punto (`.`). Nell'albero, il livello successivo più elevato è rappresentato da due punti (`..`). Immettendo `ls ..`, è possibile vedere i contenuti della directory superiore della directory corrente. Il comando `ls ../..` mostra i contenuti della directory di due livelli superiori nella gerarchia.

Secondo esempio: Lavorare con i percorsi

Qui di seguito è riportato un altro esempio che mostra come muoversi nelle directory del sistema SUSE Linux.

1. Modificare la home directory con il comando `cd`. Quindi creare una directory all'interno di essa con il nome `prova2` immettendo `mkdir prova2`.

2. Modificare la nuova directory in `cd prova2` e creare una sottodirectory all'interno di essa con il nome`sottodirectory`. Per modificarla, utilizzare

la funzione espansione: immettere `cd su`quindi premere Tab. La shell espande il resto del nome della directory.

3. Ora, cercare di spostare il file precedentemente creato `Provabackup` nella directory corrente (`sottodirectory`) senza modificare di nuovo la directory. Per effettuare questa operazione, indicare il percorso relativo a quel file: `mv ../../test/Testbackup .` (notare il punto alla fine). Il punto alla fine di questo comando è necessario per dire alla shell che la directory corrente è la destinazione nella quale spostare il file. `../../`, in questo esempio, si riferisce alla propria home directory.

27.1.5 Caratteri jolly

Un'altra comodità offerta dalla shell sono i caratteri jolly per l'espansione del nome del percorso. In Bash ne esistono di tre tipi diversi:

?
: Esatta corrispondenza con un carattere arbitrario

*****
: Corrispondenza con qualsiasi numero di caratteri

[set]
: Corrisponde a uno dei caratteri dal gruppo indicato tra parentesi quadre, che è rappresentato dalla stringa *set*. Come parte di*set* è anche possibile indicare le classi di carattere utilizzando la sintassi *[:`classe`:]*, dove una classe è `alnum`, `alpha`, `ascii` e così via.

  L'utilizzo di `!` o `^` all'inizio del gruppo (*[!set]*) corrisponde a un carattere diverso da quelli identificati da *set*.

Supponendo che la directory `prova` contenga i file `File di prova`, `File di prova1`, `File di prova2` e `datafile`, il comando `ls File di prova?` elenca i file `File di prova1` e `File di prova2`. Con `ls Prova*`, la lista comprende anche`File di prova`. `ls *fil*` mostra tutti i file campione. Infine è possibile utilizzare il carattere jolly`set` per indicare tutti i file campione aventi un numero come ultimo carattere. `ls File di prova[1-9]` o uso di classi, `ls File di prova[[:digit:]]`.

Dei quattro tipi di caratteri jolly, il più inclusivo è l'asterisco. Può essere utilizzato per copiare tutti i file contenuti in una directory in un'altra o per cancellare tutti i file con un comando. Il comando `rm *fil*`, ad esempio, cancellerebbe tutti i file nella directory corrente il cui nome comprenda la stringa *fil*.

27.1.6 Less e More

Linux comprende due programmini per visualizzare i file di testo direttamente nella shell. Anzichè avviare un editor per leggere un file come `Readme.txt`, immettere semplicemente `less Readme.txt` per visualizzare il testo nella finestra della console. Utilizzare lo Spazio per scorrere la pagina verso il basso. Utilizzare i tasti Pagina su e Pagina giù per spostarsi all'interno del testo. Per uscire da less, premere Q.

Al posto di less, è possibile utilizzare il programma più vecchio more. Comunque, non è così comodo perchè non consente di scorrere la pagina verso il basso.

Il programma less ha preso il nome dalla massima *meno è di più* e può anche essere utilizzato per visualizzare in modo comodo l'output dei comandi. Per informazioni sul suo funzionamento, leggere Sezione 27.1.7, «Pipe e reindirizzamento» (p. 419).

27.1.7 Pipe e reindirizzamento

Di solito, l'output standard nella shella è lo schermo o la finestra della console e l'input standard è la tastiera. Per inoltrare l'output di un comando a un'applicazione come less, utilizzare una *pipeline*.

Per visualizzare i file nella directory `test`, immettere il comando`ls test | less`. I contenuti della directory `test` vengono quindi visualizzati con less. Questa operazione ha senso se l'output normale con `ls` fosse troppo lungo. Ad esempio, se si visualizzano i contenuti della directory `dev` con `ls /dev`, nella finestra se ne vede solo una piccola parte. Visualizzare l'intera lista con `ls /dev | less`.

È anhe possibile salvare l'output dei comandi in un file. Ad esempio, `echo "test one" > Content` genera un nuovo file chiamato `Content` contenente le parole`test one`. Visualizzare il file con `less Content`.

È anche possibile utilizzare un file come input per un comando. Ad esempio, con `tr` sostituire i caratteri dall'input standard reindirizzati dal file `Content` e scrivere il

risultato nell'output standard: sostituire `t` con `x`chiamando`tr t x < Content`. L'output di`tr`viene inviato allo schermo.

Se è necessario un nuovo file contenente l'output, collegare a cascata l'output di`tr` a un file. Per provare questa operazione, modificare `test` e immettere il comando `tr t x < ../Content > new`. Infine visualizzare `new` con `less new`.

Allo stesso modo dell'output standard, l'output di errore standard viene inviato alla console. In ogni caso, per reindirizzare l'output di errore standard a un file chiamato `errors`, aggiungere `2> errors` al comando corrispondente. Sia l'output standard, sia l'errore standard vengono salvati in un file chiamato `alloutput` se si aggiunge `>& alloutput`. Infine, per aggiungere l'output di un comando a un file già esistente, il comando deve essere seguito da `>>` anzichè`>`.

27.1.8 Archivi e compressione dei dati

A questo punto che è già stato creato un certo numero di file e directory, vengono presi in considerazione gli argomenti relativi agli archivi e alla compressione dei dati. Supponendo che si voglia avere l'intera directory `test` in un file da salvare su uno stick USB come copia di backup o inviarlo per e-mail. Per eseguire questa operazione, utilizzare il comando `tar` (per *tape archiver*). Con `tar --help`, visualizzare tutte le opzioni per il comando `tar`. Qui di seguito è riportata la spiegazione delle opzioni più importanti:

-c
: (come creare) Creare un nuovo archivio.

-t
: (come tabella) Visualizzare i contenuti di un archivio.

-x
: (come estrarre) Decomprimere l'archivio.

-v
: (come prolisso) Mostra tutti i file a video durante la creazione dell'archivio.

-f
: (come file) Scegliere un nome di file per il file dell'archivio. Durante la creazione di un archivio, questa opzione deve essere sempre data come ultima.

Per comprimere la directory `test` con tutti i suoi file e sottodirectory in un archivio chiamato `testarchive.tar`, utilizzare le opzioni `-c` e `-f`. Come prova, aggiungere anche `-v` per seguire l'avanzamento dell'archiviazione anche se questa opzione non è obbligatoria. Dopo aver utilizzato `cd` per modificare la propria home directory dove è posizionata la directory`test`, immettere `tar -cvf testarchive.tar test`. Dopo di che, visualizzare i contenuti del file dell'archivio con `tar -tf testarchive.tar`. La directory `test` con tutti i suoi file e directory sul disco rigido è rimasta invariata. Per decomprimere l'archivio, immettere `tar -xvf testarchive.tar`, ma attendere ancora.

Per la compressione dei file la scelta ovvia è `gzip` o, per un rapporto di compressione ancora migliore, `bzip2`. Immettere semplicemente `gzip testarchive.tar` (o `bzip2 testarchive.tar`, anche se in questo esempio è stato utilizzato `gzip`). Con `ls`, a questo punto si noterà che il file `testarchive.tar` non è più in questa posizione e che, invece, è stato creato il file`testarchive.tar.gz`. Questo file è molto più piccolo e quindi adatto al trasferimento via e-mail o all'archiviazione su uno stick USB.

Ora, decomprimere questo file nella directory`test2` creata in precedenza. Per eseguire questa operazione, immettere `cp testarchive.tar.gz test2` per copiare il file in quella directory. Modificare la directory con `cd test2`. Ora è possibile decomprimere un file compresso con estensione `.tar.gz` con il comando`gunzip`. Immettere `gunzip testarchive.tar.gz`, che darà il file `testarchive.tar`, che dovrà essere estratto o *decompresso* con `tar -xvf testarchive.tar`. È anche possibile decomprimere ed estrarre un archivio compresso in un solo passaggio con `tar -xvf testarchive.tar.gz` (non è più necessario aggiungere l'opzione`-z`). Con `ls`, è possibile vedere che è stata creata una nuova directory `test` con gli stessi contenuti della directory `test` presente nella home directory.

27.1.9 mtools

Gli`mtools` sono un set di comandi per lavorare con i file system MS-DOS. I comandi inclusi in`mtools` consentono di indirizzare la prima unità floppy come `a:`, analogamente a MS-DOS e i comandi sono gli stessi di MS-DOS con la sola eccezione che sono preceduti dal prefisso `m`.

`mdir a:`
Visualizza i contenuti del disco floppy nell'unità `a:`

mcopy Testfile a:
Copia il file `Testfile` sul disco floppy

mdel a:Testfile
Cancella `Testfile` in `a:`

mformat a:
Formatta il disco floppy in formato in MS-DOS (con il comando`fdformat`)

mcd a:
Trasforma `a:` in directory corrente

mmd a:test
Crea ka sottodirectory `test` sul disco floppy

mrd a:test
Cancella la sottodirectory `test` dal disco floppy

27.1.10 Ripulitura

Al termine di questo corso intensivo, l'utente dovrebbe essere a conoscenza delle nozioni fondamentali relative alla shell Linux o alla riga di comando. A questo punto è possibile ripulire la propria home directory cancellando i vari file di prova e le directory con i comandi `rm` e `rmdir`. In Sezione 27.3, «Comandi Linux importanti» (p. 429), si trova una lista dei comandi più importanti e una breve descrizione delle loro funzioni.

27.2 Utenti e autorizzazioni di accesso

Sin dall'inizio nei primi anni novanta, Linux è stato sviluppato come un sistema multi-utente. Un numero qualsiasi di utenti può utilizzarlo contemporaneamente. Gli utenti devono eseguire il login al sistema prima di avviare una sessione nella propria workstation. Ogni utente dispone di un nome utente e di una parola d'ordine corrispondente. Questa differenziazione di utenti garantisce che utenti non autorizzati non possano accedere ai file per i quali non dispongono dell'autorizzazione. Modifiche al sistema più rilevanti, ad esempio l'installazione dei nuovi programmi, non sono in genere possibili o limitate per normali utenti. Solo l'utente radice o il *superutente* ha la

capacità senza restrizioni di apportare modifiche al sistema e dispone di un accesso illimitato a tutti i file. Coloro che utilizzano questo concetto in modo appropriato, eseguendo il login con l'accesso `root` completo quando necessario, possono ridurre il rischio di una perdita involontaria di dati. Poiché in normali circostanze solo root può cancellare file del sistema o formattare i dischi rigidi, la minaccia proveniente dall'*effetto del cavallo di Troia* o da un'immissione accidentale di comandi distruttivi può essere ridotta in modo significativo.

27.2.1 Autorizzazioni del file system

In genere, ogni file in un file system Linux appartiene a un utente e a un gruppo. Entrambi questi gruppi proprietari e tutti gli altri possono essere autorizzati a scrivere, leggere o eseguire questi file.

Un gruppo, in questo caso, può essere definito come un insieme di utenti collegati con determinati diritti collettivi. Ad esempio, denominare un gruppo che lavora su un determinato progetto `project3`. Ogni utente in un sistema Linux è un membro di almeno un gruppo proprietario, in genere `users`. In un sistema possono essere presenti tutti i gruppi necessari, ma solo `root` è in grado di aggiungere gruppi. Ogni utente può individuare, con il comando `groups`, di quali gruppi è membro.

Accesso ai file

L'organizzazione delle autorizzazioni nel file system differisce per file e directory. Le informazioni sulle autorizzazioni dei file possono essere visualizzate con il comando `ls -l`. L'output potrebbe presentare il formato mostrato in Esempio 27.1, «Output di esempio con le autorizzazioni dei file» (p. 423).

Esempio 27.1 *Output di esempio con le autorizzazioni dei file*

```
-rw-r----- 1 tux project3 14197 Jun 21  15:03 Roadmap
```

Come mostrato nella terza colonna, il file appartiene all'utente `tux`. È assegnato al gruppo `project3`. Per individuare le autorizzazioni utente del file `Roadmap`, la prima colonna deve essere esaminata molto attentamente.

-	rw-	r--	---

Tipo	Autorizzazioni degli utenti	Autorizzazioni del gruppo	Autorizzazioni per altri utenti

Questa colonna è composta da un carattere iniziale seguito da nove caratteri suddivisi in tre gruppi. La prima delle dieci lettere indica il tipo di componente del file system. Il trattino (`-`) indica che si tratta di un file. Possono essere indicate anche una directory (`d`), un collegamento (`l`), un dispositivo a blocchi (`b`) o un dispositivo a caratteri.

I tre blocchi successivi seguono uno schema standard. I primi tre caratteri indicano se il file è leggibile (`r`) o meno (`-`). Il carattere `w` nella parte centrale indica che l'oggetto corrispondente può essere modificato, mentre un trattino (`-`) indica che non è possibile scrivere sul file. Il carattere `x` in terza posizione indica che l'oggetto può essere eseguito. Poiché il file in questo esempio è un file di testo e non è quindi eseguibile, l'accesso eseguibile per questo determinato file non è necessario.

In questo esempio, `tux` dispone, come proprietario del file `Roadmap`, dell'accesso in lettura (`r`) e scrittura (`w`), ma non può eseguirlo (`x`). I membri del gruppo `project3` possono leggere il file, ma non possono modificarlo o eseguirlo. Altri utenti non dispongono di alcun accesso a questo file. Altre autorizzazioni possono essere assegnate mediante gli elenchi di controllo dell'accesso (ACL, Access Control Lists). Per ulteriori informazioni, vedere la Sezione 27.2.6, «Elenchi di controllo dell'accesso» (p. 428).

Autorizzazioni delle directory

Le autorizzazioni di accesso per le directory sono indicate dal carattere `d`. Per le directory, le singole autorizzazioni hanno un significato leggermente differente.

Esempio 27.2 *Output di esempio con le autorizzazioni delle directory*

```
drwxrwxr-x 1 tux project3 35 Jun 21 15:15  ProjectData
```

In Esempio 27.2, «Output di esempio con le autorizzazioni delle directory» (p. 424), il proprietario (`tux`) e il gruppo proprietario (`project3`) della directory `ProjectData` sono facili da riconoscere. In contrasto con le autorizzazioni di accesso ai file da Accesso ai file (p. 423), l'autorizzazione di lettura impostata (`r`) indica che è possibile mostrare il contenuto della directory. L'autorizzazione di scrittura (`w`) indica che è possibile creare nuovi file. L'autorizzazione eseguibile (x) indica che l'utente può passare questa directory. Nell'esempio precedente, l'utente

`tux` nonché i membri del gruppo `project3` possono passare alla directory `ProjectData` (`x`), visualizzare il contenuto (`r`) e aggiungervi o cancellare nuovi file (`w`). Al resto degli utenti invece viene concesso un accesso limitato. Possono immettere la directory (`x`) e accedere ad essa (`r`), ma non inserire alcun nuovo file (`w`).

27.2.2 Modifica delle autorizzazioni dei file

Modifica delle autorizzazioni di accesso

Le autorizzazioni di accesso di un file o di una directory possono essere modificate dal proprietario e da `root` con il comando `chmod` seguito dai parametri per la modifica delle autorizzazioni e uno o più nomi file. I parametri costituiscono differenti categorie:

1. utenti interessati

- `u` (*user*, utente) - proprietario del file
- `g` (*group*, gruppo) - gruppo proprietario del file
- `o` (*others*, altri) - altri utenti (se non viene specificato alcun parametro, le modifiche vengono applicate a tutte le categorie)

2. un carattere per la cancellazione (–), l'impostazione (=) o l'inserimento (+)
3. abbreviazioni

- `r` - *read*
- `w` - *write*
- `x` - *execute*

4. nomefile o nomifile separati da spazi

Se ad esempio l'utente `tux` in Esempio 27.2, «Output di esempio con le autorizzazioni delle directory» (p. 424) desidera concedere anche ad altri utenti l'accesso in scrittura (`w`) alla directory `ProjectData`, può effettuare questa operazione utilizzando il comando `chmod o+w ProjectData`.

Se tuttavia desidera negare le autorizzazioni di scrittura a tutti gli altri utenti, può effettuare questa operazione immettendo il comando `chmod go-w ProjectData`. Per impedire a tutti gli utenti di aggiungere un nuovo file alla cartella `ProjectData`, immettere `chmod -w ProjectData`. In questo modo, anche al proprietario verrà negata la scrittura sul file. Tale operazione sarà possibile solo dopo aver ripristinato le autorizzazioni di scrittura.

Modifica delle autorizzazioni di proprietà

Altri importanti comandi per il controllo della proprietà e delle autorizzazioni dei componenti del file system sono `chown` (change owner, proprietario della modifica) e `chgrp` (change group, gruppo della modifica). Il comando `chown` può essere utilizzato per trasferire la proprietà di un file a un altro utente. Tuttavia, solo a `root` è permesso eseguire questa modifica.

Si supponga che il file `Roadmap` di Esempio 27.2, «Output di esempio con le autorizzazioni delle directory» (p. 424) non appartenga più a `tux`, ma all'utente `geeko`. `root` deve quindi immettere `chown geeko Roadmap`.

`chgrp` modifica la proprietà del gruppo relativa al file. Tuttavia, il proprietario deve essere un membro del nuovo gruppo. In questo modo, l'utente `tux` da Esempio 27.1, «Output di esempio con le autorizzazioni dei file» (p. 423) può modificare il gruppo proprietario del file `ProjectData` passando a `project4` con il comando `chgrp project4 ProjectData`, finché è membro di questo nuovo gruppo.

27.2.3 Bit setuid

In determinate situazioni, le autorizzazioni di accesso possono essere troppo restrittive. Quindi, in Linux sono disponibili impostazioni aggiuntive che consentono di eseguire una modifica temporanea dell'identità del gruppo e dell'utente attuale per una specifica azione. Ad esempio, il programma `passwd` in genere richiede autorizzazioni root per l'accesso a `/etc/passwd`. Questo file contiene alcune informazioni importanti, ad esempio le home directory degli utenti, ID utente e di gruppo. Quindi, un normale utente non è in grado di modificare `passwd`, poiché risulta troppo pericoloso concedere a tutti gli utenti accesso diretto a questo file. Una possibile soluzione a questo problema è il meccanismo *setuid*. setuid, (set user ID, ID utente impostato) è un particolare attributo di file che indica al sistema di eseguire programmi contrassegnati da un ID utente specifico. Considerare il comando `passwd`:

```
-rwsr-xr-x  1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

Si noti che la `s` indica che il bit setuid è impostato per l'autorizzazione utente. Mediante il bit setuid, tutti gli utenti che avviano il comando `passwd` lo eseguono come `root`.

27.2.4 Bit setgid

Il bit setuid viene applicato a tutti gli utenti. Tuttavia, esiste anche una caratteristica equivalente per i gruppi: il bit *setgid*. Un programma per cui è stato impostato questo bit viene eseguito con l'ID gruppo con cui è stato salvato, indipendentemente dall'utente che lo avvia. Quindi, in una directory con il bit setgid, tutte le sottodirectory e i file nuovi vengono assegnati al gruppo a cui la directory appartiene. Considerare la seguente directory di esempio:

```
drwxrws--- 2 tux archive 48 Nov 19 17:12
   backup
```

Si noti che la `s` indica che il bit setgid è impostato per l'autorizzazione del gruppo. Il proprietario della directory e i membri del gruppo `archive` possono accedere a questa directory. Gli utenti che non sono membri di questo gruppo sono «mappati» sul gruppo rispettivo. Il gruppo ID effettivo di tutti i file scritti sarà `archive`. Ad esempio, un programma di backup che viene eseguito con l'ID di gruppo `archive` è in grado di accedere a questa directory anche senza privilegi dell'utente root.

27.2.5 Bit sticky

È disponibile anche il *bit sticky*. Esiste una differenza che dipende dall'appartenenza a una directory o a un programma eseguibile. Se tale bit appartiene a un programma, un file così contrassegnato viene caricato nella RAM per evitare di doverlo recuperare dal disco rigido ogni volta che viene utilizzato. Questo attributo viene utilizzato raramente, poiché i dischi rigidi moderni sono abbastanza rapidi. Se questo attributo viene assegnato a una directory, impedisce agli utenti di cancellare i file tra di loro. I tipici esempi includono le directory `/tmp` e `/var/tmp`:

```
drwxrwxrwt   2 root  root   1160 2002-11-19 17:15 /tmp
```

27.2.6 Elenchi di controllo dell'accesso

Il concetto di autorizzazioni tradizionale per gli oggetti del file system Linux, ad esempio file o directory, può essere completato includendo gli elenchi di controllo dell'accesso (ACL, Access Control Lists). Consentono di assegnare le autorizzazioni a singoli utenti o gruppi diversi dal proprietario o dal gruppo proprietario originale di un oggetto del file system.

I file o le directory con autorizzazioni di accesso estese possono essere rilevate con il semplice comando `ls -l`:

```
-rw-r--r--+ 1 tux project3 14197 Jun 21  15:03 Roadmap
```

`Roadmap` è di proprietà di `tux` che appartiene al gruppo `project3`. `tux` dispone dell'accesso in lettura e scrittura a questo file. Il gruppo nonché tutti gli altri utenti dispongono dell'accesso in lettura. L'unica differenza che distingue questo file da uno senza un ACL è il segno + aggiuntivo nella prima colonna contenente i bit delle autorizzazioni.

Per dettagli sull'ACL, eseguire `getfacl Roadmap`:

```
# file: Roadmap
# owner: tux
# group: project3
user::rw-
user:jane:rw-       effective: r--
group::r--
group:djungle:rw-   effective: r--
mask::r--
other::---
```

Le prime righe dell'output contengono informazioni disponibili con `ls -l`. Queste righe indicano solo il nome file, il proprietario e il gruppo proprietario. Le righe 4-9 contengono gli elementi ACL. Le autorizzazioni di accesso convenzionali rappresentano un sottoinsieme di quelle possibili quando si utilizzano gli ACL. Nell'ACL di esempio viene concesso l'accesso in lettura e scrittura al proprietario del file nonché all'utente `gianni` (righe 4-5). Il concetto convenzionale è stato ampliato concedendo l'accesso a un altro utente. Le stesse indicazioni vengono applicate alla gestione dell'accesso del gruppo. Il gruppo proprietario dispone delle autorizzazioni di lettura (riga 6) e il gruppo `alfa` dispone delle autorizzazioni di lettura e scrittura. La voce `mask` nella riga 8 riduce le autorizzazioni effettive per l'utente `gianni` e il gruppo `alfa` all'accesso in lettura. Altri utenti e gruppi non ottengono alcun tipo di accesso al file (riga 9).

Finora sono state fornite solo informazioni di base. Per ulteriori informazioni sulle ACL, vedere il Capitolo 24, *Elenchi di controllo dell'accesso in Linux* (p. 373).

27.3 Comandi Linux importanti

In questa sezione sono riportati i comandi più importanti del sistema SUSE Linux. In questo capitolo sono elencati molti altri comandi. Insieme ai singoli comandi, sono elencati i parametri e, nel caso, viene presentata un'applicazione di esempio. Per ulteriori informazioni sui vari comandi, utilizzare le pagine man alle quali è possibile accedere con`man` seguito dal nome del comando, ad esempio, `man ls`.

All'interno delle pagine man, spostarsi verso l'alto e verso il basso con Pag su e Pag giù. Spostarsi tra l'inizio e la fine del documento con i tasti Home e Fine. Terminare questa modalità di visualizzazione premendo Q. È possibile ottenere ulteriori informazioni sul comando `man`con`man man`.

Nella panoramica riportata qui di seguito, gli elementi dei singoli comandi sono scritti con caratteri diversi. Il comando effettivo e le sue opzioni obbligatorie sono sempre stampati come`command option`. Le specifiche o i parametri che non sono necessari sono racchiusi tra `[parentesi quadre]`.

Adattare le impostazioni in base alle proprie esigenze. Non ha senso scrivere`ls file`, se non esiste effettivamente nessun file chiamato`file`. Generalmente è possibile combinare vari parametri, ad esempio, scrivendo `ls -la` anzichè `ls -l -a`.

27.3.1 Comandi per i file

Nella sezione riportata qui di seguito, sono elencati i comandi più importanti per la gestione dei file. Nella sezione viene trattato qualsiasi argomento, dall'amministrazione generale dei flie alla manipolazione di ACL di file system.

Amministrazione dei file

`ls [options] [files]`

Se si esegue `ls` senza nessun parametro aggiuntivo, il programma riporta un elenco dei contenuti della directory corrente in forma abbreviata.

-l
Lista dettagliata

-a
Visualizza i file nascosti

cp [options] source target

Copia `source` in `target`.

-i
Attende una conferma, se necessario, prima che venga sovrascritto un `target` esistente

-r
Copia in modo ricorsivo (include le sottodirectory)

mv [options] source target

Copia `source` in `target` poi cancella il file`source` originale.

-b
Crea una copia di backup del `source` prima di spostarlo

-i
Attende una conferma, se necessario, prima che venga sovrascritto un `targetfile` esistente

ls [options] [files]

Rimuove i file indicati dal file system. Le directory non vengono rimosse dal comando `rm` a meno che non venga utilizzata l'opzione `-r`.

-r
Cancella qualsiasi sottodirectory esistente

-i
Attende conferma prima di cancellare file.

ln [options] source target

Crea un collegamento da`source` a `target`. Normalmente, questo link punta direttamente a `source` sullo stesso file system. In ogni caso, se `ln` viene eseguito con l'opzione `-s`, crea un link simbolico che punta solo alla directory nella quale è posizionato `source`, abilitando il collegamento tramite file system.

-s
Crea un link simbolico

cd [options] [directory]

Modifica la directory corrente. `cd` senza parametri modifica la home directory dell'utente.

mkdir [options] directory

Crea una nuova directory.

rmdir [options] directory

Cancella la directory indicata se è già vuota.

chown [options] username[:[group]] files

Trasferisce la proprietà di un file all'utente con il nome utente indicato.

-R
Modifica i file e le directory in tutte le sottodirectory

chgrp [options] groupname files

Trasferisce la proprietà del gruppo di un dato `file` al gruppo con il nome gruppo indicato. Il proprietario del file può solo modificare la proprietà del gruppo se è membro sia del gruppo corrente, sia di quello nuovo.

chmod [options] mode files

Modifica i permessi di accesso.

Il parametro `mode` ha tre parti: `group`, `access` e `access type`. `group` accetta i seguenti caratteri:

u
user

g
group

o
others

Per `access`, grant access with + and deny it with −.

Il `tipo di accesso` è controllato dalle seguenti opzioni:

r
read

w
write

x
execute—esecuzione dei file o modifica alla directory

s
Setuid bit—l'applicazione o il programma viene avviato come se fosse avviato dal proprietario del file

Come alternativa, è possibile utilizzare un codice numerico. Le quattro cifre di questo codice sono composte dalla somma dei valori 4, 2 e 1—il risultato decimale di una maschera binaria. La prima cifra imposta la ID dell'utente impostato (SUID) (4), il gruppo impostato (2) e i bit permanenti (1). La seconda cifra definisce i permessi del proprietario del file. La terza cifra definisce i permessi dei membri del gruppo e l'ultima imposta i permessi per tutti gli altri utenti. Il permesso di lettura è impostato con 4, il permesso di scrittura con 2 e quello per l'esecuzione di un file è impostato con 1. Il proprietario di un file dovrebbe generalmente ricevere un 6 o un 7 per i file eseguibili.

`gzip [parameters] files`

Questo programma comprime i contenuti dei file utilizzando algoritmi matematici complessi. I file compressi in questo modo hanno estensione `.gz`e devono essere

decompressi prima di essere utilizzati. Per comprimere vari file o intere directory, utilizzare il comando `tar`.

-d
Decomprime i file gzip compressi in modo tale che tornino al formato originale e possano essere elaborati normalmente (come il comando `gunzip`)

`tar options archive files`

`tar` inserisce uno o più file in un archivio. La compressione è facoltativa. `tar` è un comando abbastanza complesso con molte opzioni disponibili. Le opzioni utilizzate con maggiore frequenza sono:

-f
Scrive l'output a un file e non sullo schermo come avviene di solito

-c
Crea un nuovo archivio tar

-r
Aggiunge file a un archivio esistente

-t
Emette i contenuti di un archivio

-u
Aggiunge file, ma solo se sono più recenti rispetto a quelli già contenuti nell'archivio

-x
Decomprime i file da un archivio (*estrazione*)

-z
Comprime l'archivio che ne risulta con `gzip`

-j
Comprime l'archivio che ne risulta con `bzip2`

-v
Elenca i file elaborati

I file di archivio creati da `tar` finiscono con `.tar`. Se l'archivio tar fosse stato solo compresso con `gzip`, la fine sarebbe `.tgz` o `.tar.gz`. Se fosse stato compresso con `bzip2`, la fine sarebbe `.tar.bz2`. Alcuni esempi di applicazione sono reperibili in Sezione 27.1.8, «Archivi e compressione dei dati» (p. 420).

`locate patterns`

Questo comando è disponibile solo se è stato installato il pacchetto `findutils-locate`. Il comando `locate` è in grado di reperire in quale directory si trova un dato file. Se si vuole, è possibile utilizzare i caratteri jolly per indicare i nomi dei file. Il programma è molto veloce perchè utilizza un database appositamente creato per questo scopo (anzichè cercare nell'intero file system). Questo presenta anche un inconveniente: locate non è in grado di trovare i file creati dopo l'ultimo aggiornamento del suo database. Il database può essere generato da `root` con `updatedb`.

`updatedb [options]`

Questo comando esegue un aggiornamento del database utilizzato da `locate`. Per includere file in tutte le directory, eseguire il programma come `root`. È anche possibile metterlo in background aggiungendovi un simbolo (`&`), in modo tale da essere subito in grado di lavorare sulla stessa riga di comando (`updatedb &`). Questo comando, di solito, esegue un processo cron quotidiano (vedere `cron .daily`).

`find [options]`

Con `find`, è possibile cercare un file in una data directory. Il primo argomento indica la directory nella quale avviare la ricerca. L'opzione `-name` deve essere seguita da una stringa di ricerca, che può anche comprendere caratteri jolly. Al contrario, `locate`, che utilizza un database, `find` effettua la scansione della directory corrente.

Comandi per accedere ai contenuti di un file

`cat [options] files`

Il comando `cat` visualizza i contenuti di un file, stampando sullo schermo tutto il contenuto senza interruzione.

-n
Numera l'output sul margine sinistro

less [options] files

Questo comando può essere utilizzato per sfogliare i contenuti del file indicato. Scorrere fino a raggiungere metà schermo verso l'alto o verso il basso con Pag su e Pag giù o l'intera schermata con lo Spazio. Andare all'inizio o alla fine di un file con Home e Fine. Premere Q per uscire dal programma.

grep [options] searchstring files

Il comando grep trova una stringa di ricerca particolare nei file indicati. Se la stringa di ricerca viene trovata, il comando visualizza la riga nella quale la `searchstring` è stata trovata insieme al nome del file.

-i
Ignora maiuscole e minuscole

-H
Visualizza solo i nomi dei rispettivi file, ma non le righe di testo

-n
Visualizza inoltre i numeri delle righe nelle quali ha trovato un risultato

-l
Elenca solo i file nei quali la`searchstring` non è presente

diff [options] file1 file2

Il comando `diff` confronta i contenuti di due file su uno. L'output prodotto dal programma elenca tutte le righe che non corrispondono. Questo comando è frequentemente utilizzato dai programmatori che devono inviare le modifiche dei programmi e non tutto il codice sorgente.

-q
Riporta solo se due file sono diversi

-u
Produce una«unified» diff, cche rende l'output più leggibile

File system

`mount [options] [device] mountpoint`

Questo comando può essere utilizzato per l'attivazione di supporti dati, come dischi rigidi, unità CD-ROM e altre unità in una directory del file system Linux.

`-r`
mount read-only

`-t filesystem`
Indica il file system, di solito `ext2`, per i dischi rigidi Linux, `msdos` per i supporti MS-DOS, `vfat` per il file system Windows e `iso9660` per i CD

Per i dischi rigidi non definiti nel file `/etc/fstab`, si deve indicare anche il tipo di dispositivo. In questo caso solo l'utente `root` può effettuare l'attivazione. Se il file system deve essere anche attivato da altri utenti, immettere l'opzione `user` nella giusta riga nel file `/etc/fstab` (separata da virgole) e salvare questa modifica. Ulteriori informazioni sono disponibili alla pagina man `mount(1)`.

`umount [options] mountpoint`

Questo comando disattiva un drive attivato dal file system. Per evitare perdite di dati, eseguire questo comando prima di rimuovere un supporto dati dalla sua unità. Di solito, solo l'utente `root` è autorizzato a eseguire i comandi `mount` e `umount`. Per abilitare altri utenti all'esecuzione di questi comandi, modificare il file `/etc/fstab` in modo tale da indicare l'opzione`user`per la rispettiva unità.

27.3.2 Comandi di sistema

La sezione riportata qui di seguito elenca alcuni dei più importanti comandi necessari a reperire le informazioni relative al sistema, al controllo dei processi e della rete.

Informazioni sul sistema

`df [options] [directory]`

Il comando `df` (disk free), quando utilizzato senza opzioni, visualizza le informazioni relative allo spazio totale su disco, allo spazio su disco attualmente in uso e allo

spazio libero presente su tutte le unità attivate. Se viene indicata una directory, le informazioni sono limitate all'unità sulla quale è posizionata quella directory.

-h
Mostra il numero di blocchi occupati in gigabyte, megabyte o kilobyte—in formato leggibile

-T
Tipo di file system (ext2, nfs e così via.)

du [options] [path]

Questo comando, quando eseguito senza alcun parametro, mostra lo spazio totale su disco occupato dai file e dalle sottodirectory nella directory corrente.

-a
Visualizza la dimensione di ogni singolo file

-h
Output in formato leggibile

-s
Visualizza solo la dimensione totale calcolata

free [options]

Il comando `free` consente di visualizzare informazioni sulla RAM e l'utilizzo dello spazio di scambio, mostrando la quantità totale e quella utilizzata in entrambe le categorie. Vedere la Sezione 30.1.6, «Il comando free» (p. 492)per ulteriori informazioni.

-b
Output in byte

-k
Output in kilobyte

-m
Output in megabyte

`date [options]`

Questo semplice programma consente di visualizzare l'ora corrente del sistema. Se viene eseguito come `root`, questo programma può anche essere utilizzato per modificare l'ora del sistema. Ulteriori informazioni sul programma sono disponibili alla pagina man date(1).

Processi

`top [options]`

`top` consente di ottenere una panoramica rapida dei processi attualmente in esecuzione. Premere H per accedere a una pagina nella quale sono spiegate brevemente le opzioni principali per la personalizzazione del programma.

`ps [options] [process ID]`

Se eseguito senza opzioni, questo comando consente di visualizzare una tabella di tutti i programmi o i processi—avviati. Le opzioni per questo comando non sono precedute dal trattino.

aux

Consente di visualizzare un elenco dettagliato di tutti i processi, senza tener conto del proprietario

`kill [options] process ID`

Purtroppo, a volte, non è possibile terminare normalmente un programma. Nella maggior parte dei casi, dovrebbe essere ancora possibile fermare il programma eseguendo il comando `kill`, indicando la rispettiva ID del processo (vedere `top` e `ps`). `kill` consente di inviare un segnale *TERM* che invia un'istruzione di chiusura al programma. Se questo non è di aiuto, è possibile utilizzare il seguente parametro:

-9

Invia un segnale *KILL* anzichè un segnale*TERM* che consente di terminare il programma in quasi tutti i casi

`killall [options] processname`

Questo comando è simile a `kill`, ma utilizza come argomento il nome di processo (anzichè l'ID), terminando tutti i processi con quel nome.

Rete

`ping [options] hostname or IP address`

Il comando `ping` è lo strumento standard per provare la funzionalità principale delle reti TCP/IP. Tramite questo comando viene inviato un piccolo pacchetto di dati all'host di destinazione con la richiesta di una risposta immediata. Se `ping` funziona, viene visualizzato un messaggio, a indicare che il collegamento di rete è in linea di massima funzionante.

`-c` *`number`*
Consente di definire il numero complessivo di pacchetti da inviare e terminare dopo la distribuzione (come impostazione predefinita, non è impostato alcun limite)

`-f`
flood ping: consente di inviare il maggior numero di pacchetti dati possibile; un mezzo comune, riservato agli utenti `root`, per provare le reti

`-i` *`value`*
Consente di indicare l'intervallo tra due pacchetti di dati in secondi (predefinito: un secondo)

`nslookup`

Il sistema del nome di dominio risolve i nomi di dominio agli indirizzi IP. Con questo strumento, è possibile inviare interrogazioni ai server dei nomi (server DNS).

`telnet [options] hostname or IP address [port]`
Telnet è un protocollo Internet che consente di lavorare su host remoti tramite una rete. telnet è anche il nome di un programma Linux che utilizza questo protocollo per abilitare le operazioni sui computer remoti.

AVVERTIMENTO

Non utilizzare telnet su una rete dove è possibile l' «intercettazione» da parte di terzi. In particolare su Internet, utilizzare metodi di trasferimento cifrati come `ssh`, per evitare il rischio di un uso scorretto doloso di una parola d'ordine (vedere la pagina man di `ssh`).

Varie

`passwd [options] [username]`

Questo comando consente agli utenti di modificare la loro parola d'ordine in qualsiasi momento. L'amministratore `root` può utilizzare questo comando per modificare la parola d'ordine di qualsiasi utente sul sistema.

`su [options] [username]`

Il comando `su` cosente di eseguire il log in con un nome utente diverso da una sessione in esecuzione. Specificare un nome utente e la parola d'ordine corrispondente. All'utente `root` non è richiesta la parola d'ordine, perchè l'utente `root` è autorizzato ad assumere l'identità di qualsiasi utente. Quando si utilizza il comando senza specificare un nome utente, si è invitati a immettere la parola d'ordine dell'utente `root` e a passare a superutente (`root`).

`-`

Utilizzare il comando `su -` per avviare una shell di login per l'utente diverso.

`halt [options]`

Per evitare perdite di dati, si dovrebbe sempre utilizzare questo programma per spegnere il sistema.

`reboot [options]`

Come il comando `halt` con l'unica eccezione che consente di riavviare immediatamente il sistema.

`cancella`

Questo comando consente di ripulire l'area visibile della console. Non ha opzioni.

27.3.3 Per ulteriori informazioni

In questo capitolo sono elencati molti altri comandi. Per informazioni relative agli altri comandi o ulteriori dettagli, si consigli il testo di O'Reilly *Linux guida di riferimento*.

27.4 L'editor vi

Gli editori di testo sono ancora utilizzati per più task di amministrazione del sistema nonché per la programmazione. In ambiente Unix, vi è un editor in grado di offrire pratiche funzioni di editing e risulta più ergonomico di molti editor che utilizzano il mouse.

27.4.1 Modalità operative

In genere, vi utilizza tre modalità operative: *modalità* di inserimento, *modalità* di comando e *modalità* estesa. I tasti hanno funzioni diverse a seconda della modalità. All'avvio, vi è impostato in genere sulla *modalità di* comando. È necessario conoscere innanzitutto come passare da una modalità all'altra:

Dalla modalità di commando alla modalità di inserimento
Esistono diverse possibilità, tra cui A per l'aggiunta, I per l'inserimento oppure O per una nuova riga sotto la riga corrente.

Dalla modalità di inserimento alla modalità di comando
Premere Esc per uscire dalla modalità di *inserimento*. Non è possibile chiudere vi nella modalità di *inserimento*, perciò è importante utilizzare il tasto Esc.

Dalla modalità di commando alla modalità estesa
Per attivare la modalità *estesa* di vi, immettere due punti (:). La modalità *estesa* o *es* è simile a un editor indipendente basato sulle righe che si può utilizzare per vari task semplici e più complessi.

Dalla modalità estesa alla modalità di commando
Dopo aver eseguito un comando nella modalità *estesa*, l'editor torna automaticamente alla modalità di *comando*. Nel caso si decida di non eseguire un qualsiasi commando nella modalità *estesa*, cancellare i due punti con . L'editor torna alla modalità di *comando*.

Non è possibile passare direttamente dalla modalità di *inserimento* alla modalità *estesa* senza prima passare alla modalità di *comando*.

Come gli altri editor, vi termina il programma secondo una procedura propria. Non è possibile terminare vi quando si trova in modalità di *inserimento*. Innanzitutto, per uscire dalla modalità di *inserimento*, premere Esc. Quindi, sono disponibili due opzioni:

1. *Exit without saving (Uscire senza salvare):* per terminare l'editor senza salvare le modifiche, digitare [:] – [Q] – [!] nella modalità di *comando*. Il punto esclamativo (!) consente di ignorare qualsiasi modifica.

2. *Save and exit (Salvare e uscire):* Sono disponibili diverse possibilità per salvare le modifiche e chiudere l'editor. Nella modalità di *comando*, utilizzare [Shift] + [Z] + [Z]. Per uscire dal programma e salvare tutte le modifiche utilizzando la modalità *estesa*, digitare [:] – [W] – [Q]. Nella modalità *estesa*, `w` indica la scrittura mentre `q` indica l'uscita.

27.4.2 Funzionamento di vi

vi può essere utilizzato come un normale editor. Nella modalità di *inserimento*, per immettere il testo e cancellarlo utilizzare i tasti [ ] e [Canc]. Utilizzare i tasti freccia per spostare il cursore.

Questi tasti di controllo, tuttavia, spesso causano dei problemi poiché esistono diversi tipi di terminali che utilizzano codici di tasti speciali. A questo punto viene utilizzata la modalità di *comando*. Premere [Esc] per passare dalla modalità di *inserimento* alla modalità di *comando*. Nella modalità di *comando*, spostare il cursore con [H], [J], [K], e [L]. Questi tasti includono le seguenti funzioni:

[H]
Sposta un carattere a sinistra.

[J]
Sposta una riga in basso.

[K]
Sposta una riga in alto.

[L]
Sposta un carattere a destra.

I comandi nella modalità di *comando* consentono diverse variazioni. Per eseguire un comando diverse volte, è sufficiente immettere il numero di ripetizioni prima del comando stesso. Ad esempio, immettere [5] [L] per spostare il cursore di cinque caratteri a destra.

Nell'elenco Tabella 27.1, «Comandi semplici dell'editor vi» (p. 443), non ancora completo, viene mostrata una selezione di comandi importanti. Per elenchi più completi, consultare la documentazione in Sezione 27.4.3, «Ulteriori informazioni» (p. 444)

Tabella 27.1 *Comandi semplici dell'editor vi*

Esc	Change to command mode (Passa alla modalità di comando)
I	Passa alla modalità di inserimento (i caratteri vengono visualizzati nella posizione del cursore attuale).
A	Passa alla modalità di inserimento (i caratteri vengono inseriti dopo la posizione del cursore attuale).
Shift + A	Passa alla modalità di inserimento (i caratteri vengono aggiunti alla fine della riga).
Shift + R	Passa alla modalità di sostituzione (sovrascrive il testo precedente).
R	Sostituisce il carattere sotto il cursore.
O	Passa alla modalità di inserimento (una nuova riga viene inserita dopo quella attuale).
Shift + O	Passa alla modalità di inserimento (una nuova riga viene inserita prima di quella attuale).
X	Cancella il carattere attuale.
D – D	Cancella la riga attuale.
D – W	Cancella fino alla fine della parola attuale.
C – W	Passa alla modalità di inserimento (il resto della parola attuale viene sovrascritto dalle voci successive digitate).
U	Annulla l'ultimo comando.
Ctrl + R	Ripete la modifica annullata.

Shift + J	Unisce la riga seguente con quella attuale.
.	Ripete l'ultimo comando.

27.4.3 Ulteriori informazioni

vi supporta un'ampia serie di comandi. Consente l'utilizzo di macro, scorciatoie, buffer denominati e molte altre utili funzioni. Una descrizione più dettagliata delle varie opzioni non rientra nello scopo del presente manuale. Con SUSE Linux è fornito vim (vi improved), una versione migliorata di vi. Per questa applicazione sono disponibili diverse fonti di informazioni:

- vimtutor è il supporto interattivo di vim.
- In vim, digitare il comando `:help` per ricevere assistenza su diversi argomenti.
- È disponibile un manuale su vim in linea all'indirizzo http://www.truth.sk/vim/vimbook-OPL.pdf.
- Le pagine Web del progetto vim reperibili all'indirizzo http://www.vim.org forniscono tutti i tipi di informazioni, elenchi di distribuzione e altra documentazione.
- Altra documentazione su vim è disponibile su Internet all'indirizzo: http://www.selflinux.org/selflinux/html/vim.html, http://www.linuxgazette.com/node/view/9039, e http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html. Per ulteriori collegamenti sui tutorial, consultare l'indirizzo http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html.

IMPORTANTE: Licenza di VIM

vim è un «charityware,» ossia gli autori non vengono retribuiti per il software ma promuovono il supporto di un progetto senza fini di lucro con un contributo in denaro. Questo progetto chiede aiuto per i bambini poveri dell'Uganda. Per ulteriori informazioni, visitare il sito http://iccf-holland.org/index.html, http://www.vim.org/iccf/ e http://www.iccf.nl/.

Avvio e configurazione di un sistema Linux

28

L'avvio di un sistema Linux coinvolge svariati componenti. In questo capitolo vengono illustrati i principi di base e vengono evidenziati i componenti coinvolti. Vengono inoltre descritti il concetto di runlevel e la configurazione del sistema SUSE tramite `sysconfig`.

28.1 Processo di avvio di Linux

Il processo di avvio di Linux comprende varie fasi ognuna delle quali è rappresentata da un componente diverso. Di seguito viene brevemente riepilogato il processo di avvio e vengono indicati i principali componenti coinvolti.

1. **BIOS** Quando il computer viene accesso, il BIOS inizializza lo schermo e la tastiera e controlla la memoria principale. Durante questa prima fase il computer non accede a supporti di memorizzazione di massa. Dopo di che, vengono caricate dai valori CMOS le informazioni riguardanti la data e l'ora correnti nonché le periferiche più importanti. Quando vengono riconosciuti il primo disco rigido e la relativa geometria, il controllo del sistema passa dal BIOS al boot loader.

2. **Boot loader** Il primo settore di dati fisico da 512 byte del primo disco rigido viene caricato nella memoria principale e il controllo viene assunto dal *boot loader* che risiede all'inizio di questo settore. La parte restante del processo di avvio dipende dai comandi eseguiti dal boot loader. Di conseguenza, i primi 512 byte nel primo disco rigido vengono denominati *MBR (Master Boot Record)*. Il boot loader passa quindi il controllo al sistema operativo effettivo, in questo

caso il kernel Linux. Per ulteriori informazioni su GRUB, il boot loader di Linux, vedere il Capitolo 29, *Boot Loader* (p. 463).

3. **Kernel e initramfs** Per passare il controllo del sistema, il boot loader carica in memoria sia il kernel che un file system iniziale basato sulla RAM (initramfs). Il contenuto del file system initramfs può essere utilizzato direttamente dal kernel. Il file system initramfs contiene un piccolo file eseguibile, denominato init, che gestisce il montaggio del file system radice effettivo. Nelle versioni precedenti di SUSE Linux questi task erano gestiti rispettivamente da initrd e linuxrc. Per ulteriori informazioni su initramfs, fare riferimento alla Sezione 28.1.1, «File system initramfs» (p. 446).

4. **Esecuzione di init su initramfs** Questo programma esegue tutte le operazioni necessarie per montare il file system radice appropriato, ad esempio fornisce le funzionalità del kernel per il file system necessario e i driver di periferica per i controller della memorizzazione di massa. Dopo che il file system radice è stato rilevato, viene sottoposto a un controllo degli errori e quindi viene montato. Se queste operazioni hanno esito positivo, initramfs viene ripulito e quindi viene eseguito il programma init sul file system radice. Per ulteriori informazioni su init, fare riferimento alla Sezione 28.1.2, «Esecuzione di init su initramfs» (p. 447).

5. **Programma init** Il programma init gestisce l'effettivo avvio del sistema attraverso svariati livelli che forniscono funzionalità diverse. Per una descrizione di init, vedere la Sezione 28.2, «Processo di init» (p. 449).

28.1.1 File system initramfs

initramfs è un file system di piccole dimensioni che il kernel può caricare in un disco RAM. Fornisce un ambiente Linux minimo che consente di eseguire programmi prima che venga montato il file system radice effettivo. Questo ambiente Linux minimo viene caricato in memoria dalle routine del BIOS e non prevede requisiti hardware specifici a parte una quantità di memoria sufficiente. initramfs deve sempre fornire un file eseguibile denominato init per l'esecuzione del programma init effettivo sul file system radice affinché il processo di avvio possa proseguire.

Prima che il file system radice effettivo possa essere montato e il sistema operativo effettivo possa essere avviato, il kernel deve caricare i driver corrispondenti per accedere al dispositivo in cui si trova il file system radice. Questi driver possono includere driver speciali per determinati tipi di unità disco rigido o persino driver di rete per l'accesso

a un file system di rete. I moduli necessari per il file system radice possono essere caricati tramite l'esecuzione di init su initramfs. initramfs è disponibile durante l'intero processo di avvio. In questo modo è possibile gestire tutti gli eventi HotPlug generati durante l'avvio.

Se è necessario sostituire i componenti hardware (i dischi rigidi) in un sistema installato e il nuovo hardware richiede la presenza di driver diversi nel kernel in fase di avvio, occorre aggiornare initramfs. Questa operazione viene eseguita come per il predecessore di initramfs, initrd, tramite una chiamata di `mkinitrd`. Quando si chiama `mkinitrd` senza argomenti, viene creato un initramfs. Quando si chiama `mkinitrd -R` , viene creato un initrd. In SUSE Linux i moduli da caricare vengono specificati tramite la variabile `INITRD_MODULES` in `/etc/sysconfig/kernel`. Al termine dell'installazione, questa variabile viene impostata automaticamente sul valore corretto. I moduli vengono caricati nell'ordine esatto in cui appaiono in `INITRD_MODULES`. Questo aspetto assume particolare importanza quando vengono utilizzati più driver SCSI perché altrimenti i nomi dei dischi rigidi cambierebbero. Nonostante sarebbe sufficiente caricare solo i driver necessari per l'accesso al file system radice, vengono caricati tutti i driver SCSI necessari per l'installazione tramite initramfs o initrd perché un caricamento successivo potrebbe creare problemi.

IMPORTANTE: aggiornamento di initramfs o initrd

Il boot loader carica initramfs o initrd allo stesso modo del kernel. Dopo l'aggiornamento di initramfs o initrd, non è necessario reinstallare GRUB perché GRUB cerca il file corretto nella directory durante l'avvio.

28.1.2 Esecuzione di init su initramfs

Lo scopo principale dell'esecuzione di init su initramfs è preparare il montaggio del file system radice effettivo e consentire di accedervi. In base alla configurazione del sistema, init esegue i task elencati di seguito.

Caricamento di moduli del kernel
: In base alla configurazione hardware, potrebbero essere necessari driver particolari per accedere ai componenti hardware del computer, il più importante dei quali è il disco rigido. Per accedere al file system radice finale, il kernel deve caricare i driver del file system appropriati.

Gestione della configurazione di RAID e LVM

Se il sistema in uso è stato configurato in modo da utilizzare RAID o LVM per memorizzare il file system radice, init imposta LVM o RAID per consentire il successivo accesso al file system radice. Per informazioni su RAID, vedere la Sezione 2.3, «Configurazione di RAID software» (p. 70). Per informazioni su LVM, vedere la Sezione 2.2, «Configurazione dell'LVM» (p. 62).

Gestione della configurazione della rete

Se il sistema in uso è stato configurato in modo da utilizzare un file system radice montato in rete tramite NFS, init deve verificare che vengano caricati i driver di rete appropriati e che siano impostati in modo da consentire l'accesso al file system radice.

Quando init viene chiamato durante l'avvio iniziale nell'ambito del processo di installazione, i task eseguiti non sono gli stessi descritti in precedenza:

Individuazione del supporto di installazione

Quando si avvia il processo di installazione, il computer carica dal supporto di installazione un kernel di installazione e un initrd speciale con il programma di installazione YaST. Il programma di installazione YaST, che viene eseguito in un file system RAM, deve essere a conoscenza dell'effettiva posizione in cui si trova il supporto di installazione in modo da potervi accedere e installare il sistema operativo.

Inizializzazione del riconoscimento dell'hardware e caricamento dei moduli del kernel appropriati

Come specificato nella Sezione 28.1.1, «File system initramfs» (p. 446), il processo di avvio ha inizio con un set minimo di driver utilizzabili con la maggior parte delle configurazioni hardware. Il programma init avvia un processo iniziale di scansione dell'hardware che determina il set di driver adeguato per la configurazione hardware disponibile. Questi valori vengono quindi scritti nella variabile `INITRD_MODULES` in `/etc/sysconfig/kernel` per consentire a qualsiasi processo di avvio successivo di utilizzare un initrd personalizzato. Durante il processo di installazione, init carica questo set di moduli.

Caricamento del sistema di installazione o del sistema di salvataggio

Immediatamente dopo il riconoscimento dell'hardware e il caricamento dei driver appropriati, init avvia il sistema di installazione, che contiene il programma di installazione YaST effettivo, oppure il sistema di salvataggio.

Avvio di YaST
Infine, init avvia YaST, il quale a sua volta avvia l'installazione dei pacchetti e la configurazione del sistema.

28.2 Processo di init

Il programma init è il primo processo eseguito. Si occupa di inizializzare il sistema nel modo richiesto e svolge un ruolo speciale. Viene avviato direttamente dal kernel ed è in grado di sopravvivere al segnale 9, che in genere termina i processi. Tutti gli altri programmi vengono avviati direttamente da init oppure da uno dei relativi processi secondari.

init è configurato a livello centrale nel file `/etc/inittab`, dove vengono definiti i *runlevel* (vedere la Sezione 28.2.1, «Runlevel» (p. 449)). Questo file specifica inoltre i servizi e i daemon disponibili in ogni livello. In base alle voci presenti nel file `/etc/inittab`, init esegue svariati script. Per motivi di chiarezza, questi script, denominati *script di init*, risiedono tutti nella directory `/etc/init.d` (vedere la Sezione 28.2.2, «Script di init» (p. 452)).

L'intero processo di avvio e arresto del sistema è gestito da init. Sotto questo punto di vista, il kernel può essere considerato un processo in background il cui task è gestire tutti gli altri processi e regolare sia il tempo di CPU sia l'accesso all'hardware in base alle richieste di altri programmi.

28.2.1 Runlevel

In Linux i *runlevel* definiscono la modalità di avvio del sistema e i servizi disponibili nel sistema in esecuzione. Dopo il processo di avvio, il sistema viene avviato come definito all'interno del file `/etc/inittab` in corrispondenza della riga `initdefault`. In genere, questa impostazione è `3` o `5`. Vedere la Tabella 28.1, «Runlevel disponibili» (p. 450). In alternativa, il runlevel può essere specificato in fase di avvio, ad esempio nel prompt di avvio. Tutti i parametri non valutati direttamente dal kernel vengono passati a init.

Tabella 28.1 *Runlevel disponibili*

Runlevel	Descrizione
0	Arresto del sistema.
S	Modalità utente singolo. Dal prompt di avvio, solo con la mappatura della tastiera statunitense.
1	Modalità utente singolo.
2	Modalità multi-utente locale senza rete remota (NFS e così via).
3	Modalità multi-utente completa con rete.
4	Non utilizzato.
5	Modalità multi-utente completa con rete e gestione visualizzazione X (KDM, GDM o XDM).
6	Riavvio del sistema.

IMPORTANTE: non utilizzare il runlevel 2 con una partizione /usr montata tramite NFS

Evitare di utilizzare il runlevel 2 quando nel sistema viene montata la partizione `/usr` tramite NFS. La directory `/usr` contiene programmi di fondamentale importanza per un corretto funzionamento del sistema. Poiché il servizio NFS non è disponibile nel runlevel 2 (modalità multi-utente locale senza rete remota), il sistema sarà soggetto a importanti restrizioni riguardanti vari aspetti.

Per modificare i runlevel mentre il sistema è in esecuzione, immettere `init` e il numero corrispondente come argomento. Questa operazione può essere eseguita solo dall'amministratore di sistema. Di seguito vengono riepilogati i più importanti comandi per l'area dei runlevel.

`init 1` o `shutdown now`
Nel sistema viene attivata la *modalità utente singolo*, che viene utilizzata per task di manutenzione e amministrazione del sistema.

init 3
Vengono avviati tutti i programmi e i servizi di fondamentale importanza, inclusa la rete, e gli utenti regolari possono eseguire il login e utilizzare il sistema senza un ambiente grafico.

init 5
Viene abilitato l'ambiente grafico, che può essere uno dei desktop (GNOME o KDE) oppure qualsiasi gestore delle finestre.

init 0 o shutdown -h now
Il sistema viene arrestato.

init 6 o shutdown -r now
Il sistema viene arrestato e quindi riavviato.

Il runlevel `5` è il runlevel di default in tutte le installazioni standard di SUSE Linux. Per visualizzare la richiesta di login agli utenti viene utilizzata un'interfaccia grafica. Se il runlevel di default è `3`, prima di poter impostare il runlevel `5` è necessario che X Window System sia configurato in modo corretto, come descritto nel Capitolo 35, *X Window System* (p. 553). Verificare quindi che il sistema funzioni nel modo desiderato immettendo `init 5` . Se tutto funziona come previsto, è possibile utilizzare YaST per impostare il runlevel di default su `5`.

AVVERTIMENTO: eventuali errori in /etc/inittab possono compromettere l'avvio del sistema

Se il file `/etc/inittab` è danneggiato, è possibile che il sistema non venga avviato in modo corretto. Prestare pertanto particolare attenzione quando si apportano modifiche a `/etc/inittab` e tenere sempre a disposizione una copia di backup di una versione intatta. Per correggere gli errori, provare a immettere `init=/bin/sh` dopo il nome del kernel al prompt di avvio per eseguire un avvio diretto in una shell. Rendere quindi scrivibile il file system radice con il comando `mount -o remount,rw /` e sostituire `/etc/inittab` con la versione di backup tramite il comando `cp`. Per evitare che vengano inseriti errori nel file system, impostare il file system radice come di sola lettura prima di eseguire il riavvio con `mount -o remount,ro /` .

La modifica dei runlevel in genere ha due conseguenze. Innanzitutto, vengono avviati gli script di arresto del runlevel corrente, che chiudono alcuni programmi di fondamentale importanza per il runlevel corrente. Dopo di che, vengono avviati gli script di avvio

del nuovo runlevel. Durante questa seconda fase nella maggior parte dei casi vengono avviati vari programmi. Ad esempio, quando il runlevel viene modificato da 3 a 5, si verificano le seguenti operazioni:

1. L'amministratore (utente `root`) richiede a init di impostare un runlevel diverso immettendo `init 5 .`

2. Il programma init analizza il relativo file di configurazione (`/etc/inittab`) e determina che deve avviare `/etc/init.d/rc` con il nuovo runlevel come parametro.

3. A questo punto, `rc` chiama gli script di arresto del runlevel corrente per cui non esiste uno script di avvio nel nuovo runlevel. In questo esempio, si tratta di tutti gli script residenti in `/etc/init.d/rc3.d` (il runlevel precedente era 3) e che iniziano con la lettera `K`. Il numero indicato dopo la `K` specifica l'ordine di avvio in quanto è necessario tenere presenti alcune dipendenze.

4. Gli ultimi a essere avviati sono gli script di avvio del nuovo runlevel, che in questo esempio si trovano in `/etc/init.d/rc5.d` e iniziano con la lettera `S`. Anche in questo caso viene applicata la stessa procedura riguardante l'ordine di avvio.

Quando il nuovo runlevel coincide con quello corrente, init verifica semplicemente le modifiche in `/etc/inittab` ed esegue i passaggi appropriati, ad esempio per l'avvio di un comando `getty` su un'altra interfaccia.

28.2.2 Script di init

In `/etc/init.d` sono presenti due tipi di script:

Script eseguiti direttamente da init
Questi script vengono utilizzati solo durante il processo di avvio oppure qualora venga inizializzato un arresto immediato del sistema a causa di un'interruzione dell'alimentazione oppure in seguito alla pressione della combinazione di tasti Ctrl + Alt + Canc da parte dell'utente. Le modalità di esecuzione di questi script sono definite in `/etc/inittab`.

Script eseguiti indirettamente da init

Questi script vengono eseguiti in caso di modifica del runlevel e chiamano sempre lo script master `/etc/init.d/rc`, che garantisce l'ordine corretto degli script rilevanti.

Tutti gli script si trovano in `/etc/init.d`. Gli script per la modifica del runlevel sono anch'essi disponibili in questo percorso, ma vengono chiamati tramite collegamenti simbolici da una delle sottodirectory (da `/etc/init.d/rc0.d` a `/etc/init.d/rc6.d`). Questo solo per motivi di chiarezza e per evitare script duplicati nel caso in cui vengano utilizzati in più runlevel. Poiché ogni script può essere eseguito sia come script di avvio che come script di arresto, deve essere in grado di interpretare i parametri `start` e `stop` nonché le opzioni `restart`, `reload`, `force-reload` e `status`. Per informazioni su queste opzioni, vedere la Tabella 28.2, «Opzioni degli script di init» (p. 453). Gli script eseguiti direttamente da init non dispongono di questi collegamenti e possono essere eseguiti in modo indipendente dal runlevel quando necessario.

Tabella 28.2 *Opzioni degli script di init*

Opzione	Descrizione
`start`	Avvia il servizio.
`stop`	Interrompe il servizio.
`restart`	Se il servizio è in esecuzione, lo interrompe e quindi lo riavvia. Se il servizio non è in esecuzione, lo avvia.
`reload`	Ricarica la configurazione senza interrompere e riavviare il servizio.
`force-reload`	Ricarica la configurazione se il servizio supporta questa operazione. In caso contrario, esegue le stesse operazioni dell'opzione `restart`.
`status`	Visualizza lo stato corrente del servizio.

I collegamenti in ogni sottodirectory specifica del runlevel consentono di associare script a runlevel diversi. Quando si installano o disinstallano pacchetti, questi

collegamenti vengono aggiunti e rimossi tramite il programma insserv oppure tramite /usr/lib/lsb/install_initd, uno script che chiama questo programma. Per informazioni, vedere la documentazione di insserv(8).

Di seguito vengono riportate una breve introduzione agli script di avvio e di arresto, avviati rispettivamente per primo e per ultimo, e una descrizione dello script di manutenzione.

boot
: Viene eseguito durante l'avvio del sistema direttamente da init. È indipendente dal runlevel scelto e viene eseguito una sola volta. Consente di montare i file system proc e pts e di attivare blogd (il daemon di registrazione del processo di avvio). Quando il sistema viene avviato per la prima volta dopo un aggiornamento o un'installazione, viene avviata la configurazione del sistema iniziale.

  Il daemon blogd è un servizio avviato dagli script boot e rc prima di qualsiasi altro. Viene interrotto al termine delle azioni generate dagli script sopra indicati, ad esempio l'esecuzione di una serie di script secondari. Il daemon blogd scrive l'output a video nel file di log /var/log/boot.msg, ma solo se e quando /var è montato in modalità di lettura/scrittura. In caso contrario, blogd memorizza nel buffer tutti i dati a video fino a quando /var non diventa disponibile. Per ulteriori informazioni su blogd, vedere la documentazione di blogd(8).

  Lo script boot si occupa inoltre di avviare tutti gli script in /etc/init.d/boot.d il cui nome inizia con la lettera S. Questi script consentono di controllare i file system e di configurare se necessario i dispositivi con loop nonché di impostare l'ora di sistema. Se si verifica un errore durante la verifica e la riparazione automatica del file system, l'amministratore di sistema può intervenire dopo avere immesso la password root. L'ultimo a essere eseguito è lo script boot.local.

boot.local
: Consente di immettere ulteriori comandi da eseguire in fase di avvio prima di impostare un altro runlevel. Corrisponde a AUTOEXEC.BAT nei sistemi DOS.

boot.setup
: Questo script viene eseguito quando si passa dalla modalità utente singolo a qualsiasi altro runlevel ed esegue una serie di impostazioni di base, quali il layout di tastiera e l'inizializzazione di console virtuali.

halt
: Questo script viene eseguito solo quando viene impostato il runlevel 0 o 6 e può essere eseguito come `halt` o `reboot`. L'arresto o il riavvio del sistema dipende dalla modalità di chiamata di `halt`.

rc
: Questo script chiama gli script di arresto appropriati del runlevel corrente e gli script di avvio del nuovo runlevel scelto.

È possibile creare script personalizzati e integrarli senza difficoltà nello schema sopra descritto. Per istruzioni sulla formattazione, la denominazione e l'organizzazione di script personalizzati, fare riferimento alle specifiche di LSB e alla documentazione di `init`, `init.d` e `insserv`. Vedere inoltre la documentazione di `startproc` e `killproc`.

AVVERTIMENTO: eventuali errori negli script di init possono causare un arresto del sistema

Gli errori presenti negli script di init possono causare un arresto del computer. Prestare particolare attenzione quando si modificano questi script e, se possibile, sottoporli ad accurati test nell'ambiente multi-utente. Per informazioni sugli script di init, vedere la Sezione 28.2.1, «Runlevel» (p. 449).

Per creare uno script di init personalizzato per un determinato programma o servizio, utilizzare il file `/etc/init.d/skeleton` come modello. Salvare una copia di questo file con un nuovo nome e modificare i nomi di file e programma rilevanti, i percorsi e altri dettagli in base alle esigenze. Potrebbe inoltre essere necessario aggiungere sezioni personalizzate allo script in modo che durante la procedura di init vengano avviate le azioni corrette.

Il blocco `INIT INFO` all'inizio è una sezione necessaria dello script e deve essere modificata. Vedere l'Esempio 28.1, «Blocco INIT INFO minimo» (p. 456).

Esempio 28.1 *Blocco INIT INFO minimo*

```
### 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
```

Nella prima riga del blocco `INFO`, dopo `Provides`, specificare il nome del programma o del servizio controllato da questo script di init. Nelle righe `Required-Start` e `Required-Stop` specificare tutti i servizi da avviare o interrompere prima dell'avvio o dell'interruzione del servizio stesso. Queste informazioni verranno utilizzate successivamente per generare la numerazione dei nomi degli script, indicata nelle directory dei runlevel. Dopo `Default-Start` e `Default-Stop` specificare i runlevel in cui il servizio deve essere avviato o interrotto automaticamente. Infine, per `Description` specificare una breve descrizione del servizio in questione.

Per creare i collegamenti dalle directory dei runlevel (`/etc/init.d/rc?.d/`) agli script corrispondenti in `/etc/init.d/`, immettere il comando `insserv` *`nome-nuovo-script`* . Il programma insserv valuta l'intestazione `INIT INFO` per creare i collegamenti necessari per gli script di avvio e arresto nelle directory dei runlevel (`/etc/init.d/rc?.d/`). Questo programma gestisce inoltre il corretto ordine di avvio e di arresto per ogni runlevel tramite l'inserimento dei numeri necessari nei nomi di questi collegamenti. Se si preferisce utilizzare uno strumento con interfaccia grafica per creare questi collegamenti, eseguire l'editor dei runlevel fornito da YaST, come descritto nella Sezione 28.2.3, «Configurazione dei servizi di sistema (runlevel) con YaST» (p. 457).

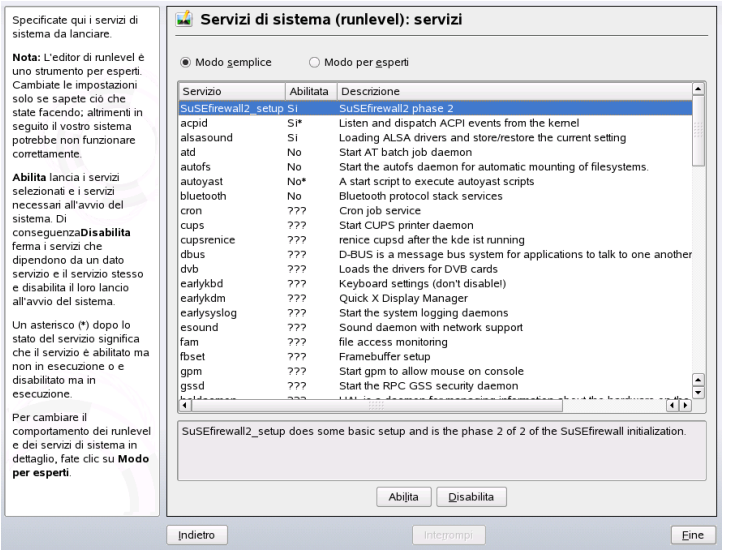
Se uno script già presente in `/etc/init.d/` deve essere integrato in uno schema di runlevel esistente, creare i collegamenti nelle directory dei runlevel direttamente con insserv oppure abilitando il servizio corrispondente nell'editor dei runlevel di YaST. Le modifiche apportate vengono applicate durante il successivo riavvio. Il nuovo servizio viene avviato automaticamente.

Non impostare questi collegamenti manualmente. Se nel blocco `INFO` è presente un errore, si verificheranno problemi durante la successiva esecuzione di `insserv` per un altro servizio.

28.2.3 Configurazione dei servizi di sistema (runlevel) con YaST

Dopo avere avviato questo modulo di YaST scegliendo *YaST → Sistema → Editor dei runlevel*, viene visualizzata una panoramica in cui sono elencati tutti i servizi disponibili e lo stato corrente di ognuno di essi (disabilitato o abilitato). Scegliere se utilizzare il modulo in *Modo semplice* o *Modo per esperti*. L'impostazione di default *Modo semplice* dovrebbe essere sufficiente nella maggior parte dei casi. Nella colonna di sinistra è indicato il nome del servizio, nella colonna centrale è indicato lo stato corrente e nella colonna di destra è disponibile una breve descrizione. Nella parte inferiore della finestra viene visualizzata una descrizione dettagliata del servizio selezionato. Per abilitare un servizio, selezionarlo nella tabella e quindi fare clic su *Abilita*. Per disabilitare un servizio, seguire questa stessa procedura.

Figura 28.1 *Servizi di sistema (runlevel)*



Per un controllo avanzato sui runlevel in cui viene avviato o arrestato un servizio oppure per modificare il runlevel di default, selezionare prima *Modo semplice*. Il runlevel di default corrente o «initdefault», ovvero il runlevel nel quale viene avviato il sistema per default, è visualizzato nella parte superiore della finestra. In genere, il runlevel di default di un sistema SUSE Linux è il runlevel 5 (modalità multi-utente completa con

rete e X). Una valida alternativa potrebbe essere il runlevel 3 (modalità multi-utente completa con rete).

In questa finestra di dialogo di YaST è possibile selezionare uno dei runlevel elencati nella Tabella 28.1, «Runlevel disponibili» (p. 450) come nuova impostazione di default. È inoltre possibile utilizzare la tabella di questa finestra per abilitare o disabilitare singoli servizi e daemon. In questa tabella sono elencati i servizi e i daemon disponibili ed è indicato se e per quali runlevel sono attualmente abilitati nel sistema. Dopo avere selezionato una delle righe con il mouse, fare clic sulle caselle di controllo rappresentanti i runlevel (*B*, *0*, *1*, *2*, *3*, *5*, *6* e *S*) per definire i runlevel in cui deve essere eseguito il servizio o il daemon selezionato. Il runlevel 4 inizialmente non è definito per consentire la creazione di un runlevel personalizzato. Sotto la tabella è disponibile una breve descrizione del servizio o del daemon attualmente selezionato.

Scegliere se attivare un servizio utilizzando il comando *Avvia/Arresta/Aggiorna*. *Aggiorna stato* consente di verificare lo stato corrente. *Imposta/Ripristina* consente di scegliere se applicare le modifiche al sistema o ripristinare le impostazioni esistenti prima dell'avvio dell'editor dei runlevel. Selezionare *Concludi* per salvare le impostazioni modificate su disco.

AVVERTIMENTO: eventuali errori nelle impostazioni dei runlevel possono danneggiare il sistema

Impostazioni dei runlevel errate possono compromettere l'uso del sistema. Prima di applicare le modifiche, è estremamente importante conoscere tutti gli effetti provocati.

28.3 Configurazione del sistema tramite /etc/sysconfig

La configurazione principale di SUSE Linux è controllata tramite i file di configurazione disponibili in `/etc/sysconfig`. I singoli file in `/etc/sysconfig` vengono letti solo dagli script per cui sono rilevanti. Ad esempio, le impostazioni di rete vengono analizzate solo dagli script correlati alla rete. Molti altri file di configurazione del sistema vengono generati in base alle impostazioni specificate in `/etc/sysconfig`. Questo task viene eseguito da SuSEconfig. Se, ad esempio, si modifica la configurazione della rete, SuSEconfig potrebbe apportare modifiche anche nel file `/etc/host.conf`,

uno dei file rilevanti per la configurazione della rete. Grazie a questo principio è possibile apportare modifiche di base alla configurazione senza riavviare il sistema.

Per modificare la configurazione del sistema è possibile scegliere tra due soluzioni: utilizzare l'editor di sysconfig disponibile in YaST oppure modificare i file di configurazione manualmente.

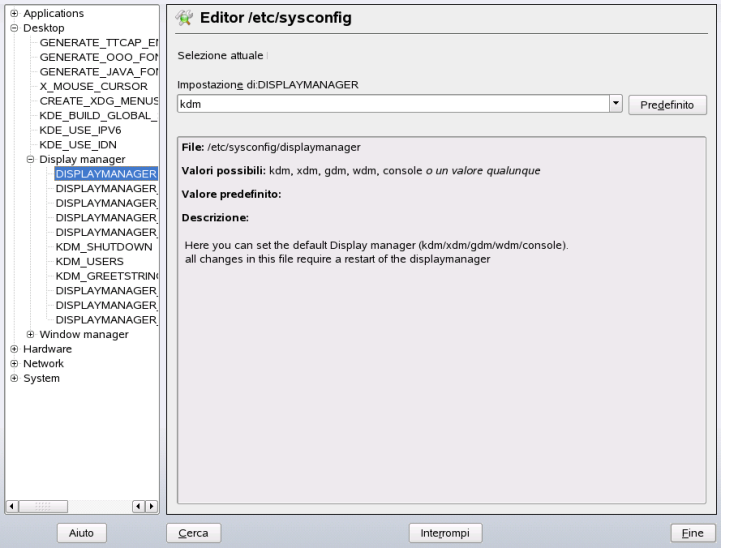
28.3.1 Modifica della configurazione del sistema con l'editor di sysconfig fornito da YaST

L'editor di sysconfig disponibile in YaST fornisce un front-end di facile uso per la configurazione del sistema. Anche se non si conosce la posizione effettiva di una variabile di configurazione da modificare, è possibile utilizzare la funzione di ricerca incorporata di questo modulo e modificare il valore di tale variabile in base alle esigenze. YaST si occuperà di applicare queste modifiche, aggiornare le configurazioni che dipendono dai valori impostati in `sysconfig` e riavviare i servizi.

AVVERTIMENTO: le modifiche dei file in /etc/sysconfig/* possono danneggiare l'installazione

I file in `/etc/sysconfig` devono essere modificati solo da utenti con precedenti esperienze e sufficienti conoscenze in materia. Una modifica errata potrebbe causare gravi danni al sistema. I file in `/etc/sysconfig` includono un breve commento per ogni variabile in cui viene descritto l'effetto provocato.

Figura 28.2 *Configurazione del sistema con l'editor di sysconfig.*



La finestra di dialogo di YaST relativa al file sysconfig è suddivisa in tre parti. Nella parte sinistra è disponibile una visualizzazione ad albero di tutte le variabili configurabili. Quando si seleziona una variabile, nella parte destra della finestra vengono visualizzate sia la selezione corrente che l'impostazione corrente di questa variabile. Nella parte inferiore della finestra viene visualizzata una breve descrizione che indica lo scopo della variabile, i possibili valori, il valore di default e il file di configurazione effettivo da cui viene originata questa variabile. In questa finestra di dialogo sono inoltre disponibili informazioni sullo script di configurazione eseguito dopo la modifica della variabile e sul nuovo servizio avviato in seguito alla modifica. Quando si chiude questa finestra di dialogo selezionando *Concludi*, viene visualizzato un messaggio per chiedere conferma delle modifiche e segnalare gli script che verranno eseguiti. Selezionare inoltre i servizi e gli script che per il momento si desidera ignorare, in modo che vengano avviati successivamente. Verranno applicate automaticamente tutte le modifiche e verranno riavviati tutti i servizi necessari per l'implementazione delle modifiche.

28.3.2 Modifica manuale della configurazione del sistema

Per modificare manualmente la configurazione del sistema, attenersi alla seguente procedura:

1. Eseguire il login come utente `root`.
2. Attivare la modalità utente singolo (runlevel 1) tramite il comando `init 1` .
3. Modificare i file di configurazione in base alle esigenze in un editor di propria scelta.

   Se non si utilizza YaST per modificare i file di configurazione in `/etc/sysconfig`, verificare che i valori vuoti delle variabili siano rappresentati da due virgolette (`KEYTABLE= ""`) e che i valori contenenti spazi siano racchiusi tra virgolette. Per i valori composti da una sola parola le virgolette non sono necessarie.
4. Eseguire `SuSEconfig` per essere certi che le modifiche vengano applicate.
5. Ripristinare il runlevel precedente nel sistema tramite un comando quale `init` *`runlevel_default`* . Sostituire *`runlevel_default`* con il runlevel di default del sistema. Scegliere `5` se si desidera ripristinare la modalità multi-utente completa con rete e X oppure `3` se si preferisce utilizzare la modalità multi-utente completa con rete.

È importante attenersi a questa procedura quando si modificano impostazioni che hanno effetto sull'intero sistema, ad esempio la configurazione della rete. Le modifiche di piccola entità in genere non richiedono l'attivazione della modalità utente singolo, che è però possibile utilizzare comunque per essere certi che vengano avviati in modo corretto tutti i programmi necessari.

SUGGERIMENTO: disabilitazione della configurazione automatica del sistema

Per disabilitare la configurazione automatica del sistema tramite SuSEconfig, impostare la variabile `ENABLE_SUSECONFIG` in `/etc/sysconfig/`

`suseconfig` su `no`. Non disabilitare SuSEconfig se si desidera utilizzare il supporto per l'installazione di SUSE. È inoltre possibile disabilitare la configurazione automatica parzialmente.

29 Boot Loader

In questo capitolo viene descritta la procedura di configurazione di GRUB, il boot loader utilizzato con SUSE Linux. È disponibile uno speciale modulo YaST per eseguire tutte le impostazioni. Per informazioni sull'avvio in Linux, leggere le sezioni seguenti per acquisire informazioni generali. In questo capitolo vengono inoltre descritti alcuni dei problemi più frequenti relativi all'avvio con GRUB e le relative soluzioni.

In questo capitolo vengono trattate la gestione dell'avvio e la configurazione del boot loader GRUB. L'intera procedura di avvio viene descritta nel Capitolo 28, *Avvio e configurazione di un sistema Linux* (p. 445). Un boot loader rappresenta l'interfaccia tra il computer (BIOS) e il sistema operativo (SUSE Linux). La configurazione del boot loader influisce direttamente sull'avvio del sistema operativo.

I termini seguenti ricorrono frequentemente nel presente capitolo e potrebbero richiedere qualche spiegazione:

Master Boot Record

La struttura dell'MBR viene definita da una convenzione indipendente dal sistema operativo. I primi 446 byte sono riservati al codice del programma e contengono in genere il programma del boot loader, in questo caso GRUB. I 64 byte successivi offrono lo spazio per una tabella della partizioni contenente fino a un massimo di quattro voci (vedere il sezione chiamata «Tipi di partizione» (Capitolo 1, *Installazione con YaST*, ↑Avvio)). La tabella delle partizioni contiene informazioni sul partizionamento del disco rigido e sul tipo di file system. Nel sistema operativo questa tabella è necessaria per la gestione del disco rigido. Gli ultimi due byte dell'MBR devono contenere un «numero magico» statico (AA55). Un MBR che

contiene valori diversi viene considerato non valido dal BIOS e da tutti i sistemi operativi per PC.

Settori di avvio

I settori di avvio sono i primi settori delle partizioni del disco rigido ad eccezione della partizione estesa che svolge esclusivamente la funzione di «contenitore» per le altre partizioni. Questi settori di avvio dispongono di 512 byte di spazio per il codice utilizzato per l'avvio di un sistema operativo installato nella partizione corrispondente. Questo vale per i settori di avvio delle partizioni DOS, Windows e OS/2 formattate, che contengono anche alcuni importanti dati di base del file system. I settori di avvio delle partizioni di Linux, invece, sono inizialmente vuoti dopo la configurazione del file system. Di conseguenza, una partizione Linux *non è avviabile autonomamente*, anche se contiene un kernel e un file system radice. Un settore di avvio con un codice valido per l'avvio del sistema ha lo stesso numero presentato dall'MBR negli ultimi due byte, ovvero `AA55`.

29.1 Gestione dell'avvio

Nei casi più semplici, se nel computer è installato un unico sistema operativo, la gestione dell'avvio avviene come descritto in precedenza. Se nel computer sono installati più sistemi operativi, sono disponibili le opzioni seguenti:

Avvio di sistemi aggiunti da supporti esterni

Uno dei sistemi operativi viene avviato dal disco rigido. Gli altri sistemi operativi vengono avviati mediante un boot manager installato in un supporto esterno, ad esempio disco floppy, CD o supporto di memorizzazione USB.

Installazione di un boot manager nell'MBR

Un boot manager consente l'installazione simultanea e l'uso alternato di più sistemi operativi in un unico computer. Gli utenti possono selezionare il sistema da avviare durante il processo di avvio. Per passare a un altro sistema, è necessario riavviare il computer. Questo è possibile solo se il boot manager selezionato è compatibile con i sistemi operativi installati. GRUB è il boot manager utilizzato in SUSE Linux.

29.2 Selezione di un boot loader

Per default, in SUSE Linux viene utilizzato il boot loader GRUB. In alcuni casi e per speciali configurazioni hardware e software, tuttavia, potrebbe essere consigliabile l'utilizzo di LILO. Se si esegue l'aggiornamento di una versione di SUSE Linux precedente che utilizza LILO, viene installato quest'ultimo.

Per ulteriori informazioni sull'installazione e la configurazione di LILO, consultare il database del supporto tecnico alla voce LILO e il file `/usr/share/doc/packages/lilo`.

29.3 Avvio con GRUB

GRUB (Grand Unified Bootloader) prevede due fasi. stage1 consiste di 512 byte e viene scritto nell'MBR o nel settore di avvio della partizione del disco rigido o del disco floppy. Successivamente viene caricato stage2. Questa fase contiene il codice effettivo del programma. L'unico task della prima fase è il caricamento della seconda fase del boot loader.

stage2 è in grado di accedere ai file system. Attualmente sono supportati i file system Ext2, Ext3, ReiserFS, Minix e il file DOS FAT utilizzato da Windows. Sono in parte supportati anche i file system JFS, XFS, UFS e FFS utilizzati dai sistemi BSD. Dalla versione 0.95, GRUB è inoltre in grado di eseguire l'avvio da un CD o DVD contenente un file system ISO 9660 standard, purché vi sia la specifica «El Torito». Anche prima dell'avvio del sistema, GRUB può accedere ai file system dei dispositivi disco del BIOS, ovvero dischi floppy o dischi rigidi, unità CD e DVD rilevate dal BIOS. Eventuali modifiche al file di configurazione di GRUB `menu.lst` non richiedono pertanto la reinstallazione del boot manager. Quando il sistema viene avviato, GRUB carica nuovamente il file di menu con i percorsi e i dati di partizione validi del kernel o il disco RAM iniziale (`initrd`) e individua questi file.

La configurazione effettiva di GRUB si basa su tre file che vengono descritti di seguito:

`/boot/grub/menu.lst`

Questo file contiene tutte le informazioni relative alle partizioni o ai sistemi operativi che possono essere avviati con GRUB. Senza queste informazioni, non è possibile passare il controllo di sistema al sistema operativo.

/boot/grub/device.map

Questo file trasforma i nomi dei dispositivi dalla notazione GRUB e BIOS a nomi dei dispositivi Linux.

/etc/grub.conf

Questo file contiene i parametri e le opzioni necessarie alla shell di GRUB per la corretta installazione del boot loader.

È possibile controllare GRUB in vari modi. È possibile selezionare le voci di una configurazione esistente dal menu grafico, ovvero dalla schermata di avvio. La configurazione viene caricata dal file `menu.lst`.

In GRUB, tutti i parametri di avvio possono essere modificati prima dell'esecuzione dell'avvio. In questo modo è ad esempio possibile correggere gli errori fatti durante la modifica del file di menu. È inoltre possibile immettere in modo interattivo i comandi di avvio mediante una sorta di prompt di input (vedere la sezione chiamata «Modifica delle voci di menu nel corso della procedura di avvio» (p. 470)). Con GRUB è possibile determinare la posizione del kernel e del file `initrd` prima dell'esecuzione dell'avvio. In questo modo è inoltre possibile avviare un sistema operativo installato per il quale non vi sono voci nella configurazione del boot loader.

La *shell di GRUB* fornisce un'emulazione di GRUB nel sistema installato che può essere utilizzata per installare GRUB o per verificare le nuove impostazioni prima di applicarle. Vedere Sezione 29.3.4, «Shell di GRUB» (p. 474).

29.3.1 Menu di avvio di GRUB

La schermata di avvio grafica contenente il menu di avvio si basa sul file di configurazione di GRUB `/boot/grub/menu.lst`, che contiene tutte le informazioni su tutte le partizioni o i sistemi operativi che possono essere avviati dal menu.

Ogni volta che il sistema viene avviato, GRUB carica il file di menu dal file system. Per questo motivo, non è necessario reinstallare GRUB in seguito a eventuali modifiche al file. Utilizzare il boot loader di YaST per modificare la configurazione di GRUB, come descritto nella Sezione 29.4, «Configurazione del boot loader con YaST» (p. 476).

Il file di menu contiene comandi. La sintassi è estremamente semplice. Ogni riga contiene un comando, seguito da parametri facoltativi separati da spazi, come nella shell. Alcuni

comandi ammettono un segno = davanti al primo parametro. I commenti sono introdotti dal carattere cancelletto (#).

Per identificare le voci di menu nella panoramica del menu, specificare `title` per ogni voce. Il testo (inclusi eventuali spazi) che segue la parola chiave `title` viene visualizzato come opzione selezionabile nel menu. Quando si seleziona questa voce di menu, vengono eseguiti tutti i comandi fino alla successiva occorrenza di `title`.

Il caso più semplice è costituito dal reindirizzamento a boot loader di altri sistemi operativi. Il comando è `chainloader` e l'argomento è solitamente il blocco di avvio di un'altra partizione nella notazione di blocco di GRUB. Ad esempio:

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

I nomi dei dispositivi in GRUB vengono illustrati nella sezione chiamata «Convenzioni di denominazione per dischi rigidi e partizioni» (p. 468). L'esempio precedente specifica il primo blocco della quarta partizione del disco rigido.

Utilizzare il comando `kernel` per specificare un immagine del kernel. Il primo argomento è il percorso dell'immagine del kernel in una partizione. Gli altri argomenti vengono passati al kernel nella riga di comando.

Se il kernel non dispone di driver incorporati per l'accesso alla partizione radice, è necessario specificare `initrd` con un comando separato di GRUB il cui unico argomento è costituito dal percorso del file `initrd`. Poiché l'indirizzo di caricamento del file `initrd` è scritto nell'immagine del kernel caricata, il comando `initrd` deve seguire immediatamente il comando `kernel`.

Il comando `root` semplifica la specifica dei file kernel e initrd. Il solo argomento del comando `root` è un dispositivo GRUB o una partizione su un dispositivo GRUB. Questo dispositivo viene utilizzato per tutti i file kernel, `initrd` o altri percorsi di file per i quali non viene specificato esplicitamente alcun dispositivo fino al successivo comando `root`. Questo comando non viene utilizzato nel file `menu.lst` generato durante l'installazione. Esso consente esclusivamente di facilitare le modifiche manuali.

Il comando `boot` è implicito alla fine di ogni voce di menu, quindi non è necessario scriverlo all'interno del file di menu. Se tuttavia si utilizza GRUB in modo interattivo per l'avvio, è necessario immettere il comando `boot` al termine. Il comando non contiene argomenti. Si limita ad avviare l'immagine del kernel caricata o il chainloader specificato.

Dopo aver scritto tutte le voci di menu, definirne una come `default`. In caso contrario, verrà utilizzata la prima voce (`0`). È inoltre possibile specificare un timeout espresso in secondi, trascorso il quale la voce di default deve eseguire l'avvio. I comandi `timeout` e `default` precedono in genere le voci di menu. Un file di esempio è descritto nella sezione chiamata «File di menu di esempio» (p. 469).

Convenzioni di denominazione per dischi rigidi e partizioni

Le convenzioni di denominazione utilizzate da GRUB per i dischi rigidi e le partizioni sono diverse da quelle utilizzate per i normali dispositivi Linux. In GRUB, la numerazione delle partizioni inizia da zero. Pertanto `hd0,0` è la prima partizione del primo disco rigido. In un computer desktop con disco rigido connesso come master primario, il nome del dispositivo Linux corrispondente è `/dev/hda1`.

Alle quattro possibili partizioni primarie sono assegnati i numeri di partizione da `0` a `3`. Le partizioni logiche sono numerate a partire da `4`:

```
(hd0,0)    first primary partition of the first hard disk
(hd0,1)    second primary partition
(hd0,2)    third primary partition
(hd0,3)    fourth primary partition (usually an extended partition)
(hd0,4)    first logical partition
(hd0,5)    second logical partition
```

In GRUB non vi è distinzione tra dispositivi IDE, SCSI e RAID. Tutti i dischi rigidi riconosciuti dal BIOS o da altri controller vengono numerati in base alla sequenza di avvio preimpostata nel BIOS.

GRUB non è in grado di mappare i nomi di dispositivi Linux ai nomi di dispositivi del BIOS in modo corretto. La mappatura viene eseguita con l'aiuto di un algoritmo e salvata nel file `device.map` che può essere modificato in caso di necessità. Per informazioni sul file `device.map`, vedere la Sezione 29.3.2, «FIle device.map» (p. 472).

Un percorso GRUB completo è composto da un nome di dispositivo scritto tra parentesi e dal percorso del file nel file system nella partizione specificata. Il percorso inizia con una barra. È possibile ad esempio specificare il kernel avviabile in un sistema con un disco rigido IDE singolo contenente Linux nella prima partizione come indicato di seguito:

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

File di menu di esempio

Nell'esempio seguente viene mostrata la struttura di un file di menu di GRUB . L'installazione di esempio include una partizione di avvio di Linux in `/dev/hda5`, una partizione radice in `/dev/hda7` e un'installazione di Windows in `/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 definisce la configurazione della schermata di avvio:

gfxmenu (hd0,4)/message
L'immagine di sfondo `message` si trova in `/dev/hda5`.

color white/blue black/light-gray
Schema dei colori: bianco (primo piano), blu (sfondo), nero (selezione) e grigio chiaro (sfondo della selezione). Lo schema dei colori non influisce sulla schermata di avvio, ma solo sul menu personalizzabile di GRUB al quale è possibile accedere quando si esce dalla schermata di avvio utilizzando il tasto Esc.

default 0
La prima voce di menu `title linux` è quella che viene avviata per default.

timeout 8
Dopo otto secondi senza alcun input da parte dell'utente, la voce di default viene avviata automaticamente. Per disattivare l'avvio automatico, cancellare la riga `timeout`. Se si imposta `timeout 0`, la voce di default viene avviata immediatamente.

Il secondo blocco, più esteso, elenca i vari sistemi operativi avviabili. Le sezioni per i singoli sistemi operativi sono introdotte da `title`.

- La prima voce (`title linux`) è responsabile dell'avvio di SUSE Linux. Il kernel (`vmlinuz`) si trova nella prima partizione logica, ovvero la partizione di avvio, del primo disco rigido. I parametri del kernel, quali la partizione radice e la modalità VGA, vengono aggiunti qui. La partizione radice viene specificata in base alla convenzione di denominazione di Linux (`/dev/hda7/`). Poiché questa informazione viene letta dal kernel non ha alcuna relazione con GRUB. Anche `initrd` è posizionato nella prima partizione logica del primo disco rigido.

- La seconda voce è responsabile del caricamento di Windows. L'avvio di Windows avviene dalla prima partizione del primo disco rigido (`hd0,0`). Il comando `chainloader +1` determina la lettura e l'esecuzione del primo settore della partizione specificata da parte di GRUB.

- La voce successiva abilita l'avvio dal disco floppy senza modificare le impostazioni del BIOS.

- L'opzione di avvio `failsafe` avvia Linux con una selezione di parametri del kernel che consentono l'avvio di Linux anche con sistemi problematici.

Il file di menu può essere modificato ogni volta che sia necessario. Le impostazioni modificate verranno utilizzate da GRUB all'avvio successivo. Modificare permanentemente il file mediante YaST oppure un editor di propria scelta. In alternativa, apportare modifiche temporanee in modo interattivo utilizzando la funzione di modifica di GRUB. Vedere sezione chiamata «Modifica delle voci di menu nel corso della procedura di avvio» (p. 470).

Modifica delle voci di menu nel corso della procedura di avvio

Dal menu di avvio grafico di GRUB, selezionare il sistema operativo da avviare mediante i tasti freccia. Se si seleziona un sistema Linux, è possibile immettere parametri di avvio aggiuntivi al prompt di avvio. Per modificare singole voci di menu direttamente, premere Esc per uscire dalla schermata di avvio e quindi premere E. Le modifiche apportate in questo modo si applicano solo alla procedura di avvio corrente e non vengono adottate permanentemente.

IMPORTANTE: Layout di tastiera durante la procedura di avvio

Il layout di tastiera USA è l'unico disponibile nella fase di avvio.

Dopo aver attivato la modalità di modifica, utilizzare i tasti freccia per selezionare la voce di menu di cui si desidera modificare la configurazione. Per rendere la configurazione modificabile, premere E ancora una volta. Modificare in questo modo le partizioni o le specifiche di percorso errate prima che possano avere effetti negativi sul processo di avvio. Premere Invio per uscire dalla modalità di modifica e tornare al menu. Premere quindi B per avviare questa voce. Nel testo della Guida nella parte inferiore vengono visualizzate le ulteriori azioni possibili.

Per immettere le opzioni di avvio modificate permanentemente e passarle al kernel, aprire il file `menu.lst` come utente `root` e aggiungere i parametri corrispondenti del kernel alla riga esistente, separati da spazi:

```
title linux
   kernel (hd0,0)/vmlinuz root=/dev/hda3 additional parameter
   initrd (hd0,0)/initrd
```

I nuovi parametri vengono automaticamente adottati da GRUB all'avvio successivo del sistema. In alternativa, questa modifica può essere effettuata mediante il modulo boot loader di YaST. Aggiungere i nuovi parametri alla riga esistente, separati da spazi.

Uso di caratteri jolly per selezionare il kernel di avvio

In particolare durante lo sviluppo o l' utilizzo di kernel personalizzati, è necessario modificare le voci in `menu.lst` oppure modificare la riga di comando per riflettere i nomi dei file kernel e initrd correnti. Per semplificare questa procedura, utilizzare i *caratteri jolly* per aggiornare dinamicamente l'elenco di kernel di GRUB. Tutte le immagini del kernel che corrispondono a un modello specifico vengono quindi aggiunte automaticamente all'elenco delle immagini avviabili. Si noti che non c'è supporto per questa funzionalità.

Attivare l'opzione dei caratteri jolly immettendo in `menu.lst` una voce di menu aggiuntiva. Per essere utili, tutte le immagini del kernel e di initrd devono avere un nome di base comune e un identificativo corrispondenti al kernel e all'initrd associati. Si consideri la configurazione seguente:

```
initrd-default
initrd-test
```

```
vmlinuz-default
vmlinuz-test
```

In questo caso, sarebbe possibile aggiungere entrambe le immagini di avvio in un'unica configurazione di GRUB. Per ottenere le voci di menu `linux-default` e `linux-test`, in `menu.lst` è necessaria la voce seguente:

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

In questo esempio, nella partizione (hd0,4) viene eseguita automaticamente una ricerca delle voci che corrispondono al carattere jolly. Queste voci vengono utilizzate per generare nuove voci di menu di GRUB. Nell'esempio precedente, GRUB si comporta come se in `menu.lst` esistessero le voci seguenti:

```
title linux-default
   wildcard (hd0,4)/vmlinuz-default
   kernel (hd0,4)/vmlinuz-default root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-default
title linux-test
   wildcard (hd0,4)/vmlinuz-test
   kernel (hd0,4)/vmlinuz-test root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-test
```

Con questa configurazione possono verificarsi degli errori se i nomi dei file non sono utilizzati in modo coerente oppure se uno dei file espansi, ad esempio l'immagine di initrd, è mancante.

29.3.2 FIle device.map

Il file `device.map` esegue la mappatura dei nomi dei dispositivi GRUB ai nomi dei dispositivi Linux. In un sistema misto che contiene dischi rigidi IDE e SCSI, è necessario che GRUB cerchi di determinare la sequenza di avvio tramite una procedura speciale poiché GRUB non dispone dell'accesso alle informazioni del BIOS nella sequenza di avvio. In GRUB i risultati di questa analisi vengono salvati nel file `/boot/grub/device.map`. Per un sistema nel quale la sequenza di avvio nel BIOS è impostata su IDE prima di SCSI, il file `device.map` può presentarsi come indicato di seguito:

```
(fd0)  /dev/fd0
(hd0)  /dev/hda
(hd1)  /dev/sda
```

Poiché l'ordine di IDE, SCSI e di altri dischi rigidi dipende da diversi fattori e Linux non è in grado di identificare la mappatura, è possibile impostare manualmente la sequenza nel file `device.map`. Se si verificano problemi durante l'avvio, verificare che la sequenza in questo file corrisponda alla sequenza nel BIOS e utilizzare la shell di GRUB, descritta nella Sezione 29.3.4, «Shell di GRUB» (p. 474), per modificarla temporaneamente, se necessario. Dopo l'avvio del sistema Linux, è possibile modificare il file `device.map` permanentemente mediante il modulo boot loader di YaST o un editor di propria scelta.

Dopo aver modificato manualmente il file `device.map`, per reinstallare GRUB eseguire il comando seguente. Questo comando determina il ricaricamento del file `device.map` e l'esecuzione dei comandi elencati in `grub.conf`:

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

29.3.3 File /etc/grub.conf

Il terzo importante file di configurazione di GRUB, oltre a `menu.lst` e `device.map` è `/etc/grub.conf`. In questo file sono contenuti i parametri e le opzioni di cui il comando `grub` ha bisogno per l'installazione corretta del boot loader:

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

Significato delle singole voci:

root (hd0,4)
: Questo comando determina in GRUB l'applicazione dei comandi indicati di seguito alla prima partizione logica del primo disco rigido (posizione dei file di avvio).

`parametro` install
: È consigliabile eseguire il comando `grub` con il parametro `install`. È consigliabile installare `stage1` del boot loader nell'MBR del primo disco rigido (`/grub/stage1 d (hd0)`). È consigliabile caricare `stage2` nell'indirizzo della memoria 0x8000 (`/grub/stage2 0x8000`). L'ultima voce (`(hd0,4)/grub/menu.lst`) indica a GRUB dove cercare il file di menu.

29.3.4 Shell di GRUB

Esistono due versioni di GRUB, come boot loader e come normale programma Linux in `/usr/sbin/grub`. Questo programma viene indicato come *shell di GRUB*. La funzionalità per installare GRUB come boot loader nel disco rigido o nel disco floppy è integrata in GRUB sotto forma dei comandi `install` e `setup` ed è disponibile nella shell di GRUB quando Linux viene caricato.

I comandi `setup` e `install` sono tuttavia disponibili anche durante la procedura di avvio prima di avviare Linux. Questo semplifica la riparazione di un sistema difettoso che non può più essere avviato poiché il file di configurazione errato del boot loader può essere ignorato immettendo i parametri manualmente. L'immissione manuale dei parametri durante la procedura di avvio è utile anche per verificare le nuove impostazioni senza creare problemi al sistema nativo. È sufficiente immettere il file di configurazione sperimentale con una sintassi simile a quella presente in `menu.lst`. Verificare quindi la funzionalità di questa voce senza modificare il file di configurazione esistente. Per verificare un nuovo kernel, ad esempio, immettere il comando `kernel` e il percorso al nuovo kernel. Se non è possibile eseguire la procedura di avvio, si può continuare a utilizzare `menu.lst` senza modifiche all'avvio successivo. Allo stesso modo, l'interfaccia della riga di comando può anche essere utilizzata per avviare un sistema indipendentemente dalla presenza di un file `menu.lst` errato, grazie all'immissione dei parametri corretti. Nel sistema in esecuzione, è possibile immettere i parametri corretti in `menu.lst` per rendere il sistema permanentemente avviabile.

La mappatura dei dispositivi GRUB ai nomi dei dispositivi Linux è rilevante solo quando si esegue la shell di GRUB come programma Linux immettendo `grub` come descritto nella Sezione 29.3.2, «FIle device.map» (p. 472). A questo scopo, il programma legge il file `device.map`. Per ulteriori informazioni, vedere Sezione 29.3.2, «FIle device.map» (p. 472).

29.3.5 Impostazione di una password di avvio

Con GRUB è possibile accedere ai file system anche prima dell'avvio del sistema operativo. Gli utenti che non dispongono di autorizzazioni radice possono accedere ai file del sistema Linux in uso ai quali non hanno accesso dopo l'avvio del sistema. Per

bloccare questo genere di accesso o evitare che gli utenti possano avviare determinati sistemi operativi, impostare una password di avvio.

IMPORTANTE: Password di avvio e schermata di avvio

Se si utilizza una password di avvio per GRUB, non viene visualizzata la normale schermata di avvio.

Come utente `root`, per impostare una password di avvio procedere come indicato di seguito:

1. Al prompt radice, immettere `grub`.

2. Cifrare la password nella shell di GRUB:

```
grub> md5crypt
Password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

3. Incollare la stringa cifrata nella sezione generale del file `menu.lst`:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

   È ora possibile eseguire i comandi GRUB solo al prompt di avvio dopo aver premuto P e aver immesso la password. Gli utenti possono tuttavia avviare ancora tutti i sistemi operativi dal menu di avvio.

4. Per evitare l'avvio di uno o più sistemi operativi dal menu di avvio, aggiungere la voce `lock` a ogni sezione nel file `menu.lst` per la quale si desidera impedire l'avvio senza l'immissione di una password. Ad esempio:

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

   Dopo il riavvio del sistema e la selezione della voce di Linux dal menu di avvio, viene visualizzato il messaggio di errore seguente:

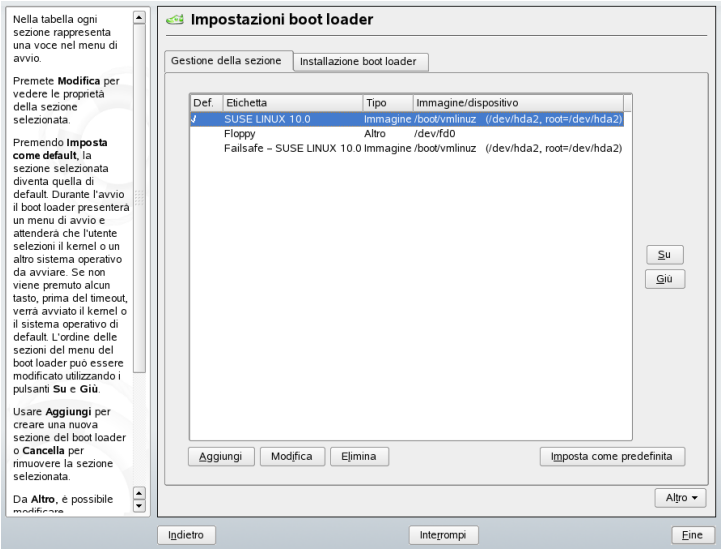
```
Error 32: Must be authenticated
```

Premere Invio per immettere il menu. Quindi premere P per il prompt della password. Dopo aver immesso la password e aver premuto Invio, il sistema operativo selezionato, in questo caso Linux, dovrebbe avviarsi.

29.4 Configurazione del boot loader con YaST

Il modo più semplice per configurare il boot loader nel sistema SUSE Linux in uso consiste nell'utilizzare il modulo di YaST. Nel centro controllo YaST selezionare *Sistema → Configurazione bootloader*. Viene visualizzata la configurazione attuale del boot loader nel sistema in uso ed è possibile apportare le modifiche desiderate. Vedere la Figura 29.1, «Configurazione del boot loader con YaST» (p. 476).

Figura 29.1 *Configurazione del boot loader con YaST*



La finestra principale è composta da due schede:

Gestione della sezione
Utilizzare questa scheda per modificare, sostituire e cancellare le sezioni del boot loader per i singoli sistemi operativi. Per aggiungere un'opzione, fare clic su

Aggiungi. Per cambiare il valore di un'opzione esistente, selezionarlo con il mouse e fare clic su *Modifica*. Se non si desidera utilizzare un'opzione esistente, selezionarla e fare clic su *Cancella*. Per informazioni sulle opzioni del boot loader, vedere la Sezione 29.3, «Avvio con GRUB» (p. 465).

Installazione boot loader
Utilizzare questa scheda per visualizzare e modificare le impostazioni del boot loader, ad esempio relative al tipo e alla posizione.

29.4.1 Tipo di boot loader

Il tipo di boot loader viene impostato nella scheda *Installazione boot loader*. Il boot loader di default in SUSE Linux è GRUB. Per utilizzare LILO, procedere come indicato di seguito:

Procedura 29.2 *Modifica del tipo di boot loader*

1. Aprire la scheda *Installazione boot loader*.
2. Nel riquadro *Tipo* fare clic sul menu *Boot Loader* e selezionare *LILO*.
3. Scegliere una delle seguenti azioni dal menu popup:

   Proponi nuova configurazione
   YaST propone una nuova configurazione.

   Converti la configurazione attuale
   YaST converte la configurazione attuale. Durante questo processo, alcune impostazioni potrebbero essere perse.

   Inizia nuova configurazione
   Utilizzare questa opzione per creare una configurazione personalizzata. Questa azione non è disponibile durante l'installazione di SUSE Linux.

   Carica configurazione salvata sul disco
   Utilizzare questa opzione per caricare un file `/etc/lilo.conf` personalizzato. Questa azione non è disponibile durante l'installazione di SUSE Linux.
4. Fare clic su *OK* per salvare le modifiche.

5 Fare clic su *Fine* nella finestra di dialogo principale per attivare le modifiche.

Dopo la conversione, la configurazione GRUB precedente viene salvata su disco. Per utilizzarla, reimpostare semplicemente il tipo di boot loader su GRUB e scegliere *Ripristina la configurazione prima della conversione* dal menu popup. Questa azione è disponibile solo in un sistema installato.

NOTA: Boot loader personalizzato

Se si desidera utilizzare un boot loader diverso da GRUB o LILO, fare clic sull'opzione *Non installare alcun boot loader*. Prima di scegliere questa opzione, leggere attentamente la documentazione del boot loader in uso.

29.4.2 Posizione del boot loader

Potrebbe essere necessario modificare la posizione del boot loader. Il modulo di YaST consente di eseguire questa operazione in modo semplificato.

Procedura 29.3 *Modifica della posizione del boot loader*

1 Per modificare la posizione del boot loader, fare clic sulla scheda *Installazione boot loader*, quindi selezionare una delle seguenti opzioni dal menu *Posizione del boot loader*:

Master boot record di /dev/hdX
Il master boot di un disco. È consigliabile utilizzare questa opzione ogni volta che SUSE determina che il sistema può essere avviato in questo modo. La X identifica il disco rigido, ovvero, a, b, c, d:

```
hda => ide0 master
     hdb => ide0 slave
     hdc => ide1 master
     hdd => ide1 slave
```

Settore di avvio della partizione di avvio /dev/hdXY
Il settore di avvio della partizione `/boot`. Questa è l'opzione di default nel caso in cui nell'unità disco rigido siano installati più sistemi operativi. La Y rappresenta la partizione, ovvero 1, 2, 3, 4, 5 e così via. La voce potrebbe quindi essere simile alla seguente:

```
/dev/hda1
```

Settore di avvio della partizione radice /dev/hdXY
Il settore di avvio della partizione / (radice). Anche questa opzione viene utilizzata se nell'unità disco rigido sono installati più sistemi operativi e si desidera continuare a utilizzare il boot manager precedente.

Altro
Questa opzione consente di specificare la posizione del boot loader.

2 Fare clic su *Fine* per attivare le modifiche.

29.4.3 Sistema di default

Per modificare il sistema di default, procedere come indicato di seguito:

Procedura 29.4 *Impostazione del sistema di default*

1 Aprire la scheda *Gestione della sezione*.

2 Selezionare il sistema desiderato dall'elenco utilizzando il mouse oppure facendo clic su *Su* o *Giù*.

3 Fare clic su *Imposta come default*.

4 Fare clic su *Fine* per attivare le modifiche.

29.4.4 Timeout del boot loader

Il sistema di default non viene avviato immediatamente dal boot loader. Durante questo timeout è possibile interrompere l'avvio del sistema di default e modificare il sistema per avviare o scrivere alcuni parametri del kernel. Per aumentare o ridurre il timeout del boot loader, procedere come indicato di seguito:

Procedura 29.5 *Modifica del timeout del boot loader*

1 Aprire la scheda *Installazione boot loader*.

2 Fare clic su *Opzioni boot loader*.

3 Selezionare *Mostra menu di avvio*.

4 In *Menu di avvio* modificare il valore di *Timeout menu di avvio* immettendo un nuovo valore, facendo clic con il mouse sul pulsante freccia appropriato oppure utilizzando i tasti freccia della tastiera.

5 Fare clic su *OK*.

6 Fare clic su *Fine* per attivare le modifiche.

È possibile decidere se il menu di avvio deve essere visualizzato in modo permanente senza limiti di tempo facendo clic sulla casella *Continua avvio dopo timeout*.

29.4.5 Impostazioni di sicurezza

Questo modulo di YaST garantisce inoltre un livello di sicurezza aggiuntivo in quanto consente di impostare una password, o parola d'ordine, per proteggere il boot loader.

Procedura 29.6 *Impostazione della password per il boot loader*

1 Aprire la scheda *Installazione boot loader*.

2 Fare clic su *Opzioni boot loader*.

3 In *Protezione con parola d'ordine* selezionare *Proteggi bootloader con parola d'ordine* e impostare la password desiderata.

4 Fare clic su *OK*.

5 Fare clic su *Fine* per attivare le modifiche.

29.4.6 Ordine dei dischi

Se nel computer in uso sono installati più dischi rigidi, è possibile specificare la sequenza di avvio dei dischi in base alla configurazione del BIOS del computer (vedere la Sezione 29.3.2, «FIle device.map» (p. 472)). A tale scopo, procedere come indicato di seguito:

Procedura 29.7 *Impostazione dell'ordine dei dischi*

1. Aprire la scheda *Installazione boot loader*.
2. Fare clic su *Dettagli installazione boot loader*.
3. Se nell'elenco sono indicati più dischi, selezionarne uno e fare clic su *Su* o *Giù* per riordinare i dischi visualizzati.
4. Fare clic su *OK* per salvare le modifiche.
5. Fare clic su *Fine* per attivare le modifiche.

Questo modulo consente inoltre di sostituire il master boot record con codice generico (che avvia la partizione attiva). Fare clic su *Sostituisci MBR con codice generico* in *Aggiornamento aree di sistema del disco*. È anche possibile fare clic su *Attiva la partizione del boot loader* nello stesso riquadro per attivare la partizione che contiene il boot loader. Fare clic su *Fine* per attivare le modifiche.

29.5 Disinstallazione del boot loader di Linux

È possibile utilizzare YaST per disinstallare il boot loader di Linux e ripristinare l'MBR nello stato precedente all'installazione di Linux. Durante l'installazione, con YaST viene creata automaticamente una copia di backup dell'MBR originale e, se richiesto, viene ripristinata sovrascrivendo GRUB.

Per disinstallare GRUB, avviare il modulo boot loader di YaST mediante *Sistema → Configurazione bootloader*. Nella prima finestra di dialogo, selezionare *Reimposta → Ripristina MBR del disco rigido* e uscire dalla finestra di dialogo facendo clic su *Fine*. Nell'MBR, i dati dell'MBR originale vengono sovrascritti su GRUB.

29.6 Creare il CD di avvio

Se doveste incontrare delle difficoltà durante l'esecuzione del boot del vostro sistema o il bootmanager non si lascia installare né nell' MBR del vostro disco rigido né su

dischetto, sussiste la possibilità di creare un CD avviabile con tutti file di avvio per Linux richiesti. Chiaramente il vostro sistema dovrà disporre di un masterizzatore di CD.

Per creare un CD-Rom avviabile con GRUB occorre un *stage2* particolare denominato `stage2_eltorito` e facoltativamente e quindi non necessariamente un `menu.lst` su misura. Non sono richiesti i classici file `stage1` e `stage2`.

Create una directory in cui generare l'immagine ISO, per esempio con `cd /tmp` e `mkdir iso`. Create una sottodirectory per GRUB con `mkdir -p iso/boot/grub`. Copiate il file `stage2_eltorito` nella directory `grub`:

```
cp /usr/lib/grub/stage2_eltorito iso/boot/grub
```

Copiate anche il kernel (`/boot/vmlinuz`), `initrd` (`/boot/initrd`) e `/boot/message` sotto `iso/boot/`:

```
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
cp /boot/message iso/boot/
```

Affinché GRUB possa individuare questi file, copiate `menu.lst` sotto `iso/boot/grub` e modificate l'indicazione del percorso in modo che vengono letti i file sul CD sostituendo nell'indicazione del percorso il nome di dispositivo del disco rigido (ad es. `(hd*)`) con il nome di dispositivo del lettore di CD (`(cd)`):

```
gfxmenu (cd)/boot/message
timeout 8
default 0

title Linux
    kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1
splash=verbose showopts
    initrd (cd)/boot/initrd
```

Create quindi un immagine ISO9660 servendovi del comando riportato di seguito:

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso iso
```

Infine masterizzate il file `grub.iso` risultante su un CD servendovi di un'applicazione di vostra preferenza.

29.7 Schermata grafica SUSE

A partire da SUSE Linux 7.2, la schermata grafica SUSE viene visualizzata nella prima console se l'opzione «vga=<valore>» viene utilizzata come parametro del kernel. Se si esegue l'installazione mediante YaST, questa opzione viene automaticamente attivata in base alla risoluzione e alla scheda grafica selezionate. Vi sono tre modi per disabilitare la schermata SUSE, se lo si desidera:

Disabilitazione della schermata SUSE quando necessario.
Immettere il comando `echo 0 >/proc/splash` nella riga di comando per disabilitare la schermata grafica. Per riattivarla, immettere `echo 1 >/proc/splash`.

Disabilitazione della schermata SUSE per default.
Aggiungere il parametro del kernel `splash=0` alla configurazione del boot loader in uso. Per ulteriori informazioni, vedere il Capitolo 29, *Boot Loader* (p. 463). Se tuttavia si preferisce la modalità testo, di default nelle versioni precedenti, impostare `vga=normal`.

Disabilitazione completa della schermata SUSE.
Compilare un nuovo kernel e disabilitare l'opzione *Utilizza schermata di avvio invece del logo di avvio* nel *Supporto framebuffer*.

SUGGERIMENTO

La disabilitazione del supporto framebuffer nel kernel disabilita automaticamente anche la schermata di avvio. SUSE non può fornire alcun supporto al sistema in uso se lo si esegue con un kernel personalizzato.

29.8 Risoluzione dei problemi

In questa sezione vengono elencati alcuni dei problemi più frequentemente riscontrati durante l'avvio mediante GRUB e una breve descrizione delle possibili soluzioni. Alcuni dei problemi sono trattati all'interno di articoli del database del supporto tecnico all'indirizzo `http://portal.suse.de/sdb/en/index.html` (in lingua inglese). Se il problema specifico riscontrato non è presente in questo elenco, utilizzare la finestra di dialogo di ricerca del database del supporto tecnico all'indirizzo `https://`

portal.suse.com/PM/page/search.pm (in lingua inglese) per cercare parole chiave come *GRUB*, *boot* e *boot loader*.

GRUB e XFS

Con XFS non viene lasciato alcuno spazio per `stage1` nel blocco di avvio della partizione. Pertanto, evitare di specificare una partizione XFS come posizione del boot loader. È possibile risolvere questo problema creando una partizione di avvio separata non formattata con XFS.

GRUB e JFS

Anche se tecnicamente possibile, la combinazione di GRUB e JFS è problematica. In questo caso, creare una partizione di avvio separata (`/boot`) e formattarla con Ext2. Installare GRUB in questa partizione.

GRUB riporta un errore GRUB Geom Error

In GRUB viene verificata la geometria dei dischi rigidi connessi quando il sistema è avviato. Talvolta, il BIOS restituisce informazioni non coerenti e GRUB segnala un errore GRUB Geom Error. In questo caso, utilizzare LILO o aggiornare il BIOS. Per ulteriori informazioni sull'installazione, la configurazione e la manutenzione di LILO, consultare il database del supporto tecnico sotto la voce LILO.

Questo messaggio di errore viene restituito da GRUB anche se Linux è installato su un disco rigido aggiuntivo non registrato nel BIOS. *stage1* del boot loader viene trovato e caricato correttamente ma *stage2* non viene trovato. Questo problema può essere risolto mediante la registrazione del nuovo disco rigido nel BIOS.

Impossibile avviare il sistema contenente dischi rigidi IDE e SCSI

Durante l'installazione, è possibile che la sequenza di avvio dei dischi rigidi non sia stata determinata correttamente da YaST e che l'utente non l'abbia corretta. Ad esempio, è possibile che GRUB consideri `/dev/hda` come `hd0` e `/dev/sda` come`hd1`, anche se nel BIOS la sequenza di avvio è invertita (SCSI *prima* di IDE).

In questo caso, correggere i dischi rigidi durante il processo di avvio tramite la riga di comando di GRUB. Dopo l'avvio del sistema, modificare il file `device.map` per applicare la nuova mappatura permanentemente. Controllare quindi i nomi dei dispositivi di GRUB nei file `/boot/grub/menu.lst` e `/boot/grub/device.map` e reinstallare il boot loader con il comando seguente:

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

Avvio di Windows dal secondo disco rigido

Alcuni sistemi operativi, ad esempio Windows, possono eseguire l'avvio solo dal primo disco rigido. Se uno di questi sistemi operativi è installato su un disco rigido diverso dal primo, è possibile effettuare una modifica logica per la voce di menu corrispondente.

```
...
title windows
map (hd0) (hd1)
map (hd1) (hd0)
chainloader(hd1,0)+1
...
```

In questo esempio, Windows viene avviato dal secondo disco rigido. A questo scopo, l'ordine logico dei dischi rigidi viene modificato con `map`. Tale modifica non influisce sulla logica all'interno del file di menu di GRUB. Il secondo disco rigido pertanto deve essere specificato per `chainloader`.

29.9 Ulteriori informazioni

Informazioni approfondite su GRUB sono disponibili all'indirizzo http://www.gnu.org/software/grub/ (in lingua inglese). Se nel computer in uso è installato texinfo, consultare le pagine informative su GRUB in una shell immettendo `info grub` . È inoltre possibile eseguire una ricerca in base alla parola chiave «GRUB» nel database del supporto tecnico all'indirizzo http://portal.suse.de/sdb/en/index.html (in lingua inglese) per informazioni su problemi particolari.

30 Funzioni speciali di SUSE Linux

La prima parte del presente capitolo descrive i vari pacchetti software, le console virtuali e il layout della tastiera. Vengono trattati i componenti software come `bash`, `cron` e `logrotate`, nella misura in cui sono stati modificati o migliorati nelle versioni più recenti. Sebbene si tratti di software secondari, è utile modificarne il comportamento poiché lavorano a stretto contatto con il sistema. Il capitolo si conclude con una sezione dedicata alle impostazioni internazionali e della lingua (I18N e L10N).

30.1 Informazioni sui pacchetti di software speciali

I programmi `bash`, `cron`, `logrotate`, `locate`, `ulimit` e `free`, e il file `resolv.conf` sono molto importanti per gli amministratori di sistema e per molti utenti. La documentazione e le pagine info sono due fonti utili, ma non sempre disponibili, di informazioni. GNU Emacs è un editor di testo diffuso e molto flessibile.

30.1.1 Il pacchetto bash e il file /etc/profile

Il pacchetto Bash è la shell di default in SUSE Linux. Se usato come shell di login, esso legge numerosi file di inizializzazione. Bash li elabora nell'ordine in cui compaiono in questo elenco.

1. `/etc/profile`

2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Le impostazioni personalizzate possono essere effettuate nei file `~/.profile` o `~/.bashrc`. Per garantire l'elaborazione corretta di questi file, è necessario copiare le impostazioni di base dal file `/etc/skel/.profile` o `/etc/skel/.bashrc` nella home directory dell'utente. Dopo un aggiornamento, si consiglia di copiare le impostazioni da `/etc/skel`. Per evitare la perdita di impostazioni personalizzate, eseguire i seguenti comandi della shell:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Quindi copiare le impostazioni personalizzate dai file `*.old`.

30.1.2 Il pacchetto cron

cron è lo strumento classico per eseguire comandi su base regolare e automatica in background. cron è controllato da tabelle orarie formattate in modo speciale. Alcune di esse vengono fornite con il sistema, altre possono essere generate dall'utente stesso.

Le tabelle cron si trovano in `/var/spool/cron/tabs`. Il file `/etc/crontab` funge da tabella cron globale. Immettere il nome dell'utente che deve eseguire il comando direttamente dopo la tabella oraria. Nell'esempio riportato in Esempio 30.1, «Esempio di voce nel file /etc/crontab» (p. 488), è stato immesso `root`. Lo stesso formato si applica alle tabelle specifiche al pacchetto ubicate in `/etc/cron.d`. Vedere la documentazione su `cron` (comando `man cron`).

Esempio 30.1 *Esempio di voce nel file /etc/crontab*

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Non è possibile modificare il file `/etc/crontab` tramite chiamata del comando `crontab -e`. Questo file deve essere direttamente caricato in un editor, modificato, quindi salvato.

Numerosi pacchetti installano degli script di shell nelle directory `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly`; le istruzioni di tali script sono controllate da `/usr/lib/cron/run-crons`. Il file `/usr/lib/cron/run-crons` viene eseguito ogni 15 minuti dalla tabella principale (`/etc/crontab`). In questo modo, si è sicuri che i processi eventualmente sfuggiti possano essere eseguiti all'orario corretto.

Per eseguire gli script `hourly`, `daily` o altri script di manutenzione periodica a orari personalizzati, rimuovere i file di registrazione dell'orario associati a voci nel file `/etc/crontab`. Vedere l'esempio Esempio 30.2, «/etc/crontab: rimozione dei file di registrazione dell'orario» (p. 489) in cui è stato rimosso lo script `hourly` prima dello scadere di ogni ora, lo script `daily` una volta al giorno alle 02:14, ecc.).

Esempio 30.2 */etc/crontab: rimozione dei file di registrazione dell'orario*

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

I lavori di manutenzione quotidiana del sistema sono stati distribuiti tra vari script per motivi di chiarezza. Questi si trovano nel pacchetto `aaa_base`. `/etc/cron.daily` contiene, ad esempio, i componenti `suse.de-backup-rpmdb`, `suse.de-clean-tmp` o `suse.de-cron-local`.

30.1.3 File di log: pacchetto logrotate

Esistono dei servizi di sistema (*daemon*) che, assieme al kernel, registrano regolarmente lo stato del sistema e specifici eventi nei file di log. In questo modo, l'amministratore può controllare lo stato del sistema in determinati momenti, identificare errori o guasti e risolverli in modo preciso. Questi file di log sono normalmente memorizzati in `/var/log` come specificato in FHS (File System Hierarchy) e la loro dimensione cresce regolarmente. Il pacchetto `logrotate` consente di controllare la crescita di questi file.

Configurazione

logrotate può essere configurato tramite il file `/etc/logrotate.conf`. In particolare, la variabile di sistema `include` indica gli ulteriori file da leggere. In SUSE Linux, i programmi che generano file di log installano i propri file di configurazione

in /etc/logrotate.d. Ad esempio, tali programmi sono inclusi nei pacchetti apache2 (/etc/logrotate.d/apache2) e syslogd (/etc/logrotate.d/syslog).

Esempio 30.3 *Esempio di /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotate è controllato da un cron e viene quotidianamente chiamato da /etc/cron.daily/logrotate.

IMPORTANTE

L'opzione create legge tutte le impostazioni effettuate dall'amministratore in /etc/permissions*. Accertarsi che non si verifichino conflitti da modifiche personali.

30.1.4 Il comando locate

locate, un comando per trovare velocemente dei file, non è incluso nell'installazione di default del software. Se desiderato, è possibile installare il pacchetto find-locate.

Il processo updatedb viene avviato automaticamente tutte le notti o 15 minuti circa dopo l'avvio.

30.1.5 Il comando ulimit

Grazie al comando `ulimit` (*limiti utente*), è possibile impostare limiti all'utilizzo delle risorse di sistema nonché visualizzare gli stessi. `ulimit` è particolarmente utile per limitare la memoria disponibile per le applicazioni. Con questo comando, è possibile impedire l'utilizzo di eccessiva memoria da parte di un'applicazione con possibile conseguente blocco del sistema.

Il comando `ulimit` può essere usato con varie opzioni: Per limitare l'utilizzo della memoria, usare le opzioni elencate in Tabella 30.1, «Comando `ulimit`: impostazione delle risorse per l'utente» (p. 491).

Tabella 30.1 *Comando ulimit: impostazione delle risorse per l'utente*

`-m`	Dimensione massima della memoria fisica
`-v`	Dimensione massima della memoria virtuale
`-s`	Dimensione massima dello stack
`-c`	Dimensione massima dei file di base
`-a`	Visualizzazione dei limiti impostati

Le impostazioni globali possono essere definite in `/etc/profile`. In questo ambito, abilitare la creazione dei file di base richiesti dai programmatori per il *debug*. Un utente normale non può aumentare i valori specificati in `/etc/profile` dall'amministratore di sistema, ma può inserire voci speciali in `~/.bashrc`.

Esempio 30.4 *Comando ulimit: impostazioni in ~/.bashrc*

```
# Limits of physical memory:
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

Le quantità di memoria devono essere specificate in KB. Per ulteriori informazioni, vedere `man bash`.

IMPORTANTE

Le direttive del comando `ulimit` non sono supportate da tutte le shell. PAM (ad esempio `pam_limits`) offre ampie possibilità di regolazione delle impostazioni per queste restrizioni.

30.1.6 Il comando free

Il comando `free` non serve a determinare la quantità di RAM attualmente usata. Tali informazioni sono disponibili in `/proc/meminfo`. Oggigiorno, gli utenti che dispongono di moderni sistemi operativi, come Linux, non dovrebbero preoccuparsi della memoria. Il concetto di *RAM disponibile* risale a prima della gestione unificata della memoria. Lo slogan *memoria libera memoria cattiva* si adatta bene a Linux. Di conseguenza, Linux ha sempre rivolto gli sforzi nell'ottica di bilanciare la cache senza consentire di fatto la memoria libera o inutilizzata.

In realtà, il kernel non è collegato direttamente ad applicazioni o a dati utente. Invece, esso gestisce le applicazioni o i dati utente in una *cache di pagina*. In caso di memoria insufficiente, parti della cache vengono scritte nella partizione di scambio o in file da cui possono essere inizialmente lette tramite il comando `mmap` (vedere `man mmap`).

Il kernel contiene anche altre cache, come la *cache slab* che memorizza le cache per l'accesso alla rete. Ciò potrebbe spiegare le differenze tra i contatori in `/proc/meminfo`. La maggior parte, ma non tutti, sono accessibili tramite `/proc/slabinfo`.

30.1.7 Il file /etc/resolv.conf

La risoluzione del nome di dominio è gestita attraverso il file `/etc/resolv.conf`. Vedere il Capitolo 40, *DNS: Domain Name System* (p. 643).

Questo file è aggiornato esclusivamente dallo script `/sbin/modify_resolvconf`; nessun altro programma è autorizzato a modificare direttamente `/etc/resolv.conf`. L'applicazione di questa regola è l'unico mezzo per garantire che la configurazione di rete del sistema e i file pertinenti vengano mantenuti in uno stato coerente.

30.1.8 Documentazione e pagine info

Per alcune applicazioni GNU (come tar), la documentazione non è più aggiornata. Per questi comandi, usare l'opzione `--help` per ottenere una rapida panoramica delle pagine info, che offrono istruzioni più dettagliate. info è il sistema ipertestuale di GNU. Per visualizzare un'introduzione su questo sistema, immettere `info info`. Le pagine info possono essere visualizzate con Emacs digitando `emacs -f info` o direttamente in una console con `info`. Per visualizzare le pagine info, è possibile anche usare tkinfo, xinfo o il sistema della guida di SUSE.

30.1.9 Impostazioni per GNU Emacs

GNU Emacs è un ambiente di lavoro complesso. Le seguenti sezioni illustrano i file di configurazione elaborati all'avvio di GNU Emacs. Ulteriori informazioni sono disponibili all'indirizzo http://www.gnu.org/software/emacs/.

All'avvio Emacs legge numerosi file contenenti le impostazioni di personalizzazione o preconfigurazione relativi a utente, amministratore di sistema e distributore. Il file di inizializzazione `~/.emacs` è installato nelle home directory dei singoli utenti a partire da `/etc/skel`. Il file `.emacs` legge a sua volta il file `/etc/skel/.gnu-emacs`. Per personalizzare il programma, copiare il file `.gnu-emacs` nella home directory (con il comando `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) quindi apportare le impostazioni desiderate in tale directory.

Il file `.gnu-emacs` definisce il file `~/.gnu-emacs-custom` come `custom-file`. Se l'utente crea alcune impostazioni con le opzioni di `personalizzazione` di Emacs, le impostazioni vengono salvate nel file `~/.gnu-emacs-custom`.

Con SUSE Linux, il pacchetto `emacs` installa il file `site-start.el` nella directory `/usr/share/emacs/site-lisp`. Il file `site-start.el` viene caricato prima del file di inizializzazione `~/.emacs`. Tra l'altro, il file `site-start.el` assicura che i file di configurazione speciali distribuiti con i pacchetti aggiuntivi di Emacs, come `psgml`, vengano caricati automaticamente. I file di configurazione di questo tipo sono anch'essi collocati in `/usr/share/emacs/site-lisp` e iniziano sempre con `suse-start-`. L'amministratore di sistema locale può specificare impostazioni valide per l'intero sistema nel file `default.el`.

Ulteriori informazioni su questi file sono disponibili nel file info di Emacs nella sezione relativa al *file di inizializzazione*: `info:/emacs/InitFile`. Sempre in tale sezione sono disponibili istruzioni per disabilitare, se necessario, il caricamento di questi file.

I componenti di Emacs sono costituiti da più pacchetti:

- Il pacchetto base `emacs`.
- `emacs-x11` (di norma installato): il programma *con* supporto per X11.
- `emacs-nox`: il programma *senza* supporto per X11.
- `emacs-info`: documentazione in linea in formato info.
- `emacs-el`: i file di libreria non compilati in Emacs Lisp. Tali file non sono necessari in fase di runtime.
- Se necessario è possibile installare numerosi pacchetti aggiuntivi: `emacs-auctex` (per LaTeX), `psgml` (per SGML e XML), `gnuserv` (per il funzionamento del client e del server) e altri.

30.2 Console virtuali

Linux è un sistema multiutente e multitasking. I vantaggi di tali funzioni sono utili anche nei sistemi PC autonomi. In modalità testo, sono disponibili 6 console virtuali. Per passare dall'una all'altra, usare le combinazioni da Alt + F1 a Alt + F6. La settima console è riservata a X e la decima console mostra i messaggi del kernel. Per assegnare più o meno console, modificare il file `/etc/inittab`.

Per passare a una console da X senza spegnere, usare le combinazioni da Ctrl + Alt + F1 a Ctrl + Alt + F6. Per tornare a X, premere Alt + F7.

30.3 Mappatura della tastiera

Per standardizzare la mappatura della tastiera per i programmi, sono stati modificati i 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
```

Queste modifiche incidono solo sulle applicazioni che usano le voci di `terminfo` o quelle i cui file di configurazione vengono modificati direttamente (tramite i comandi `vi`, `less`, ecc.). Le applicazioni non fornite con SUSE Linux devono essere adattate a questi valori di default.

In ambiente X, il tasto compose (multitasto) è accessibile tramite Ctrl + Maiusc (destro). Esaminare anche la voce corrispondente in `/usr/X11R6/lib/X11/Xmodmap`.

Ulteriori impostazioni sono possibili tramite XKB (X Keyboard Extension). Questa estensione viene anche usata dagli ambienti desktop GNOME (gswitchit) e KDE (kxkb).

SUGGERIMENTO: Per ulteriori informazioni

Informazioni su XKB sono disponibili in `/etc/X11/xkb/README` e nei documenti citati in quel file.

Informazioni dettagliate sull'immissione di cinese, giapponese e coreano (CJK) sono disponibili nella pagina di Mike Fabian all'indirizzo: http://www.suse.de/~mfabian/suse-cjk/input.html.

30.4 Impostazioni internazionali e della lingua

SUSE Linux è in larga misura internazionalizzato e può essere modificato in base alle esigenze locali. In altre parole, l'internazionalizzazione (*I18N*) consente di operare specifiche localizzazioni (*L10N*). Le abbreviazioni I18N e L10N derivano dalla prima e ultima lettera delle parole e in mezzo il numero di lettere che le separano.

Le impostazioni possono applicate tramite le variabili `LC_` definite nel file `/etc/sysconfig/language`. Le impostazioni non controllano solo il *supporto della*

lingua, ma anche le categorie *Messaggi* (lingua), *Set di caratteri*, *Ordinamento*, *ora e data*, *Numeri* e *Valuta*. Ciascuna di queste categorie può essere definita direttamente con la sua variabile o indirettamente con una variabile globale nel file `language`; consultare la pagina disponibile tramite il comando `locale`.

RC_LC_MESSAGES, RC_LC_CTYPE, RC_LC_COLLATE, RC_LC_TIME, RC_LC_NUMERIC, RC_LC_MONETARY
: Queste variabili vengono trasferite alla shell senza il prefisso `RC_` e rappresentano le categorie elencate. I profili della shell interessati sono elencati sotto. Per visualizzare l'impostazione attuale usare il comando `locale`.

RC_LC_ALL
: Se impostata, questa variabile sovrascrive i valori delle variabili già dichiarate.

RC_LANG
: Questa variabile è il valore alternativo se nessun'altra è impostata. Per default, SUSE Linux imposta solo `RC_LANG` in modo da consentire una semplice personalizzazione dei valori.

ROOT_USES_LANG
: Questa variabile è controllata da `yes` o `no`. Se è impostata su `no`, `root` lavorerà sempre nell'ambiente POSIX.

Le altre variabili possono essere impostate tramite l'editor sysconfig YaST (vedere la Sezione 28.3.1, «Modifica della configurazione del sistema con l'editor di sysconfig fornito da YaST» (p. 459)). Il valore di una tale variabile contiene il codice lingua, il codice paese, la codifica e il modificatore. I singoli componenti sono collegati da caratteri speciali:

```
LANG=<lingua>[[_<paese>].<codifica>[@<Modificatore>]]
```

30.4.1 Alcuni esempi

I valori di lingua e paese devono sempre essere impostati insieme. L'impostazione della lingua è conforme allo standard ISO 639 disponibile all'indirizzo `http://www.evertype.com/standards/iso639/iso639-en.html` e all'indirizzo `http://www.loc.gov/standards/iso639-2/`. L'elenco dei codici paese è disponibile nella pagina su ISO 3166 all'indirizzo `http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html`.

I valori validi sono quelli per i quali è disponibile un file di definizione nella directory `/usr/lib/locale`. È possibile creare ulteriori file di definizione a partire dai file nella directory `/usr/share/i18n` usando il comando `localedef`. I file di definizione fanno parte del pacchetto `glibc-i18ndata`. Un file di definizione per `it_IT.UTF-8` (italiano e Italia) può essere creato con:

```
localedef -i it_IT -f UTF-8 it_IT.UTF-8
```

`LANG=it_IT.UTF-8`
: Questa è l'impostazione di default se si seleziona Italiano Italia durante l'installazione. È possibile selezionare un'altra lingua, ma la codifica dei caratteri UTF-8 rimarrà invariata.

`LANG=it_IT.ISO-8859-1`
: Questo valore imposta la lingua su Italiano, il paese su Italia e il set di caratteri su `ISO-8859-1`. Questo set di caratteri non supporta il simbolo dell'euro ma è utile con i programmi non aggiornati al supporto della codifica `UTF-8`. La stringa che definisce il set di caratteri (in questo caso `ISO-8859-1`) viene valutata da programmi come Emacs.

`LANG=it_IT@euro`
: L'esempio precedente include in modo esplicito il simbolo Euro in un'impostazione di lingua. In pratica, questa impostazione è ormai obsoleta poiché la codifica UTF-8 attuale copre il simbolo Euro. È utile solo per quelle applicazioni senza supporto UTF-8 e con supporto ISO-8859-15.

SuSEconfig legge le variabili in `/etc/sysconfig/language` e scrive le modifiche necessarie in `/etc/SuSEconfig/profile` e in `/etc/SuSEconfig/csh.cshrc`. I valori di `/etc/SuSEconfig/profile` vengono letti o *estratti* da `/etc/profile`. I valori di `/etc/SuSEconfig/csh.cshrc` vengono estratti da `/etc/csh.cshrc`. In questo modo, le impostazioni sono disponibili in tutto il sistema.

Gli utenti possono sovrascivere i valori di default del sistema modificando il file `~/.bashrc`. Se ad esempio non si desidera usare il valore globale `it_IT` per i messaggi dell'interfaccia, includere `LC_MESSAGES=es_ES` in modo da visualizzarli in Spagnolo.

30.4.2 Impostazioni del supporto della lingua

I file della categoria *Messaggi* devono di regola essere sempre memorizzati nella directory della lingua corrispondente (come `it`), altrimenti non possono essere letti. Se si imposta `LANG` su `it_IT` e il file dei messaggi in `/usr/share/locale/it_IT/LC_MESSAGES` non esiste, viene estratto per impostazione di default il valore di `/usr/share/locale/en/LC_MESSAGES`.

È inoltre possibile definire una sequenza di valori alternativi, ad esempio, da bretone a francese, da catalano a spagnolo poi a portoghese:

```
LANGUAGE="br_FR:fr_FR"

LANGUAGE="gl_ES:es_ES:pt_PT"
```

Un altro esempio è dato dalle varianti Nynorsk e Bokmål del norvegese (con valore alternativo `no`):

```
LANG="nn_NO"

LANGUAGE="nn_NO:nb_NO:no"
```

oppure

```
LANG="nb_NO"

LANGUAGE="nb_NO:nn_NO:no"
```

Notare che in norvegese, anche la variabile `LC_TIME` viene impostata in modo diverso.

Uno dei problemi che possono sorgere è rappresentato dal separatore usato per delimitare gruppi di numeri che non vengono riconosciuti correttamente. Ciò si verifica se `LANG` viene impostato con un singolo codice lingua come `de`, e se il file di definizione glibc usato è ubicato in `/usr/share/lib/de_DE/LC_NUMERIC`. Di conseguenza, la variabile `LC_NUMERIC` deve essere impostata su `de_DE` in modo che la definizione del separatore possa essere letta dal sistema.

30.4.3 Ulteriori informazioni

- *Il manuale GNU C Library Reference*, capitolo «Locales and Internationalization». È disponibile in `glibc-info`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux (Domande frequenti su UTF-8 e Unicode per Unix/Linux),* all'indirizzo `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Unicode-Howto*, di Bruno Haible: `/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

31 Uso della stampante

CUPS (Common Unix Printing System) è il sistema di stampa standard in SUSE Linux ed è nettamente orientato all'utente. In molti casi è compatibile con lo spooler LPRng o può essere adattato senza problemi. LPRng è incluso in SUSE Linux solo per motivi di compatibilità.

Le stampanti possono essere distinte in base all'interfaccia, USB o di rete, e al linguaggio della stampante. Quando si acquista una stampante, è necessario verificare che disponga di un'interfaccia supportata dall'hardware e di un linguaggio appropriato. È possibile classificare le stampanti sulla base di tre classi di linguaggi per le stampanti:

Stampanti PostScript
PostScript è il linguaggio per stampanti utilizzato dal sistema di stampa interno per generare ed elaborare la maggior parte dei lavori di stampa in Linux e Unix. Questo linguaggio è in uso da molto tempo ed è estremamente efficiente. Se i documenti PostScript possono essere elaborati direttamente dalla stampante e non devono essere convertiti con passaggi aggiuntivi nel sistema di stampa, le possibili cause di errore si riducono. Poiché le stampanti PostScript sono soggette a costi di licenza, queste stampanti hanno in genere un costo maggiore rispetto a quelle che non dispongono di un interprete PostScript.

Stampante standard (linguaggi quali PCL e ESC/P)
Sebbene questi linguaggi per stampanti siano alquanto datati, stanno subendo un processo di espansione per poter gestire le nuove funzionalità disponibili nelle stampanti. Nel caso di linguaggi per stampanti conosciuti, il sistema di stampa può convertire i lavori PostScript nei rispettivi linguaggi per stampante con il supporto di Ghostscript. Questa fase di elaborazione viene definita interpretazione. I linguaggi più conosciuti sono PCL, utilizzato principalmente dalle stampanti HP e dai relativi

cloni, ed ESC/P, utilizzato dalle stampanti Epson. Questi linguaggi per stampanti sono in genere supportati da Linux e consentono di ottenere risultati di stampa validi. Linux potrebbe non essere in grado di gestire alcune funzionalità di stampanti estremamente innovative o sofisticate poiché è possibile che gli sviluppatori open source stiano ancora esaminando tali funzionalità. Ad eccezione dei driver `hpijs` sviluppati da HP, attualmente non esistono produttori di stampanti che sviluppano driver Linux e li rendono disponibili per i distributori Linux con licenza open source. La maggior parte di queste stampanti è collocata in una fascia di prezzi intermedia.

Stampanti proprietarie (in genere stampanti GDI)
Per le stampanti proprietarie sono in genere disponibili soltanto alcuni driver per Windows. Queste stampanti non supportano i normali linguaggi per stampanti e, quando viene rilasciata una nuova edizione di un modello, il linguaggio per stampanti in uso viene modificato. Per ulteriori informazioni, vedere Sezione 31.7.1, «Stampanti prive del supporto del linguaggio standard per stampanti» (p. 518).

Prima di acquistare una nuova stampante, è consigliabile consultare le seguenti fonti per verificare il livello di supporto della stampante desiderata:

- `http://cdb.suse.de/`—database della stampante SUSE Linux
- `http://www.linuxprinting.org/`—database della stampante LinuxPrinting.org
- `http://www.cs.wisc.edu/~ghost/`—pagina Web di Ghostscript
- `/usr/share/doc/packages/ghostscript/catalog.devices`—elenco dei driver inclusi

Nei database in linea è sempre indicato lo stato di supporto Linux più recente. In una distribuzione Linux, tuttavia, possono essere integrati solo i driver disponibili in fase di produzione. Una stampante attualmente classificata come «interamente supportata» potrebbe pertanto non aver presentato questo stato al momento del rilascio dell'ultima versione di SUSE Linux. Nei database potrebbe quindi non essere indicato lo stato corretto, ma solo un'approssimazione.

31.1 Workflow del sistema di stampa

L'utente crea un lavoro di stampa, costituito dai dati da stampare, dalle informazioni per lo spooler, quali il nome della stampante o il nome della coda di stampa e, facoltativamente, dalle informazioni per il filtro, quali le opzioni specifiche per la stampante.

Per ogni stampante è disponibile una coda di stampa dedicata. Il lavoro di stampa viene inserito nella coda dallo spooler fino a quando la stampante desiderata sarà pronta per ricevere dati. Quando la stampante è pronta, i dati vengono inviati dallo spooler tramite il filtro e il back-end alla stampante.

Il filtro converte i dati che l'utente desidera stampare (ASCII, PostScript, PDF, JPEG e così via) in dati specifici per la stampante (PostScript, PCL, ESC/P e così via). Le funzionalità della stampante sono descritte nei file PPD, in cui sono incluse opzioni specifiche della stampante con i parametri necessari per abilitarle nella stampante. Il sistema di filtri assicura che le opzioni selezionate dagli utenti siano abilitate.

Se si utilizza una stampante PostScript, il sistema di filtri converte i dati nel linguaggio PostScript pertanto non è necessario un driver della stampante. Se si utilizza una stampante non PostScript, i dati vengono convertiti in dati specifici per la stampante tramite Ghostscript. A questo scopo è necessario un driver della stampante Ghostscript adatto alla stampante in uso. Il back-end riceve i dati specifici per la stampante dal filtro e li passa alla stampante.

31.2 Metodi e protocolli per la connessione delle stampanti

Una stampante può essere connessa al sistema in vari modi. La configurazione del sistema di stampa CUPS non opera distinzioni tra una stampante locale e una stampante connessa al sistema tramite la rete. In Linux le stampanti locali devono essere collegate in base alle indicazioni specificate nel manuale fornito dal produttore. CUPS supporta collegamenti seriali, USB, paralleli e SCSI. Per ulteriori informazioni sulla connessione della stampante, leggere l'articolo *CUPS in a Nutshell* (in lingua inglese) nel database

del supporto tecnico all'indirizzo http://portal.suse.com. Per trovare l'articolo, immettere *cups* nella finestra di dialogo di ricerca.

AVVERTIMENTO: Collegamento via cavo al computer

Quando si collega la stampante al computer, è necessario tenere presente che solo i dispositivi USB possono essere collegati o scollegati mentre il computer è in funzione. Prima di modificare altri tipi di collegamento è necessario spegnere il sistema.

31.3 Installazione del software

PPD (PostScript Printer Description) è il linguaggio per computer che descrive le proprietà, quali la risoluzione, e le opzioni, ad esempio la disponibilità di un'unità fronte/retro. Queste descrizioni sono necessarie per l'utilizzo di numerose opzioni della stampante in CUPS. Senza un file PPD i dati di stampa verrebbero inviati alla stampante in uno stato «non elaborato», solitamente sconsigliato. Durante l'installazione di SUSE Linux, molti file PPD vengono preinstallati per consentire l'utilizzo anche delle stampanti senza supporto PostScript.

Per configurare una stampante PostScript, l'approccio migliore consiste nell'ottenere un file PPD appropriato. Molti file PPD sono disponibili nel pacchetto `manufacturer-PPDs`, installato automaticamente durante il processo di installazione standard. Vedere Sezione 31.6.3, «File PPD in vari pacchetti» (p. 515) e Sezione 31.7.2, «Nessun file PPD appropriato disponibile per una stampante PostScript» (p. 519).

È possibile memorizzare nuovi file PPD nella directory `/usr/share/cups/model/` o aggiungerli al sistema di stampa tramite YaST (vedere sezione chiamata «Configurazione manuale» (p. 506)). Sarà successivamente possibile selezionare il file PPD durante l'installazione.

Se un produttore di stampanti richiede l'installazione di interi pacchetti software oltre alla modifica dei file di configurazione, prestare estrema attenzione poiché questo tipo di installazione determinerebbe la perdita del supporto fornito da SUSE Linux, inoltre i comandi di stampa potrebbero funzionare diversamente e il sistema potrebbe non essere più in grado di gestire dispositivi di altri produttori. Per questo motivo non è consigliabile installare il software del produttore.

31.4 Configurazione della stampante

Dopo aver collegato la stampante al computer e aver installato il software, installare la stampante nel sistema. Questa operazione deve essere eseguita tramite gli strumenti inclusi in SUSE Linux. Poiché la sicurezza è un aspetto prioritario in SUSE Linux, gli strumenti di terze parti hanno spesso difficoltà a superare le restrizioni di sicurezza e in genere causano più disagi che vantaggi. Per ulteriori informazioni sulla risoluzione dei problemi, vedere Sezione 31.6.1, «Server e firewall CUPS» (p. 512) e Sezione 31.6.2, «Modifiche del sistema di stampa CUPS» (p. 513).

31.4.1 Stampanti locali

Se quando si esegue il login viene rilevata una stampante locale non configurata, YaST viene avviato per eseguirne la configurazione. In questo processo vengono utilizzate le stesse finestre di dialogo indicate nella descrizione della configurazione seguente.

Per configurare la stampante, selezionare *Hardware* → *Stampante* nel centro di controllo YaST. In questo modo viene aperta la finestra principale di configurazione della stampante in cui sono elencati i dispositivi rilevati nella parte superiore. Nella parte inferiore sono elencate eventuali code configurate in precedenza. Se la stampante non viene rilevata, configurarla manualmente.

IMPORTANTE

Se la voce *Stampante* non è disponibile nel centro di controllo YaST, il pacchetto `yast2-printer` potrebbe non essere stato installato. Per risolvere il problema, installare il pacchetto `yast2-printer` e riavviare YaST.

Configurazione automatica

YaST consente di configurare automaticamente la stampante se è possibile impostare automaticamente la porta parallela o USB e la stampante collegata viene rilevata. Il database della stampante deve inoltre contenere la stringa ID della stampante recuperata da YaST durante il rilevamento automatico dell'hardware. Se l'ID dell'hardware è diverso da quello richiesto per il modello specifico, selezionare il modello manualmente.

Per verificare che tutto funzioni correttamente, è necessario controllare ogni configurazione mediante la funzionalità di test di stampa in YaST. Nella pagina di prova sono inoltre incluse informazioni importanti sulla configurazione testata.

Configurazione manuale

Se i requisiti per la configurazione automatica non sono soddisfatti o si desidera definire una configurazione personalizzata, configurare la stampante manualmente. In base ai risultati del rilevamento automatico e alle informazioni relative al modello della stampante disponibili nel database, è possibile che le impostazioni corrette vengano determinate automaticamente in YaST o che venga effettuata una preselezione plausibile.

È necessario configurare i seguenti parametri:

Connessione hardware (porta)
: La configurazione della connessione hardware dipende dall'esito del rilevamento automatico in YaST, ovvero se la stampante è stata rilevata. Se il modello della stampante viene rilevato automaticamente, è possibile presumere che la connessione alla stampante funzioni correttamente a livello hardware e pertanto non è necessario modificare le impostazioni. In caso contrario, potrebbero verificarsi problemi di connessione a livello hardware. In questo caso è necessario un intervento manuale per configurare la connessione.

  Nella finestra di dialogo *Configurazione della stampante* premere *Configura* per avviare il workflow di configurazione manuale. Selezionare il *Tipo di stampante*, ad esempio `Stampante USB` e, dopo aver selezionato *Avanti*, specificare il tipo di *Collegamento stampante* e selezionare il dispositivo.

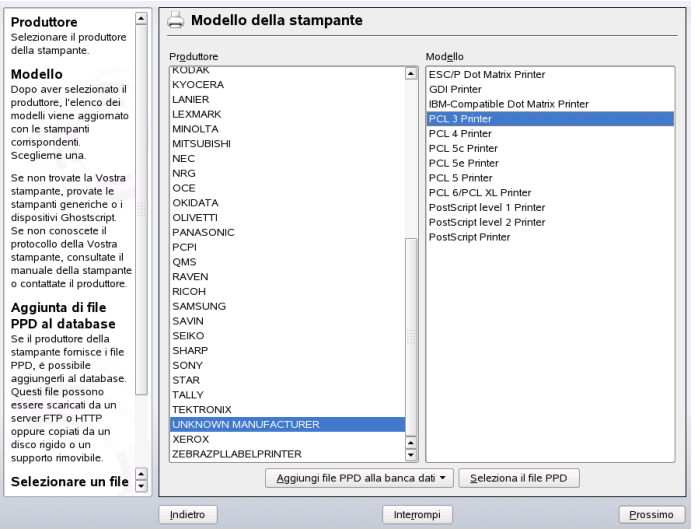
Nome della coda
: Il nome della coda viene utilizzato per l'invio di comandi di stampa. Il nome deve essere relativamente breve ed essere composto solo da lettere minuscole e numeri. Immettere *Nome per la stampa* nella finestra di dialogo successiva, ovvero *Nome della coda*.

Modello della stampante e file PPD
: Tutti i parametri specifici della stampante, ad esempio il driver Ghostscript da utilizzare e i parametri di filtro della stampante per il driver, sono memorizzati in un file PPD (PostScript Printer Description). Per ulteriori informazioni sui file PPD, vedere Sezione 31.3, «Installazione del software» (p. 504).

Per molti modelli di stampante sono disponibili diversi file PPD utilizzati, ad esempio, se più driver Ghostscript interagiscono con il modello specifico. Quando si seleziona un produttore e un modello nella finestra di dialogo successiva, ovvero *Modello della stampante*, in YaST viene selezionato il file PPD corrispondente alla stampante. Se sono disponibili diversi file PPD per il modello, uno di essi viene utilizzato come impostazione di default, in genere quello contrassegnato come `consigliato`. Il file PPD selezionato può essere modificato nella finestra di dialogo successiva mediante l'opzione *Modifica*.

Per i modelli non PostScript, tutti i dati specifici della stampante vengono generati dal driver Ghostscript. Per questo motivo la configurazione del driver è il fattore più importante per determinare la qualità dell'output. La stampa dipende dal tipo di driver Ghostscript (file PPD) selezionato e dalle opzioni specificate per tale driver. Se necessario, modificare altre opzioni disponibili nel file PPD dopo aver selezionato *Modifica*.

Figura 31.1 *Selezione del modello della stampante*



Verificare sempre se le impostazioni specificate consentono di ottenere i risultati previsti stampando una pagina di prova. Se l'output è impreciso, ad esempio con alcune pagine quasi vuote, terminare la stampa rimuovendo innanzitutto tutta la carta dalla stampante e quindi interrompendo il test tramite YaST.

Se il database della stampante non include una voce per il modello in uso, è possibile aggiungere un nuovo file PPD selezionando *Aggiungi file PPD alla banca dati* o utilizzare una raccolta di file PPD generici per consentire l'utilizzo della stampante con uno dei linguaggi standard per stampante. A questo scopo, selezionare *Produttore sconosciuto* come produttore della stampante.

Impostazioni avanzate
In genere non è necessario modificare queste impostazioni.

31.4.2 Stampanti di rete

Una stampante di rete può supportare vari protocolli simultaneamente. Sebbene la maggior parte dei protocolli sia standardizzata, alcuni produttori espandono o modificano lo standard perché testano sistemi non implementati correttamente nello standard o perché desiderano offrire determinate funzioni non presenti nello standard. I produttori forniscono quindi i driver solo per alcuni sistemi operativi, eliminando così le difficoltà relative a tali sistemi. Purtroppo i driver Linux spesso non vengono forniti. È consigliabile pertanto non presupporre che ogni protocollo funzioni correttamente in Linux e provare varie opzioni per poter ottenere una configurazione valida.

In CUPS sono supportati i protocolli `socket`, `LPD`, `IPP` e `SMB`. Di seguito sono fornite alcune informazioni dettagliate su tali protocolli:

socket
Il protocollo *socket* fa riferimento a una connessione in cui i dati vengono inviati a un socket Internet senza un preliminare handshake dei dati. Tra i numeri di porta del socket comunemente utilizzati vi sono `9100` e `35`. Un esempio di URI di dispositivo è `socket://host-printer:9100/`.

LPD (Line Printer Daemon)
Il collaudato protocollo LPD è descritto in RFC 1179. Tramite questo protocollo, alcuni dati relativi al lavoro, ad esempio l'ID della coda di stampa, vengono inviati prima dei dati effettivi da stampare. È pertanto necessario specificare una coda di stampa durante la configurazione del protocollo LPD per la trasmissione di dati. Le implementazioni di diversi produttori di stampanti sono sufficientemente flessibili da consentire qualsiasi nome per la coda della stampante. Se necessario, nel manuale della stampante verrà indicato il nome da utilizzare. Spesso vengono utilizzati nomi quali LPT, LPT1, LP1 o simili. È anche possibile configurare una coda LPD in un

host Linux o Unix diverso nel sistema CUPS. Il numero di porta per un servizio LPD è `515`. Un esempio di URI di dispositivo è `lpd://host-printer/LPT1`.

IPP (Internet Printing Protocol)
IPP è un protocollo relativamente recente (1999) basato sul protocollo HTTP che consente di trasmettere una quantità maggiore di dati relativi al lavoro rispetto agli altri protocolli. Questo protocollo viene utilizzato in CUPS per la trasmissione di dati interna. È il protocollo consigliato per l'inoltro di code tra due server CUPS. Il nome della coda di stampa è necessario per configurare correttamente il protocollo IPP. Il numero di porta per IPP è `631`. Alcuni esempi di URI di dispositivo sono `ipp://host-printer/ps` e `ipp://host-cupsserver/printers/ps`.

SMB (condivisione Windows)
In CUPS è supportata anche la stampa tramite stampanti connesse a condivisioni Windows. Il protocollo utilizzato per questo scopo è SMB. I numeri di porta utilizzati da SMB sono `137`, `138` e `139`. Alcuni esempi di URI di dispositivo sono `smb://user:password@workgroup/server/printer`, `smb://user:password@host/printer` e `smb://server/printer`.

Il protocollo supportato dalla stampante deve essere stabilito prima della configurazione. Se il produttore non fornisce le informazioni necessarie, il comando `nmap`, incluso nel pacchetto `nmap`, può essere utilizzato per individuare il protocollo. Questo controllo verifica eventuali porte aperte in un host. Ad esempio:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

Configurazione di CUPS nella rete tramite YaST

È consigliabile configurare le stampanti di rete tramite YaST poiché semplifica la configurazione ed è progettato per gestire correttamente le restrizioni di protezione presenti in CUPS (vedere Sezione 31.6.2, «Modifiche del sistema di stampa CUPS» (p. 513)). Per istruzioni sull'installazione di CUPS nella rete, leggere l'articolo *CUPS in a Nutshell* (in lingua inglese) nel database del supporto tecnico all'indirizzo `http://portal.suse.com`.

Selezionare *Altro (non rilevato)* e fare clic su *Configura*. Se non indicato diversamente dall'amministratore di rete, provare l'opzione *Stampa direttamente tramite stampante di rete* e proseguire in base ai requisiti locali.

Configurazione con gli strumenti della riga di comando

In alternativa, CUPS può essere configurato con gli strumenti della riga di comando, quali `lpadmin` e `lpoptions`. È necessario un URI (Uniform Resource Identifier) di dispositivo formato da un back-end, ad esempio usb, e da parametri quali `/dev/usb/lp0`. L'URI completo potrebbe essere, ad esempio, `parallel:/dev/lp0` per una stampante connessa alla prima porta parallela o `usb:/dev/usb/lp0` per la prima stampante rilevata connessa alla porta USB.

`lpadmin` consente all'amministratore del server CUPS di aggiungere, rimuovere o gestire classi e code di stampa. Per aggiungere una coda di stampa, utilizzare la sintassi seguente:

```
lpadmin -p queue -v device-URI \
-P PPD-file -E
```

Il dispositivo (`-v`) sarà quindi disponibile come *`queue`* (`-p`), utilizzando il file PPD specificato (`-P`). È pertanto necessario specificare il file PPD e il nome del dispositivo per configurare manualmente la stampante.

Non utilizzare `-E` come prima opzione. Per tutti i comandi CUPS, specificando `-E` come primo argomento si imposta l'uso di una connessione cifrata. Per abilitare la stampante, è necessario utilizzare `-E` come illustrato nell'esempio seguente:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

Nell'esempio seguente viene configurata una stampante di rete:

```
lpadmin -p ps -v socket://192.168.1.0:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Per ulteriori opzioni di `lpadmin`, vedere la documentazione `lpadmin(1)`.

Durante l'installazione del sistema alcune opzioni vengono impostate per default. È tuttavia possibile modificare queste opzioni per ogni lavoro di stampa, a seconda dello strumento di stampa utilizzato. Queste opzioni di default possono inoltre essere modificare tramite YaST. Utilizzando gli strumenti della riga di comando, impostare le opzioni di default come segue:

1. Innanzitutto, elencare tutte le opzioni:

   ```
   lpoptions -p queue -l
   ```

Esempio:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

L'opzione di default attivata è contrassegnata dall'asterisco che la precede (*).

2 Modificare l'opzione con `lpadmin`:

```
lpadmin -p queue -o Resolution=600dpi
```

3 Controllare la nuova impostazione:

```
lpoptions -p queue -l

Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

Quando un utente comune esegue `lpoptions`, le impostazioni vengono scritte in `~/.lpoptions`. Le impostazioni `root` vengono scritte in `/etc/cups/lpoptions`.

31.5 Configurazione per le applicazioni

Le code di stampa esistenti vengono utilizzate dalle applicazioni nello stesso modo in cui vengono gestite dagli strumenti della riga di comando. In genere non è necessario riconfigurare la stampante per una determinata applicazione poiché dovrebbe essere possibile eseguire la stampa dalle applicazioni utilizzando le code esistenti.

Per stampare dalla riga di comando, immettere `lp -d` *`queuename filename`*, sostituendo i nomi corrispondenti a *`queuename`* e *`filename`*.

Alcune applicazioni utilizzano il comando `lp` per la stampa. In questo caso, immettere il comando corretto nella finestra di dialogo di stampa dell'applicazione, in genere senza specificare *`filename`*, ad esempio `lp -d` *`queuename`*. Nel caso di programmi KDE, abilitare *Print through an external program (Stampa tramite un programma esterno)*. In caso contrario non sarà possibile immettere il comando di stampa.

Gli strumenti quali xpp e il programma kprinter KDE forniscono un'interfaccia grafica per la scelta delle code e l'impostazione delle opzioni CUPS standard e delle opzioni specifiche per la stampante rese disponibili tramite il file PPD. È possibile utilizzare kprinter come interfaccia di stampa standard delle applicazioni non KDE specificando

`kprinter` o `kprinter --stdin` come comando di stampa nelle finestre di dialogo di stampa delle applicazioni. Il comportamento dell'applicazione determina quale dei due comandi scegliere. Se la configurazione è stata eseguita correttamente, la finestra di dialogo kprinter viene richiamata ogni volta che nell'applicazione viene avviato un lavoro di stampa; pertanto sarà possibile utilizzare la finestra di dialogo per selezionare una coda e impostare altre opzioni di stampa. A questo scopo è necessario che le impostazioni di stampa dell'applicazione non siano in conflitto con quelle di kprinter e che le opzioni di stampa vengano modificate solo tramite kprinter, dopo averlo abilitato.

31.6 Funzionalità speciali in SUSE Linux

Alcune funzionalità di CUPS sono state adattate per SUSE Linux. Alcune delle modifiche più importanti sono illustrate in questa sezione.

31.6.1 Server e firewall CUPS

CUPS può essere configurato come client di un server di rete in vari modi.

1. Per ogni coda nel server di rete è possibile configurare una coda locale per l'inoltro di tutti i lavori al server di rete corrispondente. Questo approccio non è in genere consigliabile poiché tutti i computer client devono essere riconfigurati ogni volta che la configurazione del server di rete viene modificata.

2. I lavori di stampa possono anche essere inoltrati direttamente a un server di rete. Per questo tipo di configurazione non eseguire un daemon CUPS locale. `lp` o la chiamata alla libreria corrispondente di altri programmi possono inviare i lavori direttamente al server di rete. Tuttavia, questa configurazione non è valida se si desidera eseguire una stampa anche su una stampante locale.

3. Il daemon CUPS può ascoltare i pacchetti di diffusione IPP inviati da altri server di rete per segnalare code disponibili. Per utilizzare questo metodo, è necessario che la porta 631/UDP sia aperta per i pacchetti in entrata.

   Questa è la configurazione di CUPS più appropriata alla stampa su server CUPS remoti. Esiste tuttavia il rischio che un attaccante invii diffusioni IPP con code e che il daemon locale acceda a una coda contraffatta. Se tale coda viene quindi

visualizzata con lo stesso nome di un'altra coda presente nel server locale, il proprietario del lavoro può credere che il lavoro sia stato inviato a un server locale, mentre è stato inviato al server dell'attaccante.

I server CUPS possono essere individuati da YaST tramite una scansione di tutti gli host di rete per determinare se offrono questo servizio e mediante l'ascolto delle diffusioni IPP. La seconda procedura viene utilizzata durante l'installazione del sistema per individuare server CUPS adatti allo scopo. Per utilizzare questa procedura, è necessario che la porta 631/UDP sia aperta per i pacchetti in entrata. L'apertura di una porta per configurare l'accesso a code remote tramite la seconda procedura può costituire un rischio per la sicurezza poiché un attaccante potrebbe diffondere pacchetti a un server che potrebbe essere accettato dagli utenti.

L'impostazione di default del firewall illustrata nella finestra di dialogo di suggerimento consiste nel rifiutare le diffusioni IPP in qualsiasi interfaccia. Di conseguenza, la seconda procedura per il rilevamento delle code remote e la terza procedura per accedere alle code remote non possono essere utilizzate. La configurazione del firewall deve quindi essere modificata contrassegnando una delle interfacce come `interna`, scelta che determina l'apertura della porta per default, oppure aprendo esplicitamente la porta di un'interfaccia `esterna`. Per motivi di sicurezza, nessuna porta è aperta per default.

La configurazione del firewall proposta deve essere modificata per consentire a CUPS di rilevare le code remote durante l'installazione e l'accesso a server remoti dal sistema locale durante il normale funzionamento. In alternativa, l'utente può rilevare i server CUPS eseguendo attivamente una scansione degli host della rete locale o configurando manualmente tutte le code. Questa procedura non è tuttavia consigliata per i motivi illustrati all'inizio di questa sezione.

31.6.2 Modifiche del sistema di stampa CUPS

Queste modifiche sono state inizialmente applicate a SUSE Linux 9.1.

Esecuzione di cupsd come lp utente

All'avvio `cupsd` passa da `root` utente a `lp` utente. In questo modo viene garantito un livello di sicurezza nettamente più elevato poiché il servizio di stampa CUPS non

viene eseguito con autorizzazioni illimitate, ma solo con le autorizzazioni necessarie per il servizio di stampa.

L'autenticazione (controllo della password), tuttavia, non può essere eseguito tramite `/etc/shadow` poiché `lp` non ha accesso a `/etc/shadow`. È necessario quindi utilizzare l'autenticazione specifica per CUPS tramite `/etc/cups/passwd.md5`. A questo scopo è necessario immettere un amministratore CUPS con il gruppo di amministrazione CUPS `sys` e una password CUPS in `/etc/cups/passwd.md5`. Per eseguire questa operazione, immettere quanto segue come `root`:

```
lppasswd -g sys -a CUPS-admin-name
```

Questa impostazione è essenziale anche se si desidera utilizzare il front-end Web di amministrazione (CUPS) o lo strumento di amministrazione della stampante (KDE).

Quando `cupsd` viene eseguito come `lp`, `/etc/printcap` non può essere generato poiché `lp` non è autorizzato a creare file in `/etc/`. Pertanto `cupsd` genera `/etc/cups/printcap`. Per garantire che le applicazioni che possono leggere i nomi delle code solo da `/etc/printcap` continuino a funzionare correttamente, `/etc/printcap` è un collegamento simbolico che punta a `/etc/cups/printcap`.

Quando `cupsd` viene eseguito come `lp`, la porta `631` non può essere aperta. Non è quindi possibile ricaricare `cupsd` mediante `rccups reload`, ma è necessario utilizzare `rccups restart`.

Funzionalità generalizzate per `BrowseAllow` e `BrowseDeny`

Le autorizzazioni di accesso impostate per `BrowseAllow` e `BrowseDeny` si applicano a tutti i tipi di pacchetti inviati a `cupsd`. Di seguito sono riportate le impostazioni di default in `/etc/cups/cupsd.conf`:

```
BrowseAllow @LOCAL
BrowseDeny All
```

e

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
```

```
  Allow From @LOCAL
</Location>
```

In questo modo solo gli host `LOCAL` possono accedere a `cupsd` in un server CUPS. Con `LOCAL` vengono indicati gli host con indirizzi IP che appartengono a un'interfaccia non PPP (interfacce i cui flag `IFF_POINTOPOINT` non sono impostati) e con indirizzi IP che appartengono alla stessa rete del server CUPS. I pacchetti di tutti gli altri host vengono respinti immediatamente.

Attivazione di default di `cupsd`

In un'installazione standard, `cupsd` viene attivato automaticamente in modo da consentire l'accesso agevole alle code dei server di rete CUPS senza azioni manuali aggiuntive. Le voci in sezione chiamata «Esecuzione di cupsd come lp utente» (p. 513) e sezione chiamata «Funzionalità generalizzate per `BrowseAllow` e `BrowseDeny`» (p. 514) sono condizioni essenziali per questa funzionalità poiché senza di esse la sicurezza non sarebbe sufficiente per l'attivazione automatica di `cupsd`.

31.6.3 File PPD in vari pacchetti

Nella configurazione della stampante YaST vengono impostate le code per CUPS mediante i soli file PPD installati in `/usr/share/cups/model/` nel sistema. Per trovare i file PPD appropriati al modello della stampante in uso, in YaST vengono confrontati il fornitore e il modello determinati durante il rilevamento dell'hardware con i fornitori e i modelli in tutti i file PPD disponibili in `/usr/share/cups/model/` nel sistema. A questo scopo la configurazione della stampante YaST genera un database sulla base delle informazioni del fornitore e del modello estratte dai file PPD. Quando si seleziona una stampante dall'elenco di fornitori e modelli, si ricevono i file PPD corrispondenti a tale fornitore e modello.

La configurazione mediante i soli file PPD, senza altre fonti di informazione, ha il vantaggio che i file PPD in `/usr/share/cups/model/` possono essere modificati liberamente. La configurazione della stampante YaST è in grado di riconoscere le modifiche e rigenerare il database del fornitore e del modello. Se, ad esempio, si utilizzano solo stampanti PostScript, in genere i file PPD Foomatic del pacchetto `cups-drivers` o i file PPD Gimp-Print nel pacchetto `cups-drivers-stp` non sono necessari. Diversamente, i file PPD per le stampanti PostScript possono essere copiati direttamente in `/usr/share/cups/model/`, se non esistono già nel

pacchetto manufacturer-PPDs, per ottenere una configurazione ottimale per le stampanti in uso.

File PPD CUPS nel pacchetto cups

I file PPD generici nel pacchetto cups sono stati integrati con file PPD Foomatic adattati per le stampanti PostScript di livello 1 e 2:

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

File PPD nel pacchetto cups-drivers

Il filtro della stampante Foomatic foomatic-rip è in genere utilizzato insieme a Ghostscript per le stampanti non PostScript. I file PPD Foomatic validi contengono le voci *NickName: ... Foomatic/Ghostscript driver e *cupsFilter: ... foomatic-rip. Questi file PPD sono inclusi nel pacchetto cups-drivers.

In YaST viene scelto un file PPD Foomatic se un file di questo tipo con la voce *NickName: ... Foomatic ... (recommended) corrisponde al modello della stampante e il pacchetto manufacturer-PPDs non contiene un file PPD più appropriato.

File PPD Gimp-Print nel pacchetto cups-drivers-stp

Al posto di foomatic-rip, è possibile utilizzare il filtro CUPS rastertoprinter di Gimp-Print per numerose stampanti non PostScript. Questo filtro e i file PPD Gimp-Print appropriati sono disponibili nel pacchetto cups-drivers-stp. I file PPD Gimp-Print si trovano in /usr/share/cups/model/stp/ e contengono voci *NickName: ... CUPS+Gimp-Print e *cupsFilter: ... rastertoprinter.

File PPD dei produttori di stampanti nel pacchetto `manufacturer-PPDs`

Il pacchetto `manufacturer-PPDs` contiene file PPD dei produttori di stampanti concessi con licenza libera. È consigliabile configurare le stampanti PostScript con il file PPD appropriato del produttore della stampante, poiché tale file consente l'utilizzo di tutte le funzioni della stampante PostScript. In YaST viene selezionato un file PPD del pacchetto `manufacturer-PPDs` se si riscontrano le seguenti condizioni:

- Il fornitore e il modello determinati durante il rilevamento dell'hardware corrispondono al fornitore e al modello indicati in un file PPD del pacchetto `manufacturer-PPDs`.
- Il file PPD del pacchetto `manufacturer-PPDs` è l'unico file PPD valido per il modello della stampante o esiste anche un file PPD Foomatic con una voce `*NickName: ... Foomatic/Postscript (recommended)` che corrisponde al modello della stampante.

Di conseguenza, in YaST non viene utilizzato alcun file PPD del pacchetto `manufacturer-PPDs` nei seguenti casi:

- Il file PPD del pacchetto `manufacturer-PPDs` non corrisponde al fornitore e al modello. Ciò può accadere se il pacchetto `manufacturer-PPDs` contiene solo un file PPD per modelli simili, ad esempio se non sono disponibili file PPD diversi per i singoli modelli di una serie, mentre il nome del modello è specificato nel formato `Funprinter 1000 series` nel file PPD.
- Il file PPD PostScript Foomatic non è consigliato poiché il modello della stampante potrebbe non funzionare correttamente in modalità PostScript, ad esempio la stampante può risultare inaffidabile in questa modalità poiché non dispone di memoria sufficiente o è troppo lenta perché le capacità del processore non sono adeguate. La stampante, inoltre, potrebbe non supportare la modalità PostScript per default, ad esempio se il supporto PostScript è disponibile solo come modulo facoltativo.

Se un file PPD del pacchetto `manufacturer-PPDs` è adatto a una stampante PostScript ma in YaST non è possibile configurarlo per i motivi indicati, selezionare manualmente il modello della stampante corrispondente in YaST.

31.7 Risoluzione dei problemi

Nelle sezioni seguenti verranno esaminati alcuni dei problemi hardware e software riscontrati con maggiore frequenza e le procedure per risolvere o evitare tali problemi.

31.7.1 Stampanti prive del supporto del linguaggio standard per stampanti

Le stampanti che non supportano alcun linguaggio comune per stampanti e possono essere utilizzate solo con sequenze di controllo speciali sono definite *stampanti GDI*. Queste stampanti possono interagire solo con i sistemi operativi che dispongono di un driver fornito dal produttore. *GDI* è un'interfaccia di programmazione sviluppata da Microsoft per i dispositivi grafici. Il problema non è costituito dall'interfaccia di programmazione, bensì dal fatto che le stampanti GDI possono essere utilizzate solo tramite il linguaggio per stampanti proprietario del relativo modello della stampante.

In alcune stampanti è possibile attivare la modalità GDI o uno dei linguaggi standard per stampanti. Alcuni produttori forniscono driver proprietari per le proprie stampanti GDI. Lo svantaggio dei driver per stampanti proprietari è che non esiste alcuna garanzia che essi funzionino con il sistema di stampa installato e che siano adatti alle varie piattaforme hardware. Diversamente, le stampanti che supportano un linguaggio standard non dipendono da una versione speciale del sistema di stampa o da una determinata piattaforma hardware.

Anziché tentare di far funzionare un driver Linux proprietario, può essere più conveniente acquistare una stampante supportata. In questo modo si risolverebbe definitivamente il problema del driver, eliminando l'esigenza di installare e configurare software driver speciali e ottenere aggiornamenti del driver che possono essere necessari in seguito a nuovi sviluppi nel sistema di stampa.

31.7.2 Nessun file PPD appropriato disponibile per una stampante PostScript

Se il pacchetto `manufacturer-PPDs` non contiene alcun file PPD appropriato per una stampante PostScript, è in genere possibile utilizzare il file PPD dal CD dei driver del produttore della stampante o scaricare un file PPD appropriato dalla pagina Web del produttore della stampante.

Se il file PPD è disponibile in forma di archivio zip (.zip) come archivio zip autoestraente (`.exe`), decomprimerlo con il comando `unzip`. Esaminare i termini della licenza del file PPD. Utilizzare quindi l'utility `cupstestppd` per verificare se il file PPD è conforme alla specifica «Adobe PostScript Printer Description File Format Specification, version 4.3». Se l'utility restituisce «FAIL», gli errori nel file PPD sono gravi e possono provocare problemi significativi. Tutte le aree problematiche individuate da `cupstestppd` devono essere eliminate. Se necessario, richiedere un file PPD appropriato al produttore della stampante.

31.7.3 Porte parallele

L'approccio più sicuro consiste nel collegare la stampante direttamente alla prima porta parallela e selezionare le impostazioni della porta parallela seguenti nel BIOS:

- I/O address: `378` (esadecimale)
- Interrupt: irrilevante
- Mode: `Normal`, `SPP`, o `Output Only`
- DMA: disattivato

Se dopo aver specificato queste impostazioni non è ancora possibile accedere alla stampante dalla porta parallela, immettere esplicitamente l'indirizzo I/O dell'impostazione del BIOS nel formato `0x378` in `/etc/modprobe.conf`. Se sono presenti due porte parallele impostate sugli indirizzi I/O `378` e `278` (esadecimale), immettere tali impostazioni nel formato `0x378,0x278`.

Se l'interrupt `7` è libero, può essere attivato con la voce illustrata nell'Esempio 31.1, «/etc/modprobe.conf: modalità di interrupt per la prima porta parallela» (p. 520). Prima di attivare la modalità di interrupt, controllare il file `/proc/interrupts` per verificare quali interrupt siano già in uso. Vengono visualizzati solo gli interrupt attualmente utilizzati. L'utilizzo di interrupt dipende dai componenti hardware attivi. L'interrupt per la porta parallela non deve essere utilizzato da altri dispositivi. Se non si è sicuri di questo aspetto, utilizzare la modalità di polling con `irq=none`.

Esempio 31.1 *`/etc/modprobe.conf`: modalità di interrupt per la prima porta parallela*

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

31.7.4 Connessioni della stampante di rete

Identificazione dei problemi di rete
Collegare la stampante direttamente al computer. Per eseguire un test, configurare la stampante come una stampante locale. Se funziona, i problemi riguardano la rete.

Controllo della rete TCP/IP
La rete TCP/IP e la risoluzione dei nomi devono funzionare correttamente.

Controllo di un `lpd` remoto
Utilizzare il comando seguente per testare se è possibile stabilire una connessione TCP a `lpd` (porta `515`) nell'*`host`*:

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

Se la connessione a `lpd` non può essere stabilita, è possibile che `lpd` non sia attivo o che vi siano problemi nella rete.

In qualità di utente `root`, utilizzare il comando seguente per eseguire una query in un rapporto sullo stato, possibilmente molto lungo, per ricercare *`queue`* in un *`host`* remoto, purché il relativo `lpd` sia attivo e l'host accetti le query:

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

Se `lpd` non risponde alla query, è possibile che non sia attivo o che vi siano problemi nella rete. Diversamente, se `lpd` risponde, nella risposta dovrebbe essere indicato il motivo che impedisce la stampa in `queue` nell'`host`. Se si riceve una risposta

simile a quella mostrata nell'Esempio 31.2, «Messaggi di errore dall'lpd» (p. 521), il problema è causato dall'`lpd` remoto.

Esempio 31.2 *Messaggi di errore dall'lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Controllo di un `cupsd` remoto

Per default, il server di rete CUPS deve diffondere le code ogni 30 secondi nella porta UDP `631`. Di conseguenza, è possibile utilizzare il comando seguente per testare se nella rete è disponibile un server di rete CUPS.

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

Se è disponibile un server di rete CUPS che esegue la diffusione, l'output sarà simile a quello mostrato nell'Esempio 31.3, «Diffusione dal server di rete CUPS» (p. 521).

Esempio 31.3 *Diffusione dal server di rete CUPS*

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

Il comando seguente può essere utilizzato per testare se è possibile stabilire una connessione TCP a `cupsd` (porta `631`) nell'*`host`*:

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

Se la connessione a `cupsd` non può essere stabilita, è possibile che `cupsd` non sia attivo o che vi siano problemi nella rete. `lpstat -h host -l -t` restituisce un rapporto sullo stato (possibilmente molto lungo) per tutte le code sull'*`host`*, purché il relativo `cupsd` sia attivo e l'host accetti le query.

Il comando successivo può essere utilizzato per testare se *`queue`*nell'*`host`* accetta un lavoro di stampa formato da un singolo carattere di ritorno a capo. Questo comando non determina alcuna stampa. È possibile che venga emessa una pagina bianca.

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

Risoluzione dei problemi di una stampante di rete o di una casella del server di stampa

Gli spooler in esecuzione in una casella del server di stampa possono talvolta causare problemi se devono gestire numerosi lavori di stampa. Poiché tali problemi sono causati dallo spooler nella casella del server di stampa, non è possibile risolverli in alcun modo. Per evitarli, ignorare lo spooler nella casella del server di stampa utilizzando la stampante connessa a tale casella direttamente tramite il socket TCP. Vedere Sezione 31.4.2, «Stampanti di rete» (p. 508).

In questo modo la casella del server di stampa viene utilizzata solo come convertitore tra i vari formati del trasferimento di dati (connessione alla rete TCP/IP e alla stampante locale). Per utilizzare questa procedura, è necessario conoscere la porta TCP della casella del server di stampa. Se la stampante è connessa alla casella del server di stampa ed è accesa, la porta TCP può solitamente essere individuata tramite l'utility `nmap` del pacchetto `nmap` dopo un breve intervallo dall'accensione della casella del server di stampa. Ad esempio, `nmap` *`IP-address`* può restituire il seguente output per una casella del server di stampa:

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

Questo output indica che la stampante connessa alla casella del server di stampa può essere utilizzata tramite il socket TCP sulla porta `9100`. Per default, `nmap` controlla solo determinate porte note, elencate in `/usr/share/nmap/nmap-services`. Per controllare tutte le porte possibili, utilizzare il comando `nmap -p` *`from_port-to_port IP-address`*. Questa operazione potrebbe richiedere del tempo. Per ulteriori informazioni, consultare la documentazione `nmap`.

Immettere un comando simile al seguente

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

per inviare stringhe di caratteri o file direttamente alla porta corrispondente per testare se la stampante può essere utilizzata da questa porta.

31.7.5 Stampe difettose senza messaggi di errore

Per quanto riguarda il sistema di stampa, il lavoro di stampa è completo quando il back-end di CUPS ultima il trasferimento di dati alla stampante di destinazione. Se l'elaborazione successiva nel destinatario ha esito negativo, ad esempio se la stampante non è in grado di stampare i dati specifici della stampante, il sistema di stampa non rileva il problema. Se non è possibile stampare dati specifici della stampante, selezionare un file PPD diverso che risulti più adatto alla stampante in uso.

31.7.6 Code disabilitate

Se il trasferimento di dati al destinatario non può essere eseguito dopo numerosi tentativi, il back-end CUPS, ad esempio `usb` o `socket`, segnalano a `cupsd` un errore nel sistema di stampa. Nel back-end viene stabilito se effettuare tentativi ed eventualmente quanti effettuarne prima di segnalare l'impossibilità di eseguire il trasferimento dei dati. Poiché sarebbe inutile eseguire ulteriori tentativi, `cupsd` disabilita la stampa per la coda corrispondente. Dopo aver eliminato la causa del problema, l'amministratore del sistema deve abilitare nuovamente la stampa mediante il comando `/usr/bin/enable`.

31.7.7 CUPS Browsing: eliminazione di lavori di stampa

Se le code di un server di rete CUPS vengono diffuse agli host del client tramite il protocollo CUPS Browsing ed è attivo un `cupsd` locale valido negli host del client, il `cupsd` del client accetta i lavori di stampa dalle applicazioni e li inoltra al `cupsd` del server. Quando `cupsd` accetta un lavoro di stampa, viene associato a un nuovo numero di lavoro. Il numero del lavoro nell'host del client è pertanto diverso da quello nel server. Poiché in genere un lavoro di stampa viene inoltrato immediatamente, non può essere eliminato tramite il numero del lavoro disponibile nell'host del client in quanto il `cupsd` del client considera completato il lavoro di stampa nel momento in cui viene inoltrato al `cupsd` del server.

Per eliminare il lavoro di stampa nel server, utilizzare un comando quale `lpstat -h print-server -o` per determinare il numero del lavoro nel server, purché il server

non abbia già completato il lavoro di stampa, ovvero lo abbia inviato alla stampante. Utilizzando questo numero, è possibile eliminare il lavoro di stampa nel server:

```
cancel -h print-server queue-jobnnumber
```

31.7.8 Lavori di stampa difettosi ed errori nel trasferimento di dati

I lavori di stampa restano nelle code e la stampa viene ripresa se si spegne e si riaccende la stampante e si riavvia il computer durante il processo di stampa. I lavori di stampa difettosi devono essere rimossi dalla coda tramite il comando `cancel`.

Se un lavoro di stampa è difettoso o si verifica un errore nella comunicazione tra l'host e la stampante, verranno stampati numerosi fogli con caratteri illeggibili poiché i dati non possono essere elaborati correttamente. Per risolvere questo problema, attenersi alla procedura seguente:

1. Per interrompere la stampa, rimuovere tutta la carta dalle stampanti a getto d'inchiostro o aprire i cassetti della carta delle stampanti laser. Le stampanti di alta qualità sono dotate di un pulsante per l'annullamento della stampa in corso.

2. Il lavoro di stampa potrebbe ancora essere nella coda, poiché i lavori vengono rimossi solo dopo essere stati inviati completamente alla stampante. Utilizzare `lpstat -o` o `lpstat -h` *`print-server`* `-o` per controllare quale sia la coda correntemente in stampa. Eliminare il lavoro di stampa mediante il comando `cancel` *`queue-jobnumber`* o `cancel -h` *`print-server queue-jobnumber`*.

3. Anche se il lavoro di stampa è stato eliminato dalla coda, alcuni dati potrebbero comunque essere trasferiti alla stampante. Verificare se un processo nel back-end CUPS è ancora in esecuzione per la coda in questione e terminarlo. Nel caso di una stampante collegata alla porta parallela, ad esempio, il comando `fuser -k /dev/lp0` può essere utilizzato per terminare tutti i processi ancora attivi sulla stampante o nella porta parallela.

4. Reimpostare la stampante spegnendola per un breve periodo, quindi inserire la carta e riaccendere la stampante.

31.7.9 Debugging del sistema di stampa CUPS

Utilizzare la seguente procedura generica per individuare problemi nel sistema di stampa CUPS:

1. Impostare `LogLevel debug` in `/etc/cups/cupsd.conf`.
2. Interrompere `cupsd`.
3. Rimuovere `/var/log/cups/error_log*` per non dover eseguire la ricerca in file di log molto estesi.
4. Avviare `cupsd`.
5. Ripetere l'azione che aveva determinato il problema.
6. Controllare i messaggi in `/var/log/cups/error_log*` per identificare la causa del problema.

31.7.10 Ulteriori informazioni

Le soluzioni a molti problemi specifici sono illustrate nel database del supporto tecnico. Se vengono rilevati problemi relativi alla stampante, consultare gli articoli del database del supporto tecnico *Installing a Printer* (in lingua inglese) e *Printer Configuration from SUSE Linux 9.2* (in lingua inglese), che possono essere individuati effettuando una ricerca per la parola chiave *printer*.

32 Sistema Hotplug

Il sistema hotplug controlla l'inizializzazione di quasi tutti i dispositivi installati su un computer. Non può essere utilizzato solo con i dispositivi che è possibile inserire o rimuovere durante un'operazione, bensì per tutti quelli che vengono rilevati durante l'avvio del sistema. Viene inoltre utilizzato con il file system `sysfs` e lo strumento `udev`, illustrati in Capitolo 33, *Nodi di dispositivi dinamici con* `udev` (p. 535).

Finché non viene avviato il kernel, vengono inizializzati solo i dispositivi assolutamente necessari, ad esempio il bus di sistema, i dischi di avvio e la tastiera. Il kernel avvia gli eventi hotplug di tutti i dispositivi rilevati. Questi eventi vengono visualizzati nel daemon di `udevd` il quale esegue `udev` per creare il nodo del dispositivo e configurarlo. Per i dispositivi che non è possibile rilevare automaticamente, come ad esempio le vecchie schede ISA, viene utilizzata una configurazione statica.

A parte poche eccezioni, quasi tutti dispositivi vengono inizializzati non appena diventano accessibili, durante l'avvio del sistema o al momento dell'inserimento. Durante il processo di inizializzazione, le interfacce vengono registrate con il kernel. La registrazione avvia altri eventi hotplug che provocano la configurazione automatica della rispettiva interfaccia.

Nelle versioni precedenti di SUSE Linux veniva utilizzato un gruppo statico di dati di configurazione come base per l'inizializzazione dei dispositivi. Tutti gli eventi hotplug erano gestiti da script separati, chiamati agenti. In questa versione di SUSE Linux, invece, il sottosistema hotplug è integrato in udev, le cui regole forniscono le stesse funzionalità dei precedenti agenti hotplug.

Le impostazioni generali del sottosistema hotplug sono disponibili in `/etc/sysconfig/hotplug` con le descrizioni di tutte le variabili. La configurazione

generale di un dispositivo dipende dalle regole di corrispondenza disponibili in /etc/udev/rules.d (vedere il Capitolo 33, *Nodi di dispositivi dinamici con udev* (p. 535)). I file di configurazione dei dispositivi specifici sono archiviati in /etc/sysconfig/hardware. La richiamata di un evento hotplug /proc/sys/kernel/hotplug, utilizzata nella versione precedente di SUSE Linux, è generalmente vuota perché udevd riceve i messaggi hotplug mediante un socket netlink.

32.1 Dispositivi e interfacce

Un sistema hotplug può essere utilizzato anche per configurare le interfacce, oltre ai dispositivi. Un dispositivo è generalmente collegato a un bus e offre le funzionalità necessarie a un'interfaccia la quale rappresenta l'astrazione visibile dall'utente di un gruppo, intero o parziale, di periferiche. Per il corretto funzionamento di un dispositivo è necessario utilizzare il driver corrispondente sotto forma di moduli del kernel. Inoltre, per offrire l'interfaccia all'utente, potrebbero essere necessari anche alcuni driver di livello più elevato. Le interfacce sono generalmente rappresentate da nodi di dispositivi creati da udev. La distinzione tra interfacce e dispositivi è importante per la comprensione di tutto il contesto.

I dispositivi specificati nel file system sysfs sono disponibili in /sys/devices. Le interfacce, invece, sono archiviate in /sys/class o /sys/block. Tutte le interfacce in sysfs devono includere un collegamento ai relativi dispositivi. Tuttavia, alcuni driver non supportano l'aggiunta automatica di questo collegamento senza il quale non è possibile conoscere il dispositivo a cui appartiene l'interfaccia e di conseguenza non è possibile individuare la configurazione appropriata.

Per fare riferimento a un dispositivo viene generalmente utilizzata una descrizione, che può corrispondere al percorso del dispositivo in sysfs (/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0), a una descrizione del punto di connessione (bus-pci-0000:02:00.0), a un singolo ID (id-32311AE03FB82538) o simili. In passato, i nomi assegnati alle interfacce corrispondevano alla numerazione dei dispositivi esistenti e potevano quindi cambiare ogni volta che veniva aggiunto o rimosso un dispositivo.

Per indentificare le interfacce, è anche possibile utilizzare una descrizione del dispositivo associato. Generalmente, è possibile capire dal contesto se la descrizione fa riferimento al dispositivo o alla relativa interfaccia. Di seguito sono riportati alcuni esempi di dispositivi, interfacce e descrizioni.

Scheda di rete PCI

Dispositivo collegato al bus PCI (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0` o `bus-pci-0000:02:00.0`) che presenta un'interfaccia di rete (`eth0`, `id-00:0d:60:7f:0b:22` o `bus-pci-0000:02:00.0`). Quest'ultima è utilizzata dai servizi di rete oppure connessa a un dispositivo di rete virtuale, ad esempio un tunnel o una VLAN, che a sua volta dispone di un'interfaccia.

Controller SCSI PCI

Dispositivo (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` o `bus-scsi-1:0:0:0`) che crea molte interfacce fisiche sotto forma di un bus (`/sys/class/scsi_host/host1`).

Unità disco rigido SCSI

Dispositivo (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` o `bus-scsi-1:0:0:0`) con numerose interfacce (`/sys/block/sda*`).

32.2 Eventi Hotplug

A ogni dispositivo e interfaccia è associato un *evento hotplug* elaborato da `udev`. Gi eventi hotplug vengono attivati dal kernel al momento della creazione o della rimozione di un collegamento a un dispositivo oppure quando viene registrata o eliminata un'interfaccia su un driver. Dalla versione 9.3 di SUSE Linux gli eventi hotplug vengono ricevuti ed elaborati da `udevd`. Se i messaggi netlink del kernel non vengono direttamente visualizzati in `udevd`, è necessario specificare `/sbin/udevsend` in `/proc/sys/kernel/hotplug`. `udevd` consente di configurare il dispositivo in base a un gruppo di regole (vedere il Capitolo 33, *Nodi di dispositivi dinamici con* `udev` (p. 535)).

32.3 Configurazione di dispositivi hotplug

Gli agenti hotplug sono stati dichiarati di proprietà di SUSE Linux 10.0. Pertanto, tutte le operazioni di configurazione dei dispositivi devono ora essere eseguite mediante le regole di `udev` che includono anche una regola di compatibilità per chiamare gli agenti

personalizzati esistenti. È tuttavia necessario tener conto della conversione degli agenti personalizzati in regole udev.

Un agente hotplug è un programma eseguibile che esegue le azioni appropriate a un evento. Gli agenti relativi agli eventi dei dispositivi sono archiviati in `/etc/hotplug.d/`*`nome evento`* e `/etc/hotplug.d/default`. Tutti i programmi con il suffisso `.hotplug` inclusi in queste directory vengono eseguiti in ordine alfabetico.

Per semplificare la configurazione di un dispositivo, è generalmente sufficiente caricare un modulo del kernel. In alcuni casi, per configurare un dispositivo in maniera appropriata, può tuttavia essere necessario chiamare ulteriori comandi. In SUSE Linux questa operazione viene generalmente gestita mediante le regole udev. Tuttavia, le configurazioni personalizzate dei dispositivi vengono eseguite mediante `/sbin/hwup` o `/sbin/hwdown`, i quali cercano una configurazione appropriata per il dispositivo nella directory `/etc/sysconfig/hardware` e quindi la applicano. Ad esempio, per evitare che venga inizializzato un determinato dispositivo, creare un file di configurazione con un nome appropriato e impostare la modalità di avvio su `manual` o `off`. Se `/sbin/hwup` non trova una configurazione appropriata, procede con la ricerca della variabile d'ambiente `MODALIAS`. Se invece la trova, il modulo corrispondente viene automaticamente caricato in `modprobe`. La variabile `MODALIAS` viene generata automaticamente dagli eventi hotplug del kernel per tutti i dispositivi che richiedono il caricamento di un modulo. Per ulteriori informazioni, vedere la Sezione 32.4, «Caricamento automatico dei moduli» (p. 532). Per ulteriori informazioni su `/sbin/hwup`, vedere il file `/usr/share/doc/packages/sysconfig/README` e la pagina di manuale `man hwup`.

Prima di chiamare gli agenti d'interfaccia, in `udev` viene di solito generato un nodo di dispositivo a cui il sistema può accedere. `udev` supporta l'assegnazione di nomi persistenti alle interfacce. Per ulteriori informazioni, vedere il Capitolo 33, *Nodi di dispositivi dinamici con* `udev` (p. 535). Quindi, vengono configurate le interfacce stesse in base alla rispettive regole udev. Di seguito sono illustrate le procedure relative ad alcune interfacce.

32.3.1 Attivazione di interfacce di rete

Le interfacce di rete vengono inizializzate con `/sbin/ifup` e disattivate con `/sbin/ifdown`. Per ulteriori informazioni, vedere il file `/usr/share/doc/packages/sysconfig/README` e la pagina di manuale `ifup`.

Se il computer dispone di molti dispositivi di rete dotati di diverse interfacce, le relative designazioni possono cambiare quando un altro driver viene caricato più velocemente all'avvio del sistema. In SUSE Linux la numerazione rimane il più possibile persistente: i dispositivi mantengono il nome d'interfaccia assegnato loro durante il processo di configurazione. L'assegnazione dei nomi è gestita dalle regole udev. Per cambiare un nome, è quindi necessario modificare queste regole.

Tuttavia, la soluzione migliore consiste nell'utilizzare designazioni d'interfaccia persistenti. Nei file di configurazione è possibile specificare i nomi delle singole interfacce. Informazioni dettagliate su questo argomento sono disponibili nel file `/usr/share/doc/packages/sysconfig/README`. Dalla versione 9.3 di SUSE Linux, udev gestisce anche le interfacce di rete benché queste non rappresentino nodi di dispositivi. Ciò consente di utilizzare nomi d'interfaccia persistente in maniera più standard.

32.3.2 Attivazione di dispositivi di memorizzazione

Le interfacce dei dispositivi di memorizzazione devono essere montate di modo che sia possibile accedervi. È possibile pre-configurare o automatizzare completamente questa operazione. Inoltre, in SUSE Linux i dispositivi di sistema e quelli utente vengono gestiti in maniera diversa. I dispositivi di sistema possono essere montati solo automaticamente mediante la creazione di una voce in `/etc/fstab`. I dispositivi utente, invece, vengono gestiti di default mediante `hal`. I dispositivi utente che necessitano di un'altra configurazione possono essere archiviati in `/etc/fstab`.In alternativa, è possibile modificare la gestione di questi dispositivi in `hal`. Per ulteriori informazioni su `hal`, vedere `/usr/share/doc/packages/hal/hal-spec.html`.

Si consiglia di utilizzare nomi persistenti per i dispositivi perché i nomi tradizionali possono variare in base alla sequenza di inizializzazione. Per ulteriori informazioni sui nomi persistenti per i dispositivi, vedere il Capitolo 33, *Nodi di dispositivi dinamici con `udev`* (p. 535).

32.4 Caricamento automatico dei moduli

Se è impossibile per `/sbin/hwup` individuare un file di configurazione, modprobe procede con la ricerca di un modulo corrispondente in base al contenuto della variabile d'ambiente `MODALIAS`. Questa variabile viene generata dal kernel per l'evento hotplug corrispondente. Per utilizzare un driver diverso da quello standard del kernel, è necessario creare un file di configurazione appropriato in `/etc/sysconfig/hardware`.

32.5 Coldplug dello script di avvio

`boot.coldplug` consente di inizializzare tutti i dispositivi che non sono stati configurati durante l'avvio. Per ogni configurazione di dispositivo statica designata come `/etc/sysconfig/hardware/hwcfg-static-*`, viene chiamato il comando `hwup`. Quindi, per inizializzare tutte le periferiche, vengono rieseguiti tutti gli eventi archiviati in `/lib/klibc/events`.

32.6 Analisi degli errori

32.6.1 File di log

Di default `hotplug` invia a `syslog` solo alcuni messaggi importanti. Per ricevere ulteriori informazioni, impostare la variabile `HOTPLUG_DEBUG` nel file `/etc/sysconfig/hotplug` su `yes`. Se si imposta questa variabile sul valore `max`, ogni comando della shell verrà protocollato per ciascuno script hotplug. Pertanto, le dimensioni del file `/var/log/messages`, ovvero il file in cui `syslog` archivia tutti i messaggi, aumenteranno. Tuttavia, poiché durante il processo di avvio `syslog` viene avviato dopo `hotplug` e `coldplug`, è possibile che i primi messaggi non vengano protocollati. Per registrarli, specificare un altro file di log mediante la variabile `HOTPLUG_SYSLOG`. Per ulteriori informazioni, vedere `/etc/sysconfig/hotplug`.

32.6.2 Problemi di avvio

Se un computer si blocca durante il processo di avvio, disabilitare `hotplug` o `coldplug` specificando`NOHOTPLUG=yes` o `NOCOLDPLUG=yes` al prompt di avvio. In questo modo viene disattivato hotplug per impedire al kernel di segnalare gli eventi hotplug. Per attivare hotplug sul sistema in esecuzione, specificare il comando `/etc/init.d/boot.hotplug start`. Tutti gli eventi generati fino al momento specificato verrano individuati ed elaborati. Per rifiutare gli eventi in coda, immettere innanzitutto `/bin/true` in `/proc/sys/kernel/hotplug`, quindi reimpostare la voce su `/sbin/hotplug`. Essendo coldplug disattivato, non sarà possibile applicare le configurazioni statiche. Per applicarle, specificare `/etc/init.d/boot.coldplug start`.

Per scoprire se il problema è causato da un particolare modulo caricato da `hotplug`, immettere `HOTPLUG_TRACE=<N>` al prompt di avvio. Dopo *N* secondi verranno visualizzati sullo schermo i nomi di tutti i moduli da caricare prima dell'inizio del processo di caricamento effettivo. Non è possibile intervenire in questa fase.

32.6.3 Event Recorder

Per ogni evento gestito da una regola udev viene eseguito lo script `/sbin/hotplugeventrecorder`. Se una directory `/events` esiste già, tutti gli eventi hotplug verranno archiviati come singoli file in questa directory. Ciò consente di rigenerare gli eventi per le attività di verifica. Se invece la directory `/events` non esiste, non verrà registrato alcun evento.

Nodi di dispositivi dinamici con udev

33

In Linux kernel 2.6 è stata inserita una nuova soluzione per lo spazio utente dedicata alla directory dinamica dei dispositivi `/dev` con le designazioni: `udev`. Questa soluzione gestisce solo i file dei dispositivi attualmente presenti, consente di creare o rimuovere i file dei nodi dei dispositivi generalmente archiviati nella directory `/dev` nonché di rinominare le interfacce di rete. La precedente implementazione di directory dinamica `/dev` con `devfs` è stata sostituita da `udev`.

Sui sistemi Linux, i nodi dei dispositivi venivano archiviati nella directory `/dev`. Poiché era disponibile un nodo per ogni possibile tipo di dispositivo, indipendentemente dalla sua effettiva esistenza, questa directory conteneva migliaia di file inutilizzati. Per utilizzare un nuovo dispositivo del sottosistema o del kernel, era innanzitutto necessario creare i nodi corrispondenti con una speciale applicazione. Con l'aggiunta del file system `devfs` la procedura è stata notevolmente migliorata perché i nodi in `/dev` venivano assegnati solo ai dispositivi effettivamente esistenti e noti al kernel.

Con `udev` viene introdotta una nuova tecnica di creazione dei nodi di dispositivi. Il kernel esporta il proprio stato in `sysfs` che viene aggiornato al rilevamento di un nuovo dispositivo. Quindi, viene inviato un evento allo spazio utente. Grazie alla disponibilità delle informazioni in `sysfs` udev può mappare una semplice sintassi di regole con gli attributi disponibili per il dispositivo e quindi creare o rimuovere i nodi corrispondenti.

L'utente non deve creare alcuna regola udev per i nuovi dispositivi. Quando si collega un dispositivo, viene creato automaticamente il relativo nodo. Tuttavia, le regole consentono di definire una politica per la denominazione dei dispositivi e rendono possibile sostituire un nome criptico con un altro più facile da ricordare. Inoltre,

permettono di utilizzare nomi persistenti particolarmente utili quando due dispositivi dello stesso tipo vengono connessi contemporaneamente.

Si supponga ad esempio di disporre di due stampanti, una laser a colori di alta qualità e l'altra a getto d'inchiostro in bianco e nero, collegate tramite porta USB. Di default, queste vengono denominate `/dev/usb/lpX`, dove X è il numero che corrisponde all'ordine di connessione della stampante. Con udev è possibile creare apposite regole personalizzate e assegnare ad esempio il nome `/dev/colorlaser` alla stampante laser e il nome `/dev/inkprinter` a quella a getto d'inchiostro. La creazione dei nodi in base alle caratteristiche del dispositivo supportata da udev garantisce che questi facciano sempre riferimento al dispositivo corretto, indipendentemente dallo stato o dall'ordine di connessione.

33.1 Creazione di regole

Prima di creare i nodi dei dispositivi nella directory `/dev`, `udev` legge tutti i file inclusi in `/etc/udev/rules.d` che presentano il suffisso `.rules`, in ordine alfabetico. Viene utilizzata la prima regola idonea al dispositivo, anche se possono esistere altre regole valide. I commenti sono contrassegnati con il simbolo cancelletto (#). Le regole presentano la struttura seguente:

```
key, [key,...] NAME [, SYMLINK]
```

Le regole vengono assegnate ai dispositivi in base a delle chiavi, per questo motivo è necessario specificare almeno una chiave. È anche obbligatorio immettere un nome per il nodo del dispositivo creato in `/dev`. Il parametro symlink opzionale consente di creare i nodi in altre posizioni. La regola per una stampata è costituita dalla struttura seguente:

```
BUS=="usb", SYSFS{serial}=="12345", NAME="lp_hp", SYMLINK+="printers/hp"
```

Nell'esempio sono disponibili due chiavi: `BUS` e `SYSFS{serial}`. In `udev` il numero di serie viene confrontato con quello del dispositivo collegato alla porta USB. Per poter assegnare il nome `lp_hp` al dispositivo incluso nella directory `/dev`, tutte le chiavi devono essere identiche. Viene creato anche un collegamento simbolico `/dev/printers/hp` che fa riferimento al nodo del dispositivo. Nello stesso tempo, viene automaticamente creata la directory `printers`. I lavori di stampa possono essere inviati a `/dev/printers/hp` o `/dev/lp_hp`.

33.2 Sostituzione di un segnaposto

I parametri NAME e SYMLINK consentono di utilizzare i segnaposti al posto di valori speciali. La procedura viene illustrata nell'esempio riportato di seguito.

```
BUS=="usb", SYSFS{vendor}=="abc", SYSFS{model}=="xyz", NAME="camera%n"
```

L'operatore %n nel nome viene sostituito dal numero del dispositivo relativo alla fotocamera, ad esempio `camera0` o `camera1`. Un altro operatore utile è costituito da `%k` il quale viene sostituito dal nome standard del dispositivo nel Kernel, ad esempio `hda1`. È anche possibile chiamare un programma esterno nelle regole udev e utilizzare la stringa restituita nei valori NAME e SYMLINK. Per consultare l'elenco completo dei segnaposti disponibili, vedere la pagina di manuale `udev`.

33.3 Corrispondenza di motivi nelle chiavi

Nelle chiavi delle regole udev è possibile utilizzare una corrispondenza di motivi stile shell chiamati caratteri jolly. Ad esempio, è possibile utilizzare `*` come segnaposto di un carattere qualsiasi oppure `?` al posto di un preciso carattere arbitrario.

```
KERNEL="ts*", NAME="input/%k"
```

Questa regola assegna il nome standard del kernel nella directory standard a un dispositivo la cui designazione inizia con le lettere «ts». Per ulteriori informazioni sull'utilizzo della corrispondenza dei motivi nelle regole udev, vedere la pagina di manuale `udev`.

33.4 Selezione di chiavi

Per identificare un dispositivo in maniera univoca e distinguere i vari dispositivi tra di loro, è necessario specificare una proprietà esclusiva per una regola udev attiva. Di seguito sono riportati alcuni esempi di chiavi standard.

SUBSYSTEM
Sottosistema a cui appartiene il dispositivo

BUS
Tipo di bus del dispositivo

KERNEL
Nome utilizzato dal kernel per il dispositivo

ID
Numero del dispositivo sul bus, ad esempio ID del bus PCI

SYSFS{...}
Attributi del dispositivo sysfs, ad esempio l'etichetta, il produttore o il numero di serie

Benché le chiavi `SUBSYSTEM` e `ID` siano utili, vengono generalmente utilizzate le chiavi `BUS`, `KERNEL` e `SYSFS{...}`. In `udev` sono anche disponibili le chiavi che consentono di chiamare script esterni e valutarne i risultati. Per ulteriori informazioni, vedere la pagina di manuale `udev`.

Il file system `sysfs` espone le informazioni sui componenti hardware in un albero di directory. Ogni file contiene generalmente una voce, ad esempio il nome del dispositivo, il produttore o il numero di serie. Ciascuno di questi file può essere associato a una chiave. Tuttavia, per specificare più chiavi `SYSFS` in una regola, è possibile utilizzare come valori chiave solo i file inclusi nella stessa directory. Lo strumento `udevinfo` può semplificare l'individuazione di valori chiave utili e univoci.

È necessario individuare una sottodirectory di `/sys` che faccia riferimento al relativo dispositivo e che contenga un file `dev`. Tutte queste directory sono archiviate in `/sys/class` o `/sys/block`. Se per un dispositivo esiste già un nodo, `udevinfo` consente di individuare automaticamente la sottodirectory appropriata. Il comando `udevinfo -q path -n /dev/sda` restituisce `/block/sda`. Ciò significa che `/sys/block/sda` è la directory desiderata. Chiamare ora `udevinfo` con il comando `udevinfo -a -p /sys/block/sda`. È anche possibile combinare questi due comandi, come in `udevinfo -a -p `udevinfo -q path -n /dev/sda``. Di seguito è riportato uno stralcio del risultato:

```
BUS=="scsi"
ID=="0:0:0:0"
SYSFS{detach_state}=="0"
SYSFS{type}=="0"
SYSFS{max_sectors}=="240"
SYSFS{device_blocked}=="0"
SYSFS{queue_depth}=="1"
SYSFS{scsi_level}=="3"
```

```
SYSFS{vendor}==" "
SYSFS{model}=="USB 2.0M DSC"
SYSFS{rev}=="1.00"
SYSFS{online}=="1"
```

Cercare le chiavi appropriate e persistenti nei dati restituiti. Ricordarsi che non è possibile utilizzare chiavi di diverse directory in una regola.

33.5 Nomi persistenti per i dispositivi di memorizzazione di massa

SUSE Linux include regole predefinite che consentono di assegnare sempre le stesse designazioni alle unità disco rigido e ad altri dispositivi di memorizzazione, indipendentemente dal loro ordine di inizializzazione. Per leggere gli attributi univoci dei dispositivi, ad esempio i numeri di serie hardware, gli UUID o le etichette del file system, è possibile utilizzare i piccoli programmi helper inclusi in udev. Queste programmi consentono di accedere alle informazioni su un dispositivo specifico durante l'elaborazione delle regole udev. Ad esempio, la prima regola importa nell'ambiente udev i valori rilevati dal dispositivo SCSI. Quindi, la seconda regola utilizza tali valori per creare un collegamento simbolico persistente.

```
KERNEL="sd*[!0-9]", IMPORT="/sbin/scsi_id -g -x -s $p -d %N"
KERNEL="sd*[!0-9]", SYMLINK+="$env{ID_TYPE}/by-id/$env{ID_BUS}-$env{ID_SERIAL}"
```

Non appena viene caricato un driver di un dispositivo di memorizzazione di massa, tutti i dischi rigidi disponibili vengono registrati con il kernel. Per ogni registrazione viene avviato un evento di blocco hotplug che chiama `udev`. `udev` legge le regole per stabilire se è necessario creare un collegamento simbolico.

Se il driver viene caricato mediante `initrd`, gli eventi hotplug andranno perduti. Tutte le informazioni vengono tuttavia archiviate in `sysfs`. L'utility `udevstart` consente di individuare tutti i file dei dispositivi inclusi in `/sys/block` e `/sys/class`, quindi di avviare `udev`.

L'altro script di avvio `boot.udev` consente di ricreare tutti i nodi dei dispositivi durante il processo di avvio. A questo scopo, è necessario avviare tale script con l'editor a livello di esecuzione YaST oppure con il comando `insserv boot.udev`.

34 File system di Linux

Linux supporta tutta una serie di file system. Questo capitolo vi offre una breve rassegna dei file system più noti sotto Linux. Illustreremo i concetti che stanno alla base, i rispettivi vantaggi e il loro campo di impiego preferenziale. Inoltre vi daremo qualche informazione sul «Large File Support» sotto Linux.

34.1 Glossario

Inode
Gli inode contengono tutte le possibili informazioni sui file: nome, dimensione, numero dei link, data, orario di generazione, modifiche, diritti di accesso e puntatori (ingl.pointer) su blocchi del disco rigido su cui risiede il file.

Journal
Nel contesto dei file system, il cosiddetto journal è una struttura interna del disco con una specie di protocollo in cui il driver del file system registra i (meta)dati del file system da modificare. Il «journaling» riduce notevolmente il tempo necessario per ripristinare un sistema Linux, poiché il driver del file system non deve cercare i meta-dati andati distrutti su tutto il disco, gli basta invece rileggere le registrazioni del journal.

Meta-dati
La struttura interna del file system assicura un certo ordine e la disponibilità dei dati sul disco rigido. In un certo senso si tratta di «dati su altri dati». Quasi ogni file system ha una propria struttura di meta-dati. La differenza in termini di funzionalità

dei singoli file system è da ricercare in questo ambito. E' estremamente importante mantenere intatti i meta-dati, altrimenti potrebbe andare distrutto l'intero file system.

34.2 I principali file system di Linux

La situazione è cambiata rispetto a due o tre anni fa', oggi non si ha solo la scelta tra Ext2 o ReiserFS. A partire dalla versione 2.4 il kernel offre una vasta scelta di file system. Segue una breve rassegna della modalità di funzionamento dei file system e dei loro vantaggi.

Chiaramente nessun file system si adatta perfettamente a tutte le applicazioni. Ogni file system ha dei vantaggi e dei svantaggi che vanno ponderati. Neanche il file system più sofisticato potrà mai sostituire un buon concetto di backup.

I termini *integrità dei dati* o *consistenza dei dati* in questo capitolo non si riferiscono alla consistenza dei dati memorizzati di un utente (quei dati che la vostra applicazione scrive nei vostri file). La consistenza dei dati deve essere garantita dalla stessa applicazione.

IMPORTANTE: Configurare i file system

In tema di creazione e configurazione nonché partizionamento di file system si lascia realizzare tutto comodamente con YaST se non vengono indicati esplicitamente degli altri modi per apportare delle modifiche ai file system.

34.2.1 ReiserFS

Una delle funzionalità principali del kernel versione 2.4, ReiserFS, era disponibile a partire da SUSE Linux 6.4 sotto forma di kernel patch per il SUSE kernel 2.2.x. ReiserFS è stato concepito da Hans Reiser e dall'équipe di sviluppatori Namesys. ReiserFS è una valida alternativa a Ext2. I suoi maggiori punti di forza sono una migliore gestione della memoria del disco rigido, migliore accessibilità al disco e ripristino veloce dopo un crollo del sistema.

Ecco i punti di forza di ReiserFS:

Miglior gestione della memoria del disco rigido
In ReiserFS i dati vengono organizzati in un struttura ad albero bilanciato (ingl. B*-balanced tree). La struttura ad albero contribuisce a sfruttare meglio la memoria del disco rigido, dato che piccoli file possono essere memorizzati nello stesso blocco, invece di essere memorizzati altrove e dover gestire il puntatore sulla localizzazione effettiva. Inoltre la memoria non viene assegnata nella misura di unità di 1 o 4 kbyte, ma esattamente nella misura richiesta. Un altro vantaggio è l'allocazione dinamica degli inode che rende i file system più flessibili rispetto ai tradizionali file system come ad esempio Ext2, dove bisogna indicare la densità degli inode al momento della generazione del file system.

Miglior accessibilità del disco rigido
Nel caso di piccoli file vi sarete accorti che sia i dati file sia le informazioni (inode) «stat_data» vengono memorizzati gli uni accanto agli altri sul disco rigido. Basta accedere una volta sola al disco per avere tutte le informazioni di cui avete bisogno.

Ripristino veloce dopo un crollo del sistema
L'uso dei journal, per ricostruire le modifiche apportate ai meta-dati, riduce i tempi di verifica anche nel caso di grandi file system ad una manciata di secondi.

Affidabilità grazie al data Journaling
ReiserFS supporta inoltre il data journaling e ed il data odered è simile a quanto illustrato nella Sezione 34.2.3, «Ext3» (p. 544) dedicata a Ext3. Il modo di default è `data=ordered`, il quale assicura l'integrità sia dei dati che dei metadata, utilizzando comunque il journaling solo per i metadata.

34.2.2 Ext2

Ext2 risale agli inizi di Linux. Deriva dall'Extended File System ed è stato implementato nell'aprile del 1992 e dunque integrato in Linux 0.96c. L'Extended File System è stato successivamente modificato più volte e come Ext2 è stato per anni il più noto file system di Linux. Con l'avvento dei cosiddetti journaling file system e la velocità con la quale eseguono un ripristino, Ext2 perse in termini di importanza.

Forse una breve rassegna dei vantaggi di Ext2 vi aiuterà a capire come mai continua ad avere tanti sostenitori tra gli utenti Linux che ancora oggi preferiscono lavorare con questo file system.

Stabilità
L'appellativo «solido come una roccia» non è dovuta al caso visto che nel corso degli anni Ext2 è stato continuamente migliorato ed ampiamente testato. Nel caso di un crollo del sistema senza un corretto smontaggio del file system, e2fsck analizza i dati del file system. I meta-dati vengono portati in una stato consistente, e file o blocchi di dati in sospeso vengono scritti in una determinata directory (chiamata `lost+found`). Contrariamente alla maggior parte dei journaling file system, e2fsck analizza l'intero file system e non solo i bit dei meta-dati modificati di recente. Questo richiede più tempo rispetto alla verifica dei dati protocollo di un journaling file system. A seconda del volume del file system, questo processo può durare mezz'ora o oltre. Per questo motivo Ext2 non è particolarmente adatto per server ad alta disponibilità. Dato che Ext2 comunque non deve aggiornare continuamente alcun journal e richiede una quantità notevolmente inferiore di memoria a volte risulta essere più veloce di altri file system.

Upgrade facile
Basato sulla solida base di Ext2, Ext3 divenne l'acclamato file system di prossima generazione. L'affidabilità e la stabilità vennero coniugate sapientemente con i vantaggi di un journaling file system.

34.2.3 Ext3

Ext3 è stato sviluppato da Stephen Tweedie. Diversamente dai file system di «prossima generazione» Ext3 non si ispira a principi del tutto nuovi, si basa invece su Ext2. I due file system sono molto simili tra di loro; è semplice implementare un file system Ext3 su di un file system Ext2. La differenza principale tra Ext2 e Ext3 è che Ext3 supporta il journaling. Riassumendo, sono tre i vantaggi che offre Ext3:

Upgrade semplice ed estremamente affidabile da Ext2
Visto che Ext3 si basa sul codice di Ext2 e che appoggia sia il formato on-disk che il formato meta-dati di Ext2, gli upgrade da Ext2 verso Ext3 risultano essere facilissimi da eseguire. Si può eseguire un upgrade anche quando ad essere montati sono i file system di Ext2. Diversamente dalla migrazione verso altri journaling file system, come ReiserFS, JFS o XFS che può diventare una faccenda davvero laboriosa, (dovete fare delle copie di sicurezza di tutto il file system e successivamente ricostruirlo «ex novo»), passare a Ext3 è una questione di pochi minuti. Inoltre è molto sicuro visto che durante la ricostruzione di un completo file system spesso si possono verificare degli errori. Se si considera l'elevato numero di sistemi Ext2 che aspettano un upgrade a un journaling file system, si può

facilmente intuire l'importanza di Ext3 per tanti sistemisti. Eseguire un downgrade da Ext3 a Ext2 è così facile come eseguire un upgrade. Basta smontare correttamente il file system Ext3 e montarlo in seguito come file system Ext2.

Affidabilità e prestazioni
Altri journaling file system seguono l'approccio cosiddetto journaling metadata-only, cioè i vostri meta-dati rimangono in uno stato consistente, cosa che comunque non può essere garantita automaticamente per i dati del file system. Ext3 è in grado invece di assolvere entrambi i compiti, e persino il grado di consistenza si lascia impostare individualmente. Il più elevato grado di sicurezza (cioè integrità dei dati) si ottiene lanciando Ext3 nel modo `data=journal` che comunque può comportare un rallentamento del sistema, giacché vengono rilevati sia i meta-dati che i dati del journal. Un approccio relativamente recente consiste nell'utilizzo del modo `data=ordered` che provvede sia alla integrità dei dati che dei meta-dati, ma che usa il journaling solo per i meta-dati. Il driver del file system raccoglie tutti i blocchi di dati appartenenti ad un aggiornamento dei meta-dati. Questi blocchi vengono scritti sul disco prima dell'aggiornamento dei meta-dati. In questo modo si ha una consistenza dei meta-dati e dei dati senza un calo di performance. Una terza possibilità consiste nel `data=writeback`. In questo caso i dati possono essere scritti nel file system principale dopo che i meta-dati sono stati consegnati al journal. Questa opzione è considerata da tanti la migliore sotto il punto di vista delle prestazioni. Comunque può accadere che ricompaiano nei file vecchi dati a seguito di un crash e ripristino, mentre è garantita l'integrità interna del file system. Se non avete cambiato impostazioni, Ext3 viene inizializzato nel modo `data=ordered`.

34.2.4 Convertire un file system Ext2 in uno Ext3

Tale processo si compone di due passaggi:

Creare il Journal
Eseguite il log in come `root` ed eseguite `tune2fs -j` , con il quale create un journal Ext3 con i parametri di default. Per stabilire la dimensione del journal e su quale dispositivo debba risiedere, eseguite `tune2fs -J` con le opzioni desiderate riguardanti il journal `size=` e `device=`. Per maggiori informazioni sull programma tune2fs rimandiamo alla rispettiva pagina di manuale (tune2fs(8)).

Specificate il tipo di file system Type in /etc/fstab
Per assicurare che il file system Ext3 venga rilevato come tale, editate il file `/etc/fstab`: modificate il tipo di file system specificato per la partizione da `ext2` in `ext3`. Le modifiche vengono applicate al prossimo reboot.

Utilizzare Ext3 per la directory root
Per avviare un file system root impostato come partizione Ext3, includete i moduli `ext3` e `jbd` in `initrd`. Per realizzare ciò, editate il file `/etc/sysconfig/kernel` per includere i due moduli sotto `INITRD_MODULES` ed eseguite il comando `mkinitrd`.

34.2.5 Reiser4

Dopo il rilascio del kernel 2.6, alla famiglia dei journaling file systems si è aggiunto un nuovo membro: Reiser4, il quale differisce completamente dal suo predecessore ReiserFS (versione 3.6). Reiser4, tramite dei plug-ins ottimizza le funzionalità del file system ed offre un concetto di sicurezza più sofistica.

Nuovo concetto di sicurezza
In fase di sviluppo di Reiser4, gli sviluppatori hanno posto l'accento sull'implementazione di caratteristiche rilevanti da un punto di vista della sicurezza. Reiser4 offre quindi tutta una serie di plug-in preposti a incrementare la sicurezza. Nuovo in tal senso sono anche i file «items.». Attualmente, le regole di controllo di accesso vengono definite per ogni file. Se vi è un grande file con informazioni che interessano diversi utenti, gruppi o applicazioni, i permessi di accesso diventano poco precisi per non escludere nessuna delle parti interessate. Reiser4 vi permette di suddividere questi file (appunto in «items»). I permessi di accesso quindi possono essere impostati separatamente per ogni utente con dei benefici del security management. Un esempio ad-hoc è `/etc/passwd`. Finora, solo `root` poteva leggere ed editare il file, mentre tutti gli altri utenti hanno solo l'accesso in lettura. Tramite gli item di Reiser4, potete suddividere questo file in una serie di items (un item per utente) e dare il permesso agli utenti o applicazioni di modificare i propri dati, ma non di accedere ai dati di altri utenti. Questo approccio ha dei risvolti possitivi sia per la sicurezza che la flessibilità.

Scalabilità grazie ai plug-in
In Reiser4 molte funzionalità del file system ed anche funzionalità esterne a cui ricorrono solitamente i file system sono stati implementati sotto forma di plug-in. Questi plug-in possono essere integrati in modo del tutto semplice nel sistema di

base, quindi non si dovrà ricompilare il kernel o riformattare il disco rigido per intergrare delle nuove funzionalità al vostro file system.

Layout del file system ottimizzato grazie all'allocazione ritardata
Alla stregua di XFS, Reiser4 supporta l'allocazione posposta. Si veda Sezione 34.2.7, «XFS» (p. 548); questa funzionalità, se utilizzata per i metadata, contribuisce ad un miglior layout in generale.

34.2.6 JFS

JFS, il *Journaling File System*, è stato sviluppato da IBM per AIX. Nell'estate del 2000 esce la prima versione beta di JFS per Linux. La versione 1.0.0 è stata rilasciata nel 2001. JFS è tagliato per ambienti server con una elevata velocità di trasferimento dei dati (ingl. throughput), visto che in questo ambito quello che conta sono in prima linea le prestazioni. Essendo un file system a 64 bit, JFS supporta file voluminosi e partizioni (LFS ovvero Large File Support), caratteristica che lo qualifica ulteriormente per l'utilizzo in ambito server.

Se consideriamo più attentamente JFS scopriremo anche il motivo per cui questo file system si adatta bene ad un server Linux:

Journaling efficace
JFS segue alla stregua di ReiserFS l'approccio « metadata only». Al posto di una verifica dettagliata vengono rilevati solo le modifiche apportate ai meta-dati dovute a recenti attività del file system. Questo permette di velocizzare considerevolmente il ripristino. Attività contemporanee che richiedono diversi registrazioni di protocollo possono essere raccolte in un cosiddetto commit di gruppo, laddove il calo dal punto di vista della prestazione del file system viene compensato dal processo di scrittura multipla.

Efficace amministrazione delle directory
JFS si orienta alla struttura della directory. Nel caso di piccole directory consente di salvare direttamente il contenuto della directory nel suo inode. Per directory più capienti utilizza alberi bilanciati (ingl. B^+trees) che semplificano notevolmente l'amministrazione delle directory.

Miglior sfruttamento della memoria attraverso l'allocazione dinamica degli inode
Sotto Ext2 dovete indicare a priori la densità degli inode (memoria occupata da informazioni di natura amministrativa). Questo impone un limite massimo di file o

directory per il vostro file system. Con JFS invece la memoria inode viene assegnata dinamicamente e gli esuberi vengono subito messi nuovamente a disposizione del sistema.

34.2.7 XFS

Originariamente pensato come file system per il proprio sistema operativo IRIX, XFS è stato concepito dalla SGI già agli inizi degli anni '90 come journaling file system a 64 bit ad alte prestazioni per rispondere alle sempre crescenti richieste rivolte ad un file system moderno. XFS si adatta bene per file di una certa dimensione e dà prova di buona performance su hardware high-end. Comunque anche nel caso di XFS il tallone di Achille è rappresentato, come già per ReiserFS, dal fatto che XFS si concentra maggiormente sulla integrità dei meta-dati e meno sulla integrità dei dati.

Se osserviamo da vicino alcune funzionalità centrali di XFS vedremo il perché esso rappresenta una valida alternativa ad altri journaling file system in ambito della elaborazione dati high-end.

Alta scalabilità grazie agli «allocation groups»
Al momento della generazione di un file system XFS, il block device del file system viene suddiviso in otto o più settori lineari di ugual misura, detti «allocation groups» che chiameremo gruppi di allocazione. Ogni «gruppo di allocazione» gestisce gli inode e la memoria libera. I gruppi di allocazione sono in pratica dei «file system nei file system». Visto che i gruppi di allocazione sono in una certa misura autonomi, il kernel ha la possibilità di indirizzarne contemporaneamente più di uno. Ecco "il segreto" della alta scalabilità di XFS. Questa suddivisione in gruppi di allocazione è particolarmente indicata per sistemi multi-processore.

Alte prestazioni grazie ad una efficace amministrazione della memoria
La memoria libera e gli inode vengono gestiti da alberi B^+ all'interno dei gruppi di allocazione. Gli alberi B^+ contribuiscono in maniera determinante alla performance e alla scalabilità di XFS. Una caratteristica di XFS unica nel suo genere è la *delayed allocation*. XFS elabora l'assegnazione della memoria (ingl. allocation) bipartendo il processo. Una transazione «sospesa» viene memorizzata nella RAM e riservato il corrispondente spazio di memoria. XFS non stabilisce subito dove precisamente memorizzare i dati (cioè in quali blocchi del file system). Questa decisione viene rinviata il più possibile. Così file temporanei di breve durata non vengono scritti sul disco, visto che al momento di determinare la loro locazione sul disco sono già obsoleti. In tal modo XFS aumenta le prestazioni e riduce la frammentazione del

file system. Dato però che una allocazione differita comporta un minor numero di accessi in scrittura rispetto ad altri file system, è probabile che la perdita di dati in seguito al verificarsi di un crollo durante il processo di scrittura risulterà essere maggiore.

Pre-allocazione per evitare la frammentazione del file system
Prima di scrivere i dati nel file system, XFS riserva lo spazio necessario per il file (ingl. preallocate). In questo modo si riduce notevolmente la frammentazione del file system, e si aumenta la performance, dato che il contenuto di un file non viene distribuito più lungo tutto il file system.

34.3 Ulteriori file system supportati

Tabella 34.1 *Tipi di file system sotto Linux*

`cramfs`	*Compressed ROM file system*: un file system compresso con accesso in lettura per ROM.
`hpfs`	*High Performance File System*: il file system standard di OS/2—supportato solo nella modalità di lettura.
`iso9660`	File system standard dei CD-Rom.
`minix`	File system per il mount di file system per dischetti.
`msdos`	*fat*, il file system utilizzato originariamente da DOS, oggi utilizzato da vari sistemi operativi.
`ncpfs`	File system per il mount di volumi Novell tramite la rete.
`nfs`	*Network File System*: in questo caso sussiste la possibilità di memorizzare i dati su un computer qualsiasi nella rete e di accedervi tramite la rete.
`smbfs`	*Server Message Block*: viene usato p.es. Windows per accedere a file tramite rete.

`sysv`	Viene utilizzato sotto SCO UNIX, Xenix e Coherent (sistemi commerciali UNIX per PC).
`ufs`	Viene utilizzato da BSD, SunOS e NeXTstep. Viene supportato solo nella modalità di lettura.
`umsdos`	*UNIX on MSDOS*: basato su un normale file system `fat`. Generando file speciali si ottengono funzionalità UNIX (permessi, link, file con nomi lunghi).
`vfat`	*Virtual FAT*: estensione del file system `fat` (supporta lunghi nomi di file).
`ntfs`	*Windows NT file system*, accesso in sola lettura.

34.4 Large File Support sotto Linux

Originariamente Linux supportava file fino a 2 GByte che bastava fino a che non si intendeva gestire delle voluminose banche dati con Linux. Visto il crescente significato della amministrazione di banche dati sotto Linux, o gestione dei dati audio e video etc, il kernel e la libreria GNU C sono stati modificati in modo da supportare file che superano il limite di 2 GByte. Vennero introdotte nuove interfacce che possono essere utilizzate dalle applicazioni. Oggi (quasi) tutti i principali file system supportano LFS che permette elaborazione di dati high-end. Tabella 34.2, «Dimensione massima dei file system(on-disk format)» (p. 550) offre una rassegna dei limiti di file e file system Linux.

Tabella 34.2 *Dimensione massima dei file system(on-disk format)*

File system	Dim. file mass.	Dim. mass. file system
Ext2 o Ext3 (1 kB dim. di blocco)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 o Ext3 (2 kB dim. di blocco)	2^{38} (256 GB)	2^{43} (8 TB)
Ext2 o Ext3 (4 kB dim. di blocco)	2^{41} (2 TB)	2^{44} (16 TB)

File system	Dim. file mass.	Dim. mass. file system
Ext2 o Ext3 (8 kB dim. di blocco) (sistemi con pages di 8 kB (come Alpha)	2^{46} (64 TB)	2^{45} (32 TB)
ReiserFS v3	2^{46} (64 GB)	2^{45} (32 TB)
XFS	2^{63} (8 EB)	2^{63} (8 EB)
JFS (512 byte dim. di blocco)	2^{63} (8 EB)	2^{49} (512 TB)
JFS (4 kB dim. di blocco)	2^{63} (8 EB)	2^{52} (4 PB)
NFSv2 (lato client)	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3 (lato client)	2^{63} (8 EB)	2^{63} (8 EB)

IMPORTANTE: Limiti del kernel Linux

La tabella Tabella 34.2, «Dimensione massima dei file system(on-disk format)» (p. 550) indica i limiti dell' on-disk format. La dimensione massima di un file e di un file system processata correttamente dal Kernel 2.6 sottosta alle seguenti restrizioni:

Dimensione del file:
File e block device non possono superare i 2 TB (2^{41} byte) su sistemi a 32 bit.

Dimensione del file system:
file system possono raggiungere una dimensione di 2^{73} byte. Questo limite non viene (ancora) sfruttato a fondo da nessun hardware attualmente reperibile.

34.5 Ulteriori fonti di informazioni

Ogni dei file system descritti ha un proprio sito web, dove è possibile reperire ulteriori informazioni grazie a mailing list, documentazione e FAQ.

- http://e2fsprogs.sourceforge.net/ext2.html
- http://www.zipworld.com.au/~akpm/linux/ext3/
- http://www.namesys.com/
- http://oss.software.ibm.com/developerworks/opensource/jfs/
- oss.sgi.com/projects/xfs/

Un tutorial completo dedicato ai file system Linux è rappresentato dall' *IBM developerWorks*; l'indirizzo è:http://www-106.ibm.com/developerworks/library/l-fs.html. Sotto *Linuxgazette*: http://www.linuxgazette.com/issue55/florido.html troverete un confronto dei vari journaling file system sotto Linux nell'articolo di Juan I. Santos Florido. Per un compendio di LFS sotto Linux visitate le pagine dedicate a LFS di Andreas Jaeger: http://www.suse.de/~aj/linux_lfs.html

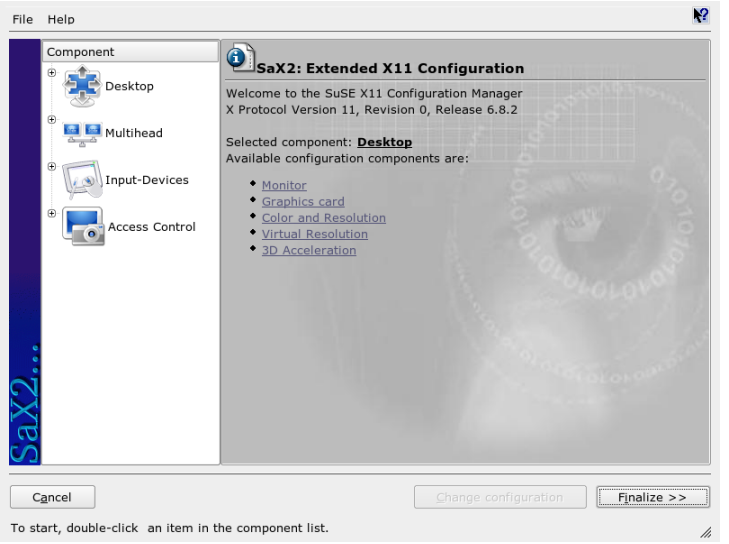
35 X Window System

X Window System (X11) è lo standard di fatto per le interfacce utente grafiche in UNIX. X è un sistema di rete che consente di visualizzare applicazioni avviate in un host su un altro host connesso al primo tramite qualsiasi tipo di rete (LAN o Internet). In questo capitolo vengono descritte le procedure di configurazione e ottimizzazione dell'ambiente X Window System. Vengono inoltre fornite informazioni generali relative all'uso di font in SUSE Linux e viene illustrata la configurazione di OpenGL e 3D.

35.1 Configurazione di X11 con SaX2

La comunicazione tra l'hardware e il software viene gestita tramite l'interfaccia utente grafica, ovvero il server X. Nei desktop, ad esempio KDE e GNOME, nonché in numerosi gestori delle finestre, il server X viene utilizzato per l'interazione con l'utente. L'interfaccia utente grafica viene inizialmente configurata durante l'installazione. Per modificare successivamente le impostazioni è possibile utilizzare l'apposito modulo del centro controllo YaST oppure eseguire SaX2 manualmente dalla riga di comando con il comando `sax2`. Nella finestra principale di SaX2 sono raggruppati i singoli moduli del centro controllo YaST.

Figura 35.1 *Finestra principale di SaX2.*



Nel riquadro di spostamento a sinistra sono disponibili sei elementi, per ognuno dei quali viene visualizzata la rispettiva finestra di configurazione del centro controllo YaST. Le sezioni descritte di seguito sono contenute nel Capitolo *Configurazione di sistema con YaST* (↑Avvio).

Monitor

Per una descrizione della configurazione della scheda grafica e del monitor, vedere la Sezione «Proprietà monitor e scheda» (Capitolo 3, *Configurazione di sistema con YaST*, ↑Avvio).

Mouse

Per una descrizione della configurazione del mouse nell'ambiente grafico, vedere la Sezione «Proprietà mouse» (Capitolo 3, *Configurazione di sistema con YaST*, ↑Avvio).

Tastiera

Per una descrizione della configurazione della tastiera nell'ambiente grafico, vedere la Sezione «Proprietà tastiera» (Capitolo 3, *Configurazione di sistema con YaST*, ↑Avvio).

Tavoletta
Per una descrizione della configurazione della tavoletta grafica, vedere la Sezione «Proprietà tavoletta» (Capitolo 3, *Configurazione di sistema con YaST*, ↑Avvio).

Schermo tattile
Per una descrizione della configurazione dello schermo tattile, vedere la Sezione «Proprietà schermo tattile» (Capitolo 3, *Configurazione di sistema con YaST*, ↑Avvio).

VNC
Per una descrizione della configurazione di VNC, vedere la Sezione «Proprietà accesso remoto» (Capitolo 3, *Configurazione di sistema con YaST*, ↑Avvio).

35.2 Ottimizzazione della configurazione di X

X.Org è un'implementazione open source di X Window System ulteriormente sviluppata dalla X.Org Foundation, che si occupa inoltre dello sviluppo di nuove tecnologie e standard per X Window System.

Per utilizzare al meglio l'hardware disponibile, ad esempio mouse, schede grafiche, monitor e tastiere, è possibile ottimizzarne la configurazione manualmente. Di seguito vengono illustrati alcuni aspetti delle procedure di ottimizzazione. Per informazioni sulla configurazione di X Window System, esaminare i file contenuti nella directory `/usr/share/doc/packages/Xorg` e `man xorg.conf`.

AVVERTIMENTO

È opportuno prestare la massima attenzione alle operazioni che si eseguono durante la configurazione di X Window System. In nessun caso avviare X Window System prima di aver completato la configurazione. L'errata configurazione del sistema può infatti causare danni irreparabili all'hardware, in particolare ai monitor a frequenza fissa. Gli autori della presente pubblicazione e SUSE Linux declinano qualsiasi responsabilità per eventuali danni. Le informazioni riportate sono state attentamente verificate. Tuttavia ciò non costituisce garanzia alcuna

che tutti i metodi descritti siano esenti da errori e che non comportino il danneggiamento dell'hardware.

Per default, il file `xorg.conf` viene creato dai programmi SaX2 e xorgconfig in `/etc/X11`. Si tratta del file di configurazione principale di X Window System in cui sono incluse tutte le impostazioni relative alla scheda grafica, al mouse e al monitor.

Nei paragrafi seguenti viene descritta la struttura del file di configurazione `/etc/X11/xorg.conf`. Il file è costituito da diverse sezioni, ognuna delle quali relativa a uno specifico aspetto della configurazione. Ogni sezione inizia con la parola chiave `Section <designation>` e termina con `EndSection`. Le sezioni si presentano nella forma seguente:

```
Section designation
  entry 1
  entry 2
  entry n
EndSection
```

I tipi di sezione disponibili sono elencati nella Tabella 35.1, «Sezioni incluse nel file /etc/X11/xorg.conf» (p. 556).

Tabella 35.1 *Sezioni incluse nel file /etc/X11/xorg.conf*

Tipo	Descrizione
`Files`	In questa sezione vengono descritti i percorsi utilizzati per i font e la mappa colori RGB.
`ServerFlags`	In questa sezione vengono impostati gli switch generali.
`InputDevice`	In questa sezione viene definita la configurazione dei dispositivi di input, ovvero tastiere e dispositivi speciali quali touchpad e joystick. I parametri principali di questa sezione sono `Driver` e le opzioni che definiscono `Protocol` e `Device`.
`Monitor`	In questa sezione viene descritto il monitor utilizzato. I singoli elementi di questa sezione sono il nome, a cui viene fatto riferimento più avanti nella definizione di `Screen`, `bandwidth` e i limiti della frequenza di sincronizzazione (`HorizSync` e `VertRefresh`). Le impostazioni sono espresse

Tipo	Descrizione
	in MHz, kHz e Hz. In genere, il server rifiuta qualsiasi modeline non conforme alle specifiche del monitor. Ciò impedisce che vengano inviate per errore al monitor frequenze troppo elevate.
`Modes`	I parametri modeline per le risoluzioni dello schermo vengono memorizzati in questa sezione. Tali parametri possono essere calcolati da SaX2 in base ai valori forniti dall'utente e in genere non è necessario modificarli. È tuttavia possibile intervenire manualmente se, ad esempio, si desidera collegare un monitor a frequenza fissa. Per informazioni sul significato dei singoli valori numerici, esaminare il file HOWTO `/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz`.
`Device`	In questa sezione viene definita una scheda grafica specifica a cui viene fatto riferimento mediante un nome descrittivo.
`Screen`	Questa sezione riunisce `Monitor` e `Device`, che consentono di specificare tutte le impostazioni necessarie per X.Org. Nella sottosezione `Display` è possibile specificare le dimensioni dello schermo virtuale (`Virtual`), nonché `ViewPort` e `Modes` utilizzati per lo schermo.
`ServerLayout`	In questa sezione viene definito il layout di una configurazione singola o multihead e vengono associati i dispositivi di input `InputDevice` e quelli di visualizzazione `Screen`.

`Monitor`, `Device` e `Screen` sono illustrati più avanti. Per ulteriori informazioni sulle altre sezioni, vedere la documentazione relativa a `X.Org` e `xorg.conf`.

È possibile includere diverse sezioni `Monitor` e `Device` nel file `xorg.conf`, nonché più sezioni `Screen`. La sezione `ServerLayout` successiva determina quale sezione verrà utilizzata.

35.2.1 Sezione Screen

Esaminare innanzitutto la sezione Screen, che combina una sezione Monitor con una sezione Device e determina le impostazioni relative alla risoluzione e alla profondità di colore da utilizzare. Una sezione Screen può presentarsi in modo analogo a quella riportata nell'Esempio 35.1, «Sezione Screen del file /etc/X11/xorg.conf» (p. 558).

Esempio 35.1 *Sezione Screen del file /etc/X11/xorg.conf*

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

La riga `Identifier`, in questo caso `Screen[0]`, consente di assegnare alla sezione un nome a cui è possibile fare riferimento in modo univoco nella sezione `ServerLayout` successiva. Le righe `Device` e `Monitor` consentono di specificare la scheda grafica e il monitor appartenenti alla definizione. Si tratta di collegamenti alle sezioni `Device` e `Monitor` con i rispettivi nomi o *identificatori*. Queste sezioni vengono descritte in dettaglio più avanti.

Utilizzare l'impostazione `DefaultDepth` per selezionare la profondità di colore che deve essere utilizzata dal server se non ne viene specificata una all'avvio. A ogni impostazione di profondità del colore corrisponde una sottosezione `Display`. La parola chiave `Depth` consente di assegnare la profondità di colore valida per la

sottosezione. I valori consentiti per `Depth` sono 8, 15, 16 e 24. I valori validi dipendono dal modulo del server X.

Dopo aver specificato il valore relativo alla profondità di colore, nella sezione `Modes` viene impostato un elenco di risoluzioni. L'elenco viene letto dal server X da sinistra a destra e per ogni risoluzione viene eseguita la ricerca della `Modeline` appropriata nella sezione `Modes`. `Modeline` dipende dalle caratteristiche del monitor e della scheda grafica. Le impostazioni incluse in `Monitor` consentono di determinare la `Modeline` risultante.

La prima risoluzione rilevata è la `modalità di default`. Per passare al valore successivo a destra nell'elenco, premere Ctrl + Alt + + sul tastierino numerico. Per passare al valore successivo a sinistra, premere Ctrl + Alt + – sul tastierino numerico. In questo modo è possibile modificare la risoluzione mentre X è in esecuzione.

L'ultima riga della sottosezione `Display` con `Depth 16` fa riferimento alle dimensioni dello schermo virtuale. Il valore massimo consentito non dipende dalla risoluzione massima del monitor, ma dipende dalla quantità di memoria installata nella scheda grafica e dalla profondità di colore desiderata. Poiché le schede grafiche più recenti dispongono di una considerevole quantità di memoria video, è possibile creare desktop virtuali di grandi dimensioni. Tuttavia, se si utilizza la maggior parte della memoria video per il desktop virtuale, potrebbe non essere più possibile utilizzare le funzionalità 3D. Se la scheda dispone di 16 MB di RAM video, ad esempio, è possibile impostare la risoluzione dello schermo virtuale su un valore massimo pari a 4096x4096 pixel con profondità di colore a 8 bit. È comunque sconsigliabile riservare tutta la memoria disponibile allo schermo virtuale, in particolare con le schede accelerate, poiché la memoria della scheda viene utilizzata anche per la memorizzazione nella cache di font e immagini.

35.2.2 Sezione Device

Nella sezione Device viene descritta una scheda grafica specifica. `xorg.conf` può contenere un numero illimitato di voci Device, a condizione che a ognuna venga assegnato un nome specifico tramite la parola chiave `Identifier`. Di norma, se si dispone di più schede grafiche, le sezioni vengono semplicemente numerate in progressione, ovvero `Device[0]`, `Device[1]` e così via. Nel file seguente viene illustrata una parte della sezione `Device` di un computer in cui è installata la scheda grafica PCI Matrox Millennium.

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

Se si utilizza SaX2 per eseguire la configurazione, la sezione Device si presenterà in modo analogo a quella nell'esempio precedente. `Driver` e `BusID` dipendono dall'hardware installato nel computer e vengono rilevati automaticamente da SaX2. `BusID` identifica lo slot PCI o AGP in cui è installata la scheda grafica e corrisponde all'ID visualizzato tramite il comando lspci. Per il corretto funzionamento del server X, il valore deve essere in formato decimale. Tuttavia, nell'output del comando lspci tale impostazione viene visualizzata in formato esadecimale.

Il parametro `Driver` consente di specificare il driver da utilizzare con la scheda grafica. Nel caso della scheda Matrox Millennium, il modulo driver è denominato `mga`. Nel server X viene quindi eseguita una ricerca in `ModulePath` definito nella sezione `Files` nella sottodirectory `drivers`. In un'installazione standard, si tratta della directory `/usr/X11R6/lib/modules/drivers`. Al nome del file viene aggiunto il suffisso `_drv.o`. Nel caso del driver `mga` viene quindi caricato il file `mga_drv.o`.

È possibile impostare opzioni aggiuntive per controllare il funzionamento del server X o del driver. Ad esempio, l'opzione `sw_cursor`, impostata nella sezione Device, consente di disattivare la gestione hardware del cursore e attivare la gestione software. Le opzioni effettivamente disponibili dipendono dal modulo del driver ed è possibile individuarle nei file di descrizione di tali moduli nella directory `/usr/X11R6/lib/X11/doc`. Le opzioni generali valide vengono inoltre descritte nella documentazione (`man xorg.conf` e `man X.Org`).

35.2.3 Sezioni Monitor e Modes

In ogni sezione `Monitor` e `Modes` viene descritto un monitor in modo analogo alla sezione `Device`. Il file di configurazione `/etc/X11/xorg.conf` può contenere un numero illimitato di sezioni `Monitor`. Nella sezione ServerLayout viene indicata la sezione `Monitor` rilevante.

È consigliabile che le definizioni dei monitor vengano impostate solo da utenti esperti. Le righe modeline rappresentano una parte importante delle sezioni `Monitor`. Le

modeline consentono infatti di impostare i valori di temporizzazione orizzontale e verticale relativi alle rispettive risoluzioni. Nella sezione `Monitor` vengono memorizzate le proprietà del monitor, in particolare le frequenze consentite.

AVVERTIMENTO

Se non si conoscono approfonditamente le funzioni di schede grafiche e monitor, è consigliabile non modificare le modeline poiché valori errati potrebbero causare gravi danni al monitor.

Prima di sviluppare descrizioni di monitor personalizzate, è consigliabile leggere con attenzione la documentazione disponibile in `/usr/X11/lib/X11/doc`. A questo proposito, la sezione relativa alle modalità video è di particolare importanza poiché contiene informazioni dettagliate sul funzionamento dell'hardware e sulle modalità di creazione delle modeline.

Nei sistemi attuali, l'impostazione manuale delle modeline non è necessaria. Se si utilizza un monitor di tipo multisync, le frequenze consentite e le impostazioni di risoluzione ottimali vengono rilevate automaticamente dal server X tramite DDC (Direct Display Channel), come illustrato nella sezione sulla configurazione di SaX2. Se per qualsiasi motivo ciò non risulta possibile, utilizzare una delle modalità VESA (Video Electronics Standards Association) incluse nel server X. Queste modalità sono compatibili praticamente con tutte le combinazioni di monitor e schede grafiche.

35.3 Installazione e configurazione di font

L'installazione di font aggiuntivi In SUSE Linux è un'operazione di facile esecuzione. È sufficiente, infatti, copiare i font in qualsiasi directory nel percorso dei font di X11 (vedere la Sezione 35.3.2, «Font di base di X11» (p. 566)). Per poter utilizzare i font è necessario installarli in una sottodirectory delle directory configurate in `/etc/fonts/fonts.conf` (vedere la Sezione 35.3.1, «Xft» (p. 562)).

Se si dispone dei privilegi di `root`, è possibile copiare i file dei font manualmente in una directory appropriata, ad esempio `/usr/X11R6/lib/X11/fonts/truetype`. In alternativa, è possibile eseguire questo task tramite l'utility di installazione dei font disponibile nel centro controllo KDE. Il risultato di tali operazioni è identico.

È inoltre possibile creare collegamenti simbolici anziché copiare i font effettivi. È possibile, ad esempio, eseguire questo tipo di operazione per utilizzare i font con licenza disponibili in una partizione Windows montata. In questo caso, eseguire `SuSEconfig --module fonts`.

`SuSEconfig --module fonts` consente di eseguire lo script `/usr/sbin/fonts-config` tramite il quale viene gestita la configurazione dei font. Per informazioni sul funzionamento di questo script, vedere la relativa documentazione (`man fonts-config`).

La procedura di installazione è identica per i font bitmap, TrueType e OpenType, nonché per i font Type1 (PostScript). È possibile installare questi tipi di font in qualsiasi directory. Per installare i font CID-keyed è invece necessario procedere in modo diverso. Per informazioni, vedere la Sezione 35.3.3, «Font CID-keyed» (p. 567).

In X.Org sono inclusi due sistemi di font completamente diversi tra loro, ovvero il *sistema di font di base di X11* e il nuovo sistema *Xft e fontconfig*. Nelle sezioni seguenti vengono brevemente descritti tali sistemi.

35.3.1 Xft

I programmatori che hanno progettato il sistema Xft si sono accertati fin dall'inizio che i font ridimensionabili dotati di antialias fossero supportati correttamente. Se si utilizza Xft, il rendering dei font viene eseguito dall'applicazione che li utilizza e non dal server X, come invece avviene nel caso del sistema di font di base di X11. In questo modo, l'applicazione in uso può accedere ai file effettivi dei font e controllare l'intero processo di rendering dei glifi. Ciò è essenziale per la visualizzazione corretta del testo in numerose lingue. L'accesso diretto ai file dei font risulta particolarmente utile ai fini dell'incorporazione dei font per la stampa in modo da garantire la conformità dell'output di stampa a quello dello schermo.

In SUSE Linux, Xft viene utilizzato per default negli ambienti desktop KDE e GNOME, in Mozilla, nonché in numerose altre applicazioni. Il sistema Xft viene attualmente utilizzato da un numero di applicazioni superiore rispetto al meno recente sistema di font di base di X11.

Per individuare i font e determinarne la modalità di rendering nell'ambito del sistema Xft viene utilizzata la libreria fontconfig. Le proprietà di fontconfig vengono definite nel file di configurazione globale `/etc/fonts/fonts.conf` e nel file di

configurazione specifico dell'utente `~/.fonts.conf`. Entrambi i file di configurazione di fontconfig devono iniziare con:

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

e terminare con

```
</fontconfig>
```

Per specificare ulteriori directory in cui eseguire le ricerche dei font, aggiungere righe del tipo seguente:

```
<dir>/usr/local/share/fonts/</dir>
```

In genere, questo tipo di modifica non è necessario. Per default, la directory specifica dell'utente `~/.fonts` è già presente in `/etc/fonts/fonts.conf`. È quindi sufficiente copiare i font aggiuntivi nella directory `~/.fonts` per installarli.

È inoltre possibile definire regole in base alle quali viene determinato l'aspetto dei font. È possibile, ad esempio, immettere:

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

per disabilitare l'antialias per tutti i font oppure

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

per disabilitare l'antialias solo per font specifici.

Per default, nella maggior parte delle applicazioni vengono utilizzati i nomi di font `sans-serif` (o l'equivalente `sans`), `serif` o `monospace`. Si tratta di alias che vengono risolti nei font appropriati in base all'impostazione della lingua, non di font effettivi.

Gli utenti possono aggiungere facilmente regole a `~/.fonts.conf` per risolvere tali alias nei font desiderati:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Poiché gli alias vengono utilizzati per default dalla maggior parte delle applicazioni, questo aspetto interessa quasi tutto il sistema. Ciò significa, inoltre, che nella maggior parte dei casi è possibile utilizzare i font desiderati senza la necessità di modificarne le impostazioni per le singole applicazioni.

Utilizzare il comando `fc-list` per determinare quali font sono installati e disponibili. Il comando `fc-list` consente ad esempio di visualizzare un elenco di tutti i font. Per individuare i font ridimensionabili (`:outline=true`) che contengono tutti i glifi necessari per la lingua ebraica (`:lang=he`), con l'indicazione dei nomi (`family`), dello stile (`style`), dello spessore (`weight`), nonché i nomi dei rispettivi file, immettere il comando seguente:

```
fc-list ":lang=he:outline=true" family style weight
```

L'output di questo comando risulterà analogo al seguente:

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
FreeSans.ttf: FreeSans:style=Medium:weight=80
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
```

```
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

Parametri importanti che possono essere utilizzati con il comando `fc-list`:

Tabella 35.2 *Parametri di fc-list*

Parametro	Descrizione e valori consentiti
`family`	Nome della famiglia di font, ad esempio `FreeSans`.
`foundry`	Il produttore del font, ad esempio `urw`.
`style`	Lo stile del font, ad esempio `Medium`, `Regular`, `Bold`, `Italic`, `Heavy`.
`lang`	La lingua supportata dal font, ad esempio `de` per il tedesco, `ja` per il giapponese, `zh-TW` per il cinese tradizionale o `zh-CN` per il cinese semplificato.
`weight`	Lo spessore del font, ad esempio `80` per normale, `200` per il grassetto.
`slant`	L'inclinazione, in genere `0` per nessuna e `100` per il corsivo.
`file`	Il nome del file contenente il font.
`outline`	`true` per i font vettoriali, `false` gli altri tipi di font.
`scalable`	`true` per i font ridimensionabili, `false` gli altri tipi di font.
`bitmap`	`true` per i font bitmap, `false` per gli altri tipi di font.
`pixelsize`	La dimensione dei font espressa in pixel. Per quanto concerne fc-list, questa opzione è valida solo per i font bitmap.

35.3.2 Font di base di X11

Il sistema di font di base di X11 supporta attualmente sia i font bitmap sia i font ridimensionabili, ad esempio i font Type1, TrueType, OpenType e CID-keyed. Per un certo periodo sono stati supportati anche i font Unicode. Il sistema di font di base di X11 fu sviluppato nel 1987 per X11R1 per consentire l'elaborazione dei font bitmap monocromatici. Tutte le estensioni citate in precedenza sono state aggiunte successivamente.

I font ridimensionabili sono supportati senza antialias né rendering dei subpixel. Il caricamento di font ridimensionabili di grandi dimensioni con glifi per numerose lingue può inoltre richiedere una notevole quantità di tempo. Anche l'utilizzo dei font Unicode può rallentare il sistema e richiedere più memoria.

Il sistema di font di base di X11 presenta alcuni svantaggi. Si tratta infatti di un sistema obsoleto che non consente un ulteriore sviluppo significativo. Sebbene sia necessario mantenerlo per motivi di compatibilità con le versioni precedenti, è consigliabile utilizzare il più moderno sistema Xft e fontconfig.

Per il corretto funzionamento del server X, è necessario che quest'ultimo sia in grado di individuare i font disponibili nel sistema. A questo scopo, viene utilizzata la variabile FontPath che contiene il percorso di tutte le directory dei font di sistema valide. In ogni directory è presente un file denominato `fonts.dir` nel quale sono elencati i font disponibili nella directory stessa. FontPath viene generata dal server X all'avvio. Viene quindi eseguita una ricerca del file `fonts.dir` valido in ognuna delle voci di `FontPath` nel file di configurazione `/etc/X11/xorg.conf`. Queste voci si trovano nella sezione `Files`. È possibile visualizzare la variabile FontPath effettiva mediante il comando `xset q`. xset consente inoltre di modificare il percorso al runtime. Per aggiungere un nuovo percorso, utilizzare `xset +fp <path>`. Per rimuovere un percorso indesiderato, utilizzare `xset -fp <path>`.

Se il server X è già attivo, è possibile rendere disponibili i font appena installati nelle directory montate mediante il comando `xset fp rehash`. Questo comando viene eseguito da `SuSEconfig --module fonts`. Poiché il comando `xset` deve accedere al server X quando quest'ultimo è in esecuzione, è necessario che `SuSEconfig --module fonts` venga avviato da una shell che dispone dell'accesso al server X in esecuzione. Il modo più semplice per eseguire questa operazione consiste nell'assumere le autorizzazioni dell'utente `root` e immettere il comando `su`, nonché la relativa password. Il comando `su` consente di trasferire le autorizzazioni di accesso

dell'utente che ha avviato il server X alla shell root. Per verificare che i font siano stati installati correttamente e siano disponibili tramite il sistema di font di base di X11, utilizzare il comando `xlsfonts` per visualizzarne un elenco.

Per default, in SUSE Linux vengono utilizzate le impostazioni internazionali UTF-8. È pertanto consigliabile utilizzare i font Unicode, ovvero quelli il cui nome termina con `iso10646-1` nell'output di `xlsfonts`. È possibile visualizzare l'elenco di tutti i font Unicode disponibili mediante `xlsfonts | grep iso10646-1`. La maggior parte dei font Unicode disponibili in SUSE Linux include almeno i glifi necessari per le lingue europee (precedentemente indicate con la codifica `iso-8859-*`).

35.3.3 Font CID-keyed

A differenza degli altri tipi di font, i font CD-keyed non possono essere installati in una directory qualsiasi. È necessario installare questo tipo di font in `/usr/share/ghostscript/Resource/CIDFont`. In effetti, ciò non è rilevante per Xft e fontconfig, ma è essenziale per Ghostscript e per il sistema di font di base di X11.

SUGGERIMENTO

Per ulteriori informazioni sui font in X11, visitare il sito `http://www.xfree86.org/current/fonts.html`.

35.4 Configurare OpenGL/3D

35.4.1 Supporto hardware

SUSE Linux include molti driver OpenGL per il supporto hardware 3D. Ecco una rassegna nella Tabella 35.3, «Hardware 3D supportato» (p. 567).

Tabella 35.3 *Hardware 3D supportato*

Driver OpenGL	Hardware supportato
nVidia	Chip nVidia: tutti tranne Riva 128(ZX)

Driver OpenGL	Hardware supportato
DRI	3Dfx Voodoo Banshee, 3Dfx Voodoo-3/4/5, Intel i810/i815/i830M, Intel 845G/852GM/855GM/865G/915, Matrox G200/G400/G450/G550, ATI Rage 128(Pro)/Radeon (fino a 9250)

Se effettuate l'installazione tramite YaST, potete attivare il supporto 3D già durante l'installazione, se sono date le premesse. Nel caso dei chip grafici nVidia si deve installare innanzitutto il driver nVidia. Selezionate a riguardo durante il processo di installazione la patch del driver nVidia in YOU (YaST Online Update). Per motivi di licenza, purtroppo non ci è consentito accludere il driver nVidia.

Se eseguite un update o dovete impostare una scheda grafica aggiuntiva 3Dfxi (Voodoo Graphics o Voodoo-2) la procedura cambia. In tema di supporto supporto hardware 3D tutto dipende dal driver OpenGL utilizzato. Per maggiori dettagli proseguite nella lettura.

35.4.2 Driver OpenGL

I driver OpenGL nVidia e DRI possono essere configurati comodamente con SaX2. Tenete presente per una scheda nVidia va installato innanzitutto il driver nVidia. Con il comando `3Ddiag`, potete verificare la correttezza della configurazione di nVidia o DRI.

Per ragioni di sicurezza, solo gli utenti appartenenti al gruppo `video` possono accedere all'hardware 3D. Accertatevi che tutti gli utenti che lavorano localmente sul computer appartengano a questo gruppo. In caso contrario, per le applicazioni OpenGL si ripiegherà sul *software rendering fallback* del driver OpenGL che è più lento. Usate il comando `id` per verificare se l'utente attuale appartiene al gruppo `video`. Se non appartiene al gruppo, potete usare YaST per aggiungere l'utente al gruppo.

35.4.3 Tool di diagnosi 3Ddiag

Per controllare la configurazione 3D su SUSE Linux vi è lo strumento di diagnosi 3Ddiag. Si tratta di uno strumento a riga di comando che deve essere invocato da un terminale. Eseguite `3Ddiag -h` per avere le opzioni ammesse per 3Ddiag.

Per verificare la configurazione di X.Org, questo tool controlla se sono installati i pacchetti richiesti per il supporto 3D e se viene utilizzata la corretta libreria OpenGL e le corrette estensioni GLX. Seguite le istruzioni di 3Ddiag se vengono visualizzati dei messaggi failed. Se tutto è andato per il verso giusto verranno visualizzati solo messaggi done.

35.4.4 Testare OpenGL

A tal fine possono essere usati accanto a `glxgears` giochi come `tuxracer` e `armagetron` (pacchetti omonimi). Se il supporto 3D è stato attivato, tali giochi dovrebbero essere giocabili in modo abbastanza fluido su un computer relativamente recente. Senza supporto 3D ciò non ha senso (effetto moviola). Per vedere se l'accelerazione 3D è abilitata o meno, utilizzate il comando `glxinfo`: se l'output presenta un rigo con `direct rendering: Yes` , allora tale funzionalità è abilitata.

35.4.5 Risoluzione di alcuni possibili problemi

Se i risultati dei test a cui è stato sottoposto OpenGL 3D lasciano a desiderare (impossibile giocare in modo fluido), usate 3Ddiag per assicurarvi che non vi siano degli errori di configurazione (messaggi `failed`) ed eventualmente eliminateli. Se ciò non è di aiuto o non vi sono dei messaggi failed, date un'occhiata al file di log di X.Org.

Spesso troverete la riga `DRI is disabled` in `/var/log/Xorg.0.log`. L'esatta causa del problema può essere individuata solo analizzando attentamente il file di log, compito che a volta si rivela troppo difficile per un neofita.

In questi casi, spesso non vi sono degli errori di configurazione, poiché questi ultimi sarebbero già stati rilevati da 3Ddiag. Perciò, a questo punto, non rimane che il software rendering fallback del driver DRI, che purtroppo non offre supporto per l'hardware 3D.

Si dovrebbe rinunciare al supporto 3D se vi sono degli errori di rappresentazione OpenGL o addirittura problemi di instabilità. Utilizzate SaX2 per disabilitare il supporto 3D.

35.4.6 Supporto all'installazione

A parte il `software rendering fallback` del driver DRI, in Linux tutti i driver OpenGL si trovano in fase di sviluppo e devono pertanto essere considerati in parte sperimentali. I driver sono inclusi nella distribuzione perché c'è una forte richiesta di funzionalità 3D sotto Linux. Considerando lo stato in parte sperimentale dei driver OpenGL, non possiamo però offrire alcun supporto all'installazione per la configurazione dell'accelerazione hardware 3D o fornire qualsiasi ulteriore assistenza per difficoltà in questo contesto. La configurazione di base dell'interfaccia utente grafica (X Window System) non include la configurazione dell'accelerazione hardware 3D. Speriamo comunque che questo capitolo fornisca una risposta a molte domande relative a questo argomento. Se avete delle difficoltà con il supporto hardware 3D, consigliamo in caso di dubbio di rinunciare al supporto 3D.

35.4.7 Ulteriore documentazione in linea

Per delle informazioni su DRI, consultate `/usr/X11R6/lib/X11/doc/README.DRI` (`xorg-x11-doc`). Per maggiori informazioni sull'installazione di driver nvidia rimandiamo al sito `http://ftp.suse.com/pub/suse/i386/supplementary/X/nvidia-installer-HOWTO.html`.

36 Autenticazione con PAM

I moduli di autenticazione aggiungibili, PAM, vengono utilizzati da Linux nel processo di autenticazione per costituire il livello che collega utente e applicazione. I moduli PAM sono disponibili in tutto il sistema e disponibili per tutte le applicazioni. Nel presente capitolo viene descritto il meccanismo di autenticazione modulare e la sua configurazione.

Gli amministratori di sistema e i programmatori hanno spesso l'esigenza di limitare l'accesso ad alcune aree del sistema o impedire l'utilizzo di alcune funzioni di un'applicazione. Senza il PAM, le applicazioni devono essere adattate in presenza di ogni nuovo meccanismo di autenticazione, come LDAP o SAMBA. Tuttavia tale processo è impegnativo dal punto di vista del tempo ed esposto a errori. Un modo per evitare questi svantaggi è quello di separare le applicazioni dal meccanismo di autenticazione e di delegare quest'ultimo a moduli a gestione unificata. In presenza di una richiesta di un nuovo schema di autenticazione, sarà sufficiente adattare o sviluppare un modulo PAM appropriato al programma in questione.

Ogni programma affidato al meccanismo PAM dispone di un proprio file di configurazione nella directory `/etc/pam.d/`*`nome_programma`*. Questi file definiscono i moduli PAM utilizzati per l'authentication. Inoltre, esistono dei file di configurazione globali per la maggior parte dei moduli PAM, sotto `/etc/security`, che definiscono il comportamento preciso di questi moduli; ad esempio `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf` e `time.conf`). L'applicazione che utilizza un modulo PAM in realtà invoca una serie di funzioni PAM, che a loro volta elaborano le informazioni del file di configurazione e restituiscono il risultato all'applicaizone invocante.

36.1 Struttura di un file di configurazione PAM

Ciascuna riga del file di configurazione PAM contiene un massimo di 4 colonne:

```
<Tipo di modulo> <Flag di controllo> <Percorso del modulo> <Opzioni>
```

I moduli PAM vengono elaborati in modalità stack. Il tipo di modulo varia a seconda dello scopo; ad esempio, un modulo verifica la parola d'ordine, un altro verifica l'ubicazione da cui si accede al sistema e un altro ancora legge le impostazioni specifiche all'utente. PAM è costituito da 4 diversi tipi di modulo:

`auth`
: Lo scopo di questo tipo di modulo è verificare l'autenticità dell'utente. Questa operazione viene di norma svolta tramite richiesta di una parola d'ordine, ma può essere effettuata anche tramite chip o verifiche biometriche (impronte digitali o iride).

`account`
: Questo tipo di modulo verifica se l'utente dispone dell'autorizzazione generale per utilizzare il servizio richiesto. Ad esempio, una tale verifica deve essere svolta per accertarsi che nessuno esegua un login con nome utente e parola d'ordine scaduti.

`password`
: Lo scopo di questo tipo di modulo è quello di abilitare la modifica di un token di authentication. Nella maggior parte dei casi, il token è una parola d'ordine.

`session`
: Questo tipo di modulo è responsabile della gestione e configurazione delle sessioni utente. Queste vengono aperte prima e dopo l'autenticazione per registrare i tentativi di login nei file di log del sistema e per configurare l'ambiente specifico dell'utente (conti e-mail, home directory, limiti del sistema, ecc.).

La seconda colonna contiene dei flag di controllo per pilotare il comportamento dei moduli avviati:

`required`
: Un modulo con un flag simile deve essere elaborato correttamente prima che possa avere luogo l'autenticazione. Se un modulo con flag `required` restituisce un

errore, vengono elaborati tutti gli altri moduli con lo stesso flag prima che il sistema invii all'utente un messaggio riguardo il fallito tentativo di autenticazione.

`requisite`
Anche i moduli con questo flag devono essere elaborati correttamente in modo analogo a quelli con flag `required`. Tuttavia, questo modulo restituisce immediatamente l'eventuale errore senza proseguire l'elaborazione di ulteriori moduli. In caso di elaborazione corretta, gli altri moduli vengono elaborati in successione analogamente a come avviene per i moduli con flag `required`. Il flag `requisite` può essere utilizzato come filtro di base per verificare l'esistenza di determinate condizioni essenziali per la corretta autenticazione.

`sufficient`
Dopo la corretta elaborazione di un modulo con flag simile, l'applicazione invocante riceve un messaggio immediato riguardo la riuscita e l'elaborazione di ulteriori moduli non avviene, a patto che non vi siano stati errori di precedenti moduli con flag `required`. L'errore di un modulo con flag `sufficient` non ha conseguenze dirette, nella misura in cui tutti i moduli successivi vengono elaborati nell'ordine.

`optional`
L'errore o riuscita di un modulo con un tale flag non ha nessuna conseguenza diretta. Risulta utile per i moduli destinati solo alla visualizzazione di messaggi (ad esempio per segnalare all'utente l'arrivo di posta) senza ulteriore elaborazione.

include
In presenza di questo flag, il file specificato come argomento viene inserito in questa ubicazione.

Il percorso del modulo non deve essere specificato in modo esplicito, a patto che il modulo si trovi nella directory di default `/lib/security` (per le piattaforme a 64 bit supportate da SUSE Linux, la directory è `/lib64/security`). L'opzione presente nella quarta colonna può essere `debug` (abilita le funzioni di debug) o `nullok` (consente l'utilizzo di parole d'ordine vuote).

36.2 Configurazione PAM per sshd

Per illustrare i meccanismi dietro le quinte di PAM, verrà preso come esempio pratico la configurazione PAM per sshd:

Esempio 36.1 *Configurazione PAM per sshd*

```
#%PAM-1.0
auth     include        common-auth
auth     required       pam_nologin.so
account  include        common-account
password include        common-password
session  include        common-session
# Abilitare la riga seguente per ottenere supporto resmgr per
# le sessioni ssh (vedere /usr/share/doc/packages/resmgr/README.SuSE)
#session  optional      pam_resmgr.so nometty_fittizio
```

La configurazione PAM tipica per un'applicazione (sshd in questo caso) contiene 4 istruzioni "include" relative ai file di configurazione di 4 tipi di modulo: `common-auth`, `common-account`, `common-password` e `common-session`. Questi 4 file contengono la configurazione di default per ciascun tipo di modulo. Includendoli, invece di invocare ciascun modulo separatamente per ciascuna applicazione PAM, si ottiene automaticamente una configurazione PAM aggiornata in caso di modifiche dei valori di default da parte dell'amministratore. In precedenza, in caso di modifiche del PAM o di installazione di nuove applicazioni, era necessario modificare manualmente tutti i file di configurazione per tutte le applicazioni. L'attuale configurazione PAM è costituita da file di configurazione centrali e tutte le modifiche vengono automaticamente ereditate dalla configurazione PAM di ciascun servizio.

Il file con istruzione "include" (`common-auth`) invoca 2 moduli di tipo `auth`: `pam_env` e `pam_unix2`. Vedere Esempio 36.2, «Configurazione di default per la sezione `auth`» (p. 574).

Esempio 36.2 *Configurazione di default per la sezione auth*

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

Il primo, `pam_env`, carica il file `/etc/security/pam_env.conf` per impostare le variabili d'ambiente come specificato nel file stesso. Questa operazione è utile per impostare la variabile `DISPLAY` sul valore corretto, poiché il modulo `pam_env` indica l'ubicazione da cui avviene il login. Il secondo, `pam_unix2`, verifica il nome di login e parola d'ordine dell'utente a fronte dei file `/etc/passwd` e `/etc/shadow`.

Al termine della corretta invocazione dei moduli specificati in `common-auth`, un terzo modulo denominato `pam_nologin` accerta l'esistenza del file `/etc/nologin`. Se l'esito è positivo, nessun utente eccetto `root` potrà effettuare il login. L'intero stack dei moduli `auth` viene elaborato prima che giunga risposta a sshd riguardo il risultato del login. Dato che tutti i moduli dello stack contengono il flag di controllo `required`,

devono tutti essere elaborati senza errori prima che venga inviato il risultato positivo a sshd. Se uno dei moduli restituisce un errore, l'intero stack del modulo viene comunque elaborato e solo dopo giunge la notifica a sshd riguardo il risultato negativo.

Al termine dell'elaborazione corretta di tutti i moduli di tipo `auth`, viene elaborata un'altra istruzione "include", in questo caso quella in Esempio 36.3, «Configurazione di default per la sezione `account`» (p. 575). Il tipo `common-account` contiene un solo modulo, `pam_unix2`. Se il file `pam_unix2` conferma l'esistenza del risultato, sshd ne viene notificato e inizia l'elaborazione dello stack di moduli successivo (`password`), descritto in Esempio 36.4, «Configurazione di default per la sezione `password`» (p. 575).

Esempio 36.3 *Configurazione di default per la sezione account*

```
account required        pam_unix2.so
```

Esempio 36.4 *Configurazione di default per la sezione password*

```
password required       pam_pwcheck.so  nullok
password required       pam_unix2.so    nullok use_first_pass use_authtok
#password required      pam_make.so     /var/yp
```

Anche in questo caso, la configurazione PAM implica solo un'istruzione "include" relativa alla configurazione di default per i moduli `password` ubicati in `common-password`. Questi moduli devono essere correttamente completati (flag di controllo `required`) ogni volta che l'applicazione richiede la modifica del token di autenticazione. La modifica di una parole d'ordine o di altro token di autenticazione richiede una verifica di sicurezza. Questa operazione viene svolta dal modulo `pam_pwcheck`. Il modulo `pam_unix2` utilizzato successivamente ricava sia la vecchia parola d'ordine che quella nuova dal modulo `pam_pwcheck`, in modo che l'utente non debba essere riautenticato. Questo metodo impedisce i tentativi di evitare le verifiche svolte da `pam_pwcheck`. I moduli di tipo `password` devono essere utilizzati ogni volta che i moduli precedenti di tipo `account` o `auth` sono configurati per verificare una parola d'ordine scaduta.

Esempio 36.5 *Configurazione di default per la sezione session*

```
session required        pam_limits.so
session required        pam_unix2.so
```

Nell'ultima fase, i moduli di tipo `session`, raccolti nel file `common-session`, vengono invocati per configurare la sessione in base alle impostazioni dell'utente in questione. L'ulteriore elaborazione di `pam_unix2` non ha conseguenze pratiche a

causa dell'opzione `none` specificata nel relativo file di configurazione per questo modulo `pam_unix2.conf`. Il modulo `pam_limits` carica il file `/etc/security/limits.conf` contenente i limiti di utilizzo di alcune risorse di sistema. I moduli `session` vengono di nuovi invocati quando l'utente esegue il logout.

36.3 Configurazione dei moduli PAM

Alcuni moduli PAM possono essere configurati. I corresponding file di configuration si trovano in `/etc/security`. La presnte sezione descrive brevemente i file di configuration pertinenti all'esempio di sshd - `pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` e `limits.conf`.

36.3.1 pam_unix2.conf

Il metodo tradizionale di autenticazione in base alla parola d'ordine è controllato dal modulo PAM `pam_unix2`. Il modulo è in grado di leggere i dati necessari dai file `/etc/passwd`, `/etc/shadow`, dalle mappe NIS, dalle tabelle NIS+ e dai database LDAP. Il controllo di questo modulo varia in base alla configurazione delle opzioni PAM della singola applicazione o delle opzioni globali impostate nel file `/etc/security/pam_unix2.conf`. Un file di configurazione di base per il modulo è mostrato in Esempio 36.6, «pam_unix2.conf» (p. 576).

Esempio 36.6 *pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        none
```

L'opzione `nullok` per i moduli di tipo `auth` e `password` specifica che le parole d'ordine sono autorizzate per il tipo di conto. Gli utenti sono anche autorizzati a modificare la parola d'ordine del proprio conto. L'opzione `none` per il modulo di tipo `session` specifica la relativa registrazione di messaggi è disabilitata (valore di default). Per saperne di più sulle opzioni di configurazione, esaminare i commenti nel file stesso e consultare la sezione dedicata a pam_unix2.

36.3.2 pam_env.conf

Questo file è utile per definire un ambiente utente standardizzato che viene proposto ogniqualvolta che il modulo `pam_env` viene invocato. Per impostare le variabili d'ambiente, rispettare la seguente sintassi:

```
VARIABILE  [DEFAULT=[valore]]  [OVERRIDE=[valore]]
```

`VARIABILE`
Nome della variabile d'ambiente da impostare.

`[DEFAULT=[valore]]`
Valore di default impostato dall'amministratore.

`[OVERRIDE=[valore]]`
Valori che possono essere interrogati e impostati da `pam_env` per sovrascrivere il valore di default.

Un esempio tipico sull'utilizzo di `pam_env` consiste nell'adattamento della variabile `DISPLAY` quando viene effettuato un login remoto. L'esempio è mostrato in Esempio 36.7, «pam_env.conf» (p. 577).

Esempio 36.7 *pam_env.conf*

```
REMOTEHOST     DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY        DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

La prima riga imposta il valore della variabile `REMOTEHOST` su `localhost`, che viene utilizzata ogni volta che il modulo `pam_env` non riesce a determinare altri valori. A sua volta, la variabile `DISPLAY` determina il valore di `REMOTEHOST`. Per ulteriori informazioni, esaminare i commenti nel file `/etc/security/pam_env.conf`.

36.3.3 pam_pwcheck.conf

Questo file di configurazione riguarda il modulo `pam_pwcheck`, che ne ricava le opzioni per tutti i moduli di `password`. Le impostazioni di questo file sovrascrivono le impostazioni PAM definite a livello della singola applicazione. Se queste non sono state definite, l'applicazione utilizza le impostazioni globali come definito nel file Esempio 36.8, «pam_pwcheck.conf» (p. 578) `pam_pwcheck`, ossia autorizzare le

parole d'ordine vuote e la modifica delle stesse. Per ulteriori informazioni sulle opzioni del modulo, vedere `/etc/security/pam_pwcheck.conf`.

Esempio 36.8 *pam_pwcheck.conf*

```
password:    nullok
```

36.3.4 limits.conf

I limiti del sistema possono essere impostati a livello di un singolo o più utenti a partire dal file `limits.conf`, che viene letto dal modulo`pam_limits`. Questo file consente di impostare dei limiti rigidi che non possono in nessun caso essere oltrepassati e limiti flessibili che lo possono essere temporaneamente. Per saperne di più sulla sintassi e le opzioni disponibili, leggere i commenti nel file.

36.4 Per ulteriori informazioni

Nella directory `/usr/share/doc/packages/pam` del sistema installato, è disponibile la seguente documentazione:

README
: Alla radice di questa directory, sono disponibili alcuni file README di carattere generale. La sottodirectory `modules` contiene dei file README sui moduli PAM disponibili.

Manuale dell'amministratore del sistema Linux-PAM
: Questo documento include tutte le informazioni necessario per l'amministrazione di PAM. L'ampia gamma degli argomenti trattati va dalla sintassi dei file di configurazione agli aspetti della sicurezza di PAM. Il documento è disponibile nei formati PDF, HTML e testo.

Manuale dell'autore di moduli Linux-PAM
: Questo documento analizza gli aspetti dal punto di vista dello sviluppatore, incluse informazioni su come scrivere moduli PAM conformi allo standard. Il documento è disponibile nei formati PDF, HTML e testo.

Manuale dello sviluppatore di applicazioni Linux-PAM

Questo documento include tutte le informazioni richieste da uno sviluppatore di applicazioni per l'utilizzo delle librerie PAM. Il documento è disponibile nei formati PDF, HTML e testo.

Thorsten Kukuk ha sviluppato una serie di moduli per SUSE Linux corredata da alcune informazioni disponibile all'indirizzo `http://www.suse.de/~kukuk/pam/`.

37 Virtualizzazione con Xen

Xen consente di eseguire più sistemi Linux in un unico computer. L'hardware per i diversi sistemi viene fornito in modo virtuale. In questo capitolo viene fornita una panoramica delle potenzialità e delle limitazioni di questa tecnologia. Le sezioni relative all'installazione, la configurazione e l'esecuzione di Xen completano questa introduzione.

Nei computer virtuali l'hardware necessario per il funzionamento di un sistema deve essere in genere emulato. L'hardware emulato è tuttavia molto più lento di quello reale. In Xen viene adottato un approccio diverso. L'emulazione viene limitata al minimo indispensabile. A questo scopo, viene utilizzata la *paravirtualizzazione*. Si tratta di una tecnica che presenta i computer virtuali all'hardware sottostante in modo simile, ma non identico. I sistemi operativi host e guest vengono quindi adattati a livello di kernel mentre lo spazio utente rimane immutato. In Xen la gestione dell'hardware viene eseguita tramite un ipervisore e un guest di controllo, denominato anche domain-0, che forniscono tutti i dispositivi virtuali di rete e del blocco. I dispositivi virtuali di rete e del blocco vengono utilizzati per l'esecuzione dei sistemi guest e la connessione ad altri guest o alla rete locale. Se più computer che eseguono Xen sono configurati in modo da disporre dei dispositivi virtuali di rete e del blocco, è inoltre possibile eseguire la migrazione di un sistema guest da un componente hardware a un altro in fase di esecuzione. Xen è stato originariamente sviluppato per eseguire fino a 100 sistemi guest in un computer. Il numero effettivo, tuttavia, dipende dai requisiti dei sistemi guest in esecuzione, in particolare dal consumo di memoria.

Per limitare l'utilizzo della CPU, l'ipervisore di Xen dispone di tre diversi scheduler. Lo scheduler può inoltre essere modificato mentre il sistema guest è in esecuzione in modo da cambiare la priorità dei sistemi guest eseguiti. A un livello superiore, la migrazione di un guest consente inoltre di modificare le risorse della CPU disponibili.

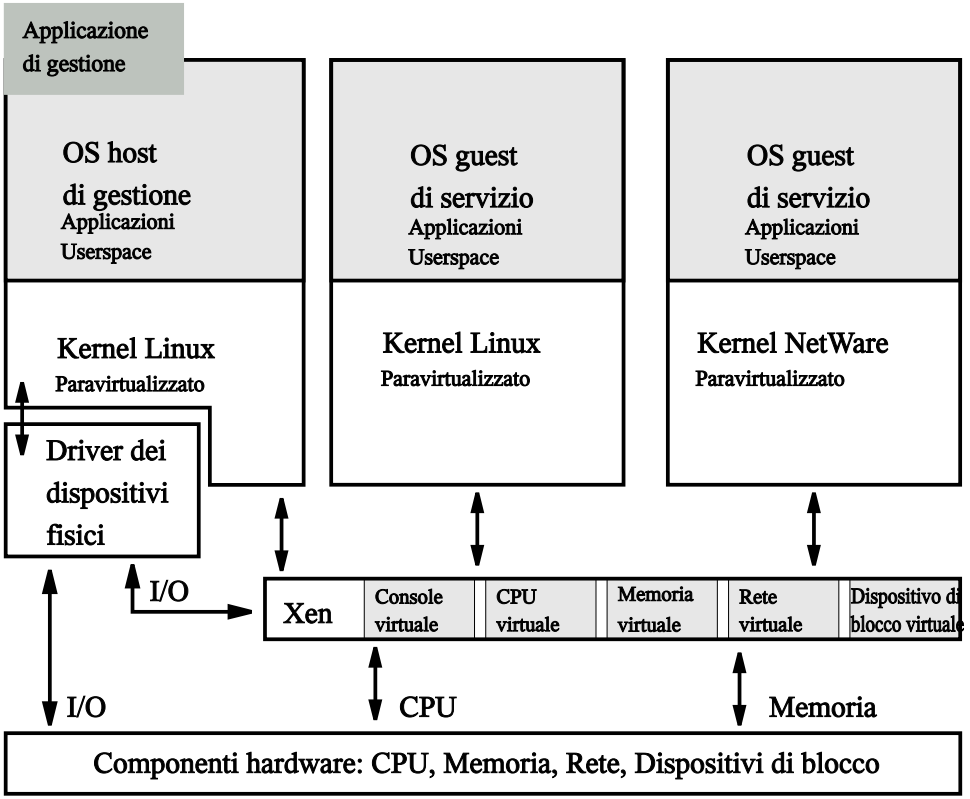
Il sistema di virtualizzazione Xen comporta anche alcuni limiti relativi all'hardware supportato:

- Diversi driver closed source, ad esempio quelli di Nvidia o ATI, non funzionano nel modo previsto. In questi casi, è necessario utilizzare i driver open source, se disponibili, anche se non supportano tutte le funzionalità dei chip. Diversi chip WLAN e bridge CardBus non sono supportati quando si utilizza Xen.

- Nella versione 2 di Xen, PAE (Physical Address Extension, estensione indirizzo fisico) non è supportata, il che implica una limitazione alla quantità di memoria supportata che è pari a 4 GB.

- Non è disponibile il supporto per ACPI (Advanced Configuration and Power Interface). La gestione dell'alimentazione e di altre modalità dipendenti da ACPI non funziona.

Figura 37.1 *Panoramica di Xen*



37.1 Installazione di Xen

La procedura di installazione di Xen prevede la configurazione di un dominio domain-0 e l'installazione dei client Xen. Accertarsi innanzitutto che siano installati i pacchetti necessari, ovvero `python`, `bridge-utils`, `xen` e un pacchetto `kernel-xen`. Se si utilizzano i pacchetti SUSE, Xen viene aggiunto alla configurazione di GRUB. In caso contrario, aggiungere una voce in `boot/grub/menu.lst`. Tale voce deve essere analoga alla seguente:

```
title Xen2
    kernel (hd0,0)/boot/xen.gz dom0_mem=458752
    module (hd0,0)/boot/vmlinuz-xen <parameters>
    module (hd0,0)/boot/initrd-xen
```

Sostituire (hd0,0) con la partizione che contiene la directory `/boot`. Vedere anche il Capitolo 29, *Boot Loader* (p. 463). Modificare la quantità di dom0_mem affinché corrisponda a quella del sistema utilizzato. Il valore massimo corrisponde alla memoria del sistema utilizzato espressa in kB meno 65536. Sostituire <parameters> con i parametri normalmente utilizzati per l'avvio di un kernel Linux. Riavviare quindi il sistema in modalità Xen. In questo modo vengono avviati l'ipervisore di Xen e un kernel Linux leggermente modificato come Domain-0 che esegue la maggior parte dell'hardware. Ad eccezione degli elementi descritti in precedenza, il funzionamento dovrebbe risultare normale.

37.2 Installazione del dominio

L'installazione e la configurazione di un dominio guest prevedono diverse procedure. Di seguito vengono illustrati l'installazione di un primo dominio guest e tutti i passaggi necessari per creare una prima connessione di rete.

Per installare un sistema guest, è necessario specificare un file system radice in un dispositivo del blocco o in un'immagine di file system che è necessario configurare. Per accedere successivamente a questo sistema, utilizzare una console emulata oppure configurare una connessione di rete per il guest. In YaST è supportata l'installazione di SUSE Linux in una directory. I requisiti hardware di tale guest sono analoghi a quelli di una normale installazione di Linux.

I domini possono condividere file system montati in sola lettura da tutti i domini, ad esempio `/usr` o `/opt`. Non condividere un file system montato in lettura/scrittura. Per la condivisione di dati scrivibili tra più domini guest, utilizzare NFS (Network File System, file system di rete) o altri file system connessi in rete o cluster.

AVVERTIMENTO: Avvio di un dominio guest

Quando si avvia un dominio guest, verificare che i rispettivi file system non siano più montati da un programma di installazione o dal domain-0 di controllo.

È innanzitutto necessario creare un'immagine del file system in cui sia installato Linux per il guest:

1. Per creare un'immagine vuota denominata `guest1` nella directory `/var/tmp/` di dimensioni pari a 4 GB, utilizzare il comando seguente:

```
dd if=/dev/zero of=/var/tmp/guest1 seek=1M bs=4096 count=1
```

2 L'immagine è un file vuoto di grandi dimensioni che non contiene alcuna informazione. Per poter scrivere file nell'immagine, è necessario un file system:

```
mkreiserfs -f /var/tmp/guest1
```

Il comando `mkreiserfs` informa che non è presente alcun dispositivo speciale del blocco e ne chiede conferma. Premere Y e quindi Invio per continuare.

3 L'installazione effettiva viene eseguita in una directory. È quindi necessario montare l'immagine del file system `/var/tmp/guest1` in una directory:

```
mkdir -p /var/tmp/dirinstall
mount -o loop /var/tmp/guest1 /var/tmp/dirinstall
```

IMPORTANTE

Al termine dell'installazione, smontare nuovamente l'immagine del file system. YaST consente inoltre di montare il file system `/proc` durante l'installazione, il quale deve essere ugualmente smontato:

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall
```

37.2.1 Utilizzo di YaST per installare un dominio guest

Per installare un dominio guest mediante YaST, è necessaria l'immagine del file system preparata in precedenza per il nuovo guest. Avviare YaST e selezionare *Software → Installazione in directory per XEN*.

Il modulo YaST per l'installazione in directory dispone di diverse opzioni che è necessario configurare in base alle proprie esigenze:

- Directory meta: `/var/tmp/dirinstall`

  Impostare questa opzione sul punto di montaggio dell'immagine del file system da utilizzare. In genere non è necessario modificare il valore di default.

- Esegui YaST e SuSEconfig al primo avvio: Sì

Impostare questa opzione su *Sì*. Al primo avvio del guest verrà richiesta la password radice e un primo utente.

- Crea immagine: No

  L'immagine creata mediante questa opzione è un archivio tar della directory di installazione il quale non risulta di alcuna utilità in questo caso.

- Software

  Selezionare il tipo di installazione da utilizzare. È possibile utilizzare una qualsiasi delle impostazioni di default.

Fare clic su *Avanti* per avviare l'installazione. La durata dell'installazione dipende dal numero dei pacchetti. Al termine dell'installazione è necessario spostare le librerie tls:

```
mv /var/tmp/dirinstall/lib/tls /var/tmp/dirinstall/lib/tls.disabled
```

Xen utilizza uno dei kernel installati in domain-0 per avviare il dominio guest. Per poter utilizzare il networking nel guest, è necessario che i moduli del kernel siano disponibili anche per il guest.

```
cp -a /lib/modules/$(rpm -qf --qf %{VERSION}-%{RELEASE}-xen \
    /boot/vmlinuz-xen) /var/tmp/dirinstall/lib/modules
```

Per evitare errori del file system, è necessario smontarne l'immagine al termine dell'installazione:

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall/
```

È eventualmente possibile creare kernel specializzati per domain-0, nonché per i sistemi guest. La differenza principale consiste nei driver dell'hardware che nel caso dei sistemi guest non sono necessari. Poiché si tratta di driver modulari e non utilizzati nei sistemi guest, in SUSE è disponibile un unico kernel per entrambi i task.

37.2.2 Configurazione di un sistema di salvataggio da utilizzare come dominio guest

Il modo più semplice per ottenere rapidamente un sistema funzionante consiste nel riutilizzare un file system radice esistente, ad esempio il sistema di salvataggio di SUSE Linux. Si tratta fondamentalmente di scambiare l'immagine del kernel e i driver dei dispositivi virtuali di rete e del blocco in tale immagine. Per semplificare l'esecuzione di questo task, è disponibile lo script `mk-xen-rescue-img.sh` in `/usr/share/doc/packages/xen/`.

Lo svantaggio di questo metodo consiste nell'assenza di un database RPM nel sistema risultante, il che complica l'aggiunta di pacchetti mediante RPM. D'altra parte, ne risulta un sistema di dimensioni ridotte ma dotato di tutti gli elementi essenziali per iniziare a utilizzare il networking.

Per eseguire lo script `mk-xen-rescue-img.sh`, sono necessarie almeno la directory con l'immagine di salvataggio e una posizione di destinazione per l'immagine risultante. Per default, la directory si trova nel DVD di avvio nella directory `/boot`.

```
cd /usr/share/doc/packages/xen
./mk-xen-rescue-img.sh /media/dvd/boot /usr/local/xen 64
```

Il primo parametro dello script è la directory dell'immagine di salvataggio. Il secondo parametro corrisponde alla destinazione del file di immagine. I parametri facoltativi rappresentano i requisiti di spazio su disco del nuovo dominio guest e la versione del kernel da utilizzare.

Lo script consente quindi di copiare l'immagine nella nuova posizione, di sostituire il kernel e diversi suoi moduli, nonché di disabilitare la directory `tls` nel sistema. L'ultimo passaggio consiste nella generazione di un file di configurazione per la nuova immagine in `/etc/xen/`.

37.3 Configurazione di un dominio guest di Xen

La documentazione relativa alle procedure di configurazione di un dominio guest non è esaustiva. La maggior parte delle informazioni su come configurare il dominio si trova nel file di configurazione di esempio `/etc/xen/config`. Le opzioni necessarie vengono illustrate con il rispettivo valore di default o almeno un esempio di configurazione. Per l'installazione descritta nella Sezione 37.2.1, «Utilizzo di YaST per installare un dominio guest» (p. 585), creare un file `/etc/xen/guest1` contenente quanto segue:

```
kernel = "/boot/vmlinuz-xen"    ❶
ramdisk = "/boot/initrd-xen"    ❷
memory = 128                    ❸
name = "guest1"                 ❹
nics = "1"                      ❺
vif = [ 'mac=aa:cc:00:00:00:ab, bridge=xen-br0' ] ❻
disk = [ 'file:/var/tmp/guest1,hda1,w' ] ❼
root = "/dev/hda1 ro"           ❽
extra = "3"                     ❾
```

❶ Immettere il percorso del kernel Xen in domain-0. Il kernel verrà successivamente eseguito nel sistema guest.

❷ Selezionare il disco RAM iniziale appropriato contenente i driver dei dispositivi per il kernel Xen. In caso contrario, il kernel non funzionerà correttamente poiché non sarà possibile montare il rispettivo file system radice.

❸ Definire la quantità di memoria da assegnare al dominio guest. Ciò non è possibile se il sistema non dispone di memoria sufficiente per i rispettivi guest.

❹ Il nome del guest.

❺ Il numero di interfacce di rete virtuali per il dominio guest.

❻ La configurazione dell'interfaccia di rete virtuale, inclusi l'indirizzo MAC e il bridge a cui è connessa.

❼ Impostare i dispositivi virtuali del blocco per il guest Xen. Per utilizzare dispositivi reali del blocco, creare voci quali `['phy:sdb1,hda1,w', 'phy:system/swap1,hda2,w']`.

❽ Impostare il dispositivo radice per il kernel. Deve corrispondere al dispositivo virtuale visto dal guest.

❾ Aggiungere qui ulteriori parametri del kernel. `3` significa, ad esempio, che il guest viene avviato al runlevel 3.

37.4 Avvio e controllo dei domini Xen

Per poter avviare il dominio guest, l'ipervisore di Xen deve disporre di memoria libera sufficiente per il nuovo guest. Verificare innanzitutto la quantità di memoria utilizzata:

```
xm list
Name              Id  Mem(MB)  CPU  State  Time(s)  Console
Domain-0           0      458    0  r----    181.8
```

Se il computer dispone di 512 MB, l'ipervisore di Xen ne riserva per sé 64 MB e domain-0 occupa il resto. Per liberare memoria per il nuovo guest, si utilizza il comando `xm balloon`. Per impostare le dimensioni di domain-0 su 330 MB, immettere quanto segue come utente `root`:

```
xm balloon 0 330
```

Nel comando successivo `xm list`, l'uso della memoria da parte di domain-0 dovrebbe risultare pari a 330 MB. È quindi disponibile memoria sufficiente per avviare un guest con 128 MB. Il comando `xm start guest1 -c` consente di avviare il guest e di collegare la rispettiva console al terminale attuale. Se si tratta del primo avvio del guest, completarne l'installazione mediante YaST.

È sempre possibile scollegare la console o collegarla da un altro terminale. Per scollegarla, premere Ctrl +]. Per ricollegarla, controllare innanzitutto l'ID del guest necessario con `xm list` e collegarla a tale ID con `xm console` *`ID`*.

Lo strumento xm di Xen dispone di numerosi parametri. Per visualizzarne un elenco con una breve descrizione, immettere `xm help`. A titolo esemplificativo, nella Tabella 37.1, «Comandi di xm» (p. 590) vengono illustrati alcuni dei comandi più importanti.

Tabella 37.1 *Comandi di xm*

`xm help`	Consente di visualizzare un elenco dei comandi disponibili per lo strumento xm.
`xm console` *`ID`*	Consente di eseguire la connessione alla prima console (tty1) del guest con ID *`ID`*.
`xm balloon` *`ID Mem`*	Consente di impostare le dimensioni della memoria del dominio con ID *`ID`* su *`Mem`* (in MB).
`xm create` *`domname`* `[-c]`	Consente di avviare il dominio con il file di configurazione *`domname`*. Il parametro facoltativo `-c` consente di collegare il terminale attuale alla prima tty del nuovo guest.
`xm shutdown` *`ID`*	Consente di arrestare normalmente il guest con ID *`ID`*.
`xm destroy` *`ID`*	Consente di terminare immediatamente il guest con ID *`ID`*.
`xm list`	Consente di visualizzare un elenco di tutti i domini in esecuzione con i rispettivi valori di ID; memoria e tempo di CPU.
`xm info`	Consente di visualizzare informazioni sull'host Xen, inclusi dati sulla CPU e la memoria.

37.5 Ulteriori informazioni

Per ulteriori informazioni su Xen, visitare i siti Web seguenti:

- `file:/usr/share/doc/packages/xen/user/html/index.html`—Informazioni ufficiali per gli utenti Xen. È necessario il pacchetto `xen-doc-html`.
- `file:/usr/share/doc/packages/xen/interface/html/index.html`—Ulteriore documentazione tecnica sull'interfaccia. È necessario il pacchetto `xen-doc-html`.

- http://www.cl.cam.ac.uk/Research/SRG/netos/xen/index.html—Home page di Xen con numerosi collegamenti a diverse fonti di documentazione.
- http://lists.xensource.com/—Diverse mailing list su Xen.

Parte IX. Servizi

38 Networking di base

In Linux sono disponibili le funzionalità e gli strumenti di networking necessari per l'integrazione in qualsiasi tipo di struttura di rete. Il protocollo TCP/IP utilizzato in Linux dispone di funzionalità speciali e vari servizi illustrati di seguito. È possibile configurare l'accesso alla rete mediante una scheda di rete, un modem o un altro dispositivo utilizzando YaST oppure manualmente. In questo capitolo vengono descritti solo i meccanismi fondamentali e i relativi file di configurazione di rete.

In Linux, come in altri sistemi operativi UNIX, viene utilizzato il protocollo TCP/IP che non è un protocollo di rete unico, ma una famiglia di protocolli di rete in grado di offrire numerosi servizi. I protocolli elencati nella Tabella 38.1, «Numerosi protocolli della famiglia TCP/IP» (p. 596) vengono forniti allo scopo di consentire lo scambio di dati tra due computer tramite TCP/IP. Le reti unite mediante TCP/IP, che costituiscono una rete mondiale, vengono identificate complessivamente come «Internet.»

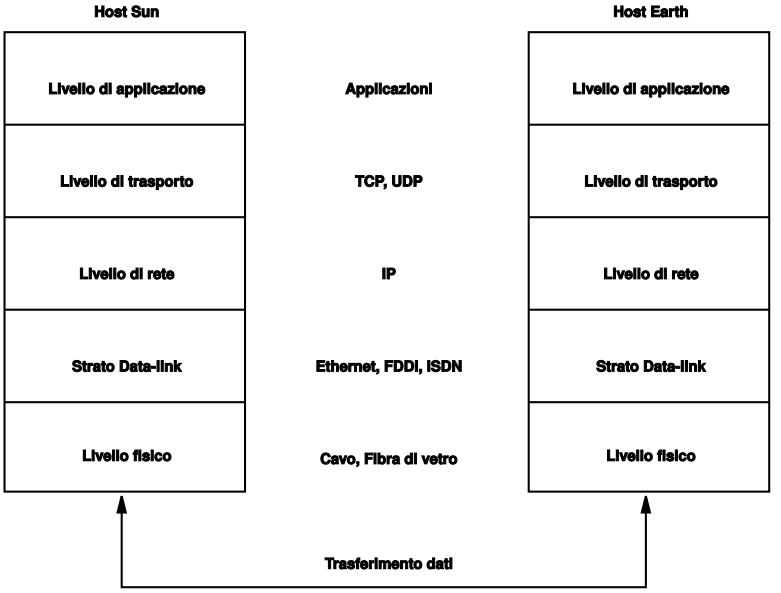
RFC è l'acronimo di *Request for Comments*. In questi documenti sono descritti i diversi protocolli Internet e le procedure di implementazione per il sistema operativo e le relative applicazioni. Nei documenti RFC viene descritta la configurazione dei protocolli Internet. Per ulteriori informazioni su uno qualsiasi di questi protocolli, fare riferimento ai relativi documenti RFC disponibili in linea all'indirizzo `http://www.ietf.org/rfc.html` (in lingua inglese).

Tabella 38.1 *Numerosi protocolli della famiglia TCP/IP*

Protocollo	Descrizione
TCP	Transmission Control Protocol: protocollo sicuro orientato alla connessione. I dati da trasmettere vengono inizialmente inviati dall'applicazione come un flusso di dati, quindi convertiti dal sistema operativo nel formato appropriato. I dati pervengono alla rispettiva applicazione sull'host di destinazione nel formato del flusso di dati originale in cui sono stati inviati inizialmente. Il protocollo TCP determina se si sono verificate perdite o scambi di pacchetti di dati durante la trasmissione, per questo viene implementato ovunque sia importante mantenere la corretta sequenza dei dati.
UDP	User Datagram Protocol: protocollo non sicuro senza connessione. I dati da trasmettere vengono inviati sotto forma di pacchetti generati dall'applicazione. L'ordine in cui i dati pervengono al destinatario non è garantito ed è possibile che si verifichino perdite di dati. Il protocollo UDP è adatto per le applicazioni orientate ai record e presenta un periodo di latenza inferiore rispetto al TCP.
ICMP	Internet Control Message Protocol: essenzialmente non si tratta di un protocollo per l'utente finale, ma di uno speciale protocollo di controllo che genera un rapporto degli errori ed è in grado di controllare il comportamento dei computer che partecipano al trasferimento di dati TCP/IP. Dispone, inoltre, di una speciale modalità echo che è possibile visualizzare utilizzando il programma PING.
IGMP	Internet Group Management Protocol: controlla il comportamento del computer quando viene implementato l'IP multicast.

Come illustrato nella Figura 38.1, «Modello a strati semplificato per TCP/IP» (p. 597), lo scambio dei dati avviene in diversi strati. Nello strato Rete vero e proprio avviene il trasferimento dei dati non sicuro tramite IP (Internet Protocol). Oltre all'IP, il protocollo TCP (Transmission Control Protocol) garantisce, fino a un certo punto, la sicurezza del trasferimento dei dati. Lo strato IP è supportato dal sottostante protocollo dipendente dall'hardware, ad esempio Ethernet.

Figura 38.1 *Modello a strati semplificato per TCP/IP*



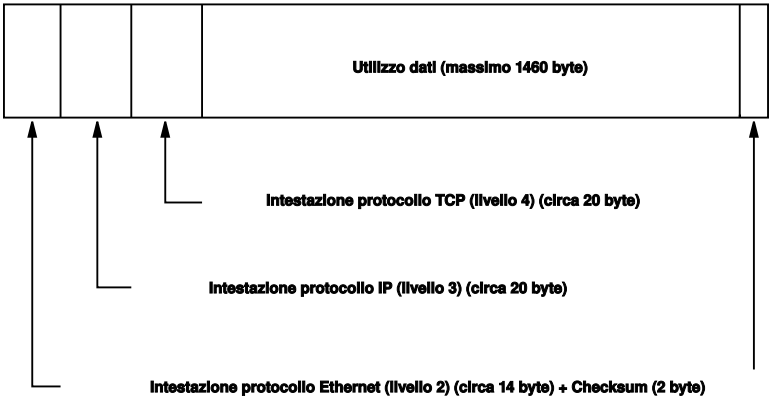
Nel diagramma vengono forniti uno o due esempi per ogni strato. L'ordinamento degli strati avviene in base ai *livelli di astrazione*. Lo strato più basso si trova molto vicino all'hardware, mentre lo strato più alto è quasi un'astrazione completa dall'hardware. Ogni strato ha una speciale funzione e le funzioni speciali di ogni strato sono per lo più implicite nella relativa descrizione. Gli strati Collegamento dati e Fisico rappresentano la rete fisica utilizzata, ad esempio Ethernet.

Quasi tutti i protocolli hardware funzionano in base a un'architettura orientata ai pacchetti. I dati da trasmettere vengono inclusi in *pacchetti*, in quanto non possono essere inviati tutti simultaneamente. La dimensione massima di un pacchetto TCP/IP è di circa 64 KB, tuttavia i pacchetti sono normalmente molto più piccoli poiché l'hardware della rete può rappresentare un fattore limitante. La dimensione massima di un pacchetto di dati su una rete Ethernet è di circa 1500 byte, pertanto la dimensione di un pacchetto TCP/IP inviato su una rete Ethernet è limitata a tale valore. Se la quantità di dati da trasferire è maggiore, dovranno essere inviati più pacchetti da parte del sistema operativo.

Affinché gli strati possano svolgere le funzioni designate, è necessario che nel pacchetto di dati siano salvate informazioni aggiuntive relative a ogni strato. Questo processo avviene nell'*intestazione* del pacchetto. All'inizio di ogni pacchetto generato viene

aggiunto un piccolo blocco di dati per ogni strato, definito intestazione del protocollo. Nella Figura 38.2, «Pacchetto Ethernet TCP/IP» (p. 598) è illustrato un pacchetto di dati TCP/IP di esempio trasmesso su un cavo Ethernet. Il valore proof sum si trova alla fine del pacchetto anziché all'inizio, per semplificare la trasmissione dei pacchetti da parte dell'hardware di rete.

Figura 38.2 *Pacchetto Ethernet TCP/IP*



I dati inviati da un'applicazione in rete passano attraverso ogni strato. Tutti gli strati sono implementati nel kernel Linux ad eccezione dello strato Fisico. Ogni strato è preposto alla preparazione dei dati affinché possano essere passati allo strato successivo. Allo strato più basso è infine affidato il compito di inviare i dati. Alla ricezione dei dati l'intera procedura viene invertita, rimuovendo in successione da ogni strato le intestazioni del protocollo dai dati trasportati. Lo strato Trasporto rende infine disponibili i dati affinché possano essere utilizzati dalle applicazioni alla destinazione. In questo modo, un solo strato comunica con lo strato direttamente precedente o successivo. Per le applicazioni è irrilevante il fatto che i dati vengano trasmessi su una rete FDDI a 100 MBit/s o su una linea modem a 56-kbit/s. In modo analogo, a condizione che il formato dei pacchetti sia corretto, per la linea dati è irrilevante il tipo di dati trasmesso.

38.1 Indirizzi IP e instradamento

In questa sezione vengono descritte solo le reti IPv4. Per informazioni sul protocollo IPv6, la versione successiva a IPv4, fare riferimento alla Sezione 38.2, «IPv6, la generazione futura di Internet» (p. 601).

38.1.1 Indirizzi IP

A ogni computer su Internet è associato un indirizzo a 32 bit univoco. Questi 32 bit (o 4 byte) sono normalmente scritti come illustrato nella seconda riga dell'Esempio 38.1, «Scrittura di indirizzi IP» (p. 599).

Esempio 38.1 *Scrittura di indirizzi IP*

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.     168.       0.      20
```

Nel formato decimale i quattro byte sono scritti in base al sistema numerico decimale, separati da punti. L'indirizzo IP viene assegnato a un host o a un'interfaccia di rete e non può essere utilizzato in alcun'altra parte del mondo. Esistono eccezioni a questa regola, che tuttavia sono ininfluenti nei passaggi che seguono.

I punti negli indirizzi IP indicano il sistema gerarchico. Fino agli anni '90 gli indirizzi IP erano rigidamente suddivisi in categorie di classi, tuttavia questo sistema è stato abbandonato essendosi rivelato troppo inflessibile. Attualmente viene utilizzato l'*instradamento senza classe* (CIDR, Classless Interdomain Routing).

38.1.2 Maschere di rete e instradamento

Le maschere di rete vengono utilizzate per definire l'intervallo di indirizzi di una sottorete. Se due host si trovano nella stessa sottorete, possono connettersi direttamente. In caso contrario devono disporre dell'indirizzo di un gateway che gestisca tutto il traffico tra la sottorete e il resto della rete mondiale. Per verificare se due indirizzi IP si trovano nella stessa sottorete, collegare semplicemente entrambi gli indirizzi con la maschera di rete mediante «AND». Se il risultato è identico, significa che entrambi gli indirizzi IP si trovano nella stessa rete locale. Se sono presenti differenze, l'indirizzo IP remoto e quindi l'interfaccia remota possono essere raggiunti solo attraverso un gateway.

Per comprendere il funzionamento della maschera di rete, vedere l'Esempio 38.2, «Collegamento di indirizzi IP alla maschera di rete» (p. 600). La maschera di rete è composta da 32 bit che identificano la parte dell'indirizzo IP che appartiene alla rete. Tutti i bit uguali a `1` contrassegnano il bit corrispondente nell'indirizzo IP come appartenente alla rete. Tutti i bit uguali a `0` contrassegnano i bit all'interno della sottorete. Ciò significa che a un maggior numero di bit uguali a `1` corrisponde una sottorete più piccola. Poiché la maschera di rete è sempre composta da più bit uguali a `1` in

successione, è inoltre possibile contare semplicemente il numero di bit nella maschera di rete. Nell'Esempio 38.2, «Collegamento di indirizzi IP alla maschera di rete» (p. 600) la prima rete con 24 bit potrebbe inoltre essere scritta nel formato `192.168.0.0/24`.

Esempio 38.2 *Collegamento di indirizzi IP alla maschera di rete*

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

Per fare un altro esempio, tutti i computer connessi con lo stesso cavo Ethernet si trovano di solito nella stessa sottorete e sono accessibili direttamente. Anche se la sottorete è fisicamente divisa mediante commutatori o bridge, questi host possono comunque essere raggiunti direttamente.

Gli indirizzi IP all'esterno della sottorete locale possono essere raggiunti solo se per la rete di destinazione è configurato un gateway. Nel caso più comune viene utilizzato un solo gateway per la gestione di tutto il traffico esterno, tuttavia è possibile configurare più gateway per diverse sottoreti.

Se è stato configurato un gateway, tutti i pacchetti esterni vengono inviati al gateway appropriato, il quale tenta di inoltrarli allo stesso modo, ovvero da host a host, finché raggiungono la destinazione oppure si verifica la scadenza del TTL (Time-To-Live) del pacchetto.

Tabella 38.2 *Indirizzi specifici*

Tipo di indirizzo	Descrizione
Indirizzo di rete di base	Corrisponde alla maschera di rete AND per tutti gli indirizzi della rete, come illustrato nella sezione `Result` dell'Esempio 38.2, «Collegamento di indirizzi IP alla maschera di rete» (p. 600). Questo indirizzo non può essere assegnato a qualsiasi host.

Tipo di indirizzo	Descrizione
Indirizzo di diffusione	Sostanzialmente significa che è possibile «accedere a tutti gli host della sottorete». Per generare questo indirizzo, la maschera di rete viene invertita in formato binario e collegata all'indirizzo di rete di base mediante un operatore logico OR. L'esempio precedente restituisce quindi 192.168.0.255. Questo indirizzo non può essere assegnato a qualsiasi host.
Host locale	L'indirizzo `127.0.0.1` viene assegnato al «dispositivo di loopback» su ogni host. È possibile configurare una connessione al proprio computer utilizzando questo indirizzo.

Poiché gli indirizzi IP devono essere univoci su tutta la rete mondiale, non è possibile selezionare indirizzi casuali. Per configurare una rete privata basata su IP sono disponibili tre domini di indirizzi che non possono tuttavia ricevere connessioni da Internet, in quanto non possono essere trasmessi su Internet. Questi indirizzi sono specificati nel documento RFC 1597 ed elencati nella Tabella 38.3, «Domini di indirizzi IP privati» (p. 601).

Tabella 38.3 *Domini di indirizzi IP privati*

Rete/Maschera di rete	Dominio
`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`

38.2 IPv6, la generazione futura di Internet

A seguito dell'introduzione del WWW (World Wide Web), negli ultimi 15 anni si è verificata una crescita eccezionale della diffusione di Internet ed è aumentato conseguentemente il numero di computer che comunicano tramite TCP/IP. Da quando

Tim Berners-Lee presso il CERN (http://public.web.cern.ch, in lingua inglese) inventò il WWW nel 1990, il numero degli host su Internet è passato da alcune migliaia a circa cento milioni di unità.

Come accennato in precedenza, un indirizzo IPv4 è composto solo da 32 bit, inoltre un discreto numero di indirizzi IP viene sprecato non essendo utilizzabili a causa del modo in cui sono organizzate le reti. Il numero di indirizzi disponibili in una sottorete corrisponde a 2 elevato alla potenza del numero di bit, meno 2. In una sottorete sono disponibili, ad esempio, 2, 6 o 14 indirizzi. Per eseguire la connessione di 128 host a Internet, ad esempio, è necessaria una sottorete con 256 indirizzi IP, di cui solo 254 sono utilizzabili poiché due indirizzi IP sono necessari per la struttura della stessa sottorete, ovvero l'indirizzo di diffusione e l'indirizzo di rete di base.

Con l'attuale protocollo IPv4 viene normalmente utilizzato DHCP o NAT (Network Address Translation) come meccanismo per sopperire alla potenziale carenza di indirizzi. Insieme alla convenzione di mantenere separati gli spazi di indirizzamento pubblico e privato, questi metodi sono sicuramente in grado di attenuare tale carenza. Esiste tuttavia un problema legato alla configurazione che risulta estremamente impegnativa sia in fase d'impostazione che di manutenzione. Per configurare un host in una rete IPv4, è necessario disporre di numerosi elementi dell'indirizzo, ad esempio l'indirizzo IP dello stesso host, la maschera di sottorete, l'indirizzo del gateway e, probabilmente, l'indirizzo del server dei nomi. Tutti questi elementi devono essere noti e non possono essere dedotti da altre fonti.

Con il protocollo IPv6, invece, sia la carenza di indirizzi che la complessità della configurazione dovrebbero essere completamente superate. Nelle sezioni seguenti vengono fornite ulteriori informazioni sui miglioramenti e sui vantaggi introdotti dalla tecnologia IPv6, oltre che sulla transizione dal protocollo precedente a quello nuovo.

38.2.1 Vantaggi

Il miglioramento più importante e tangibile introdotto dal nuovo protocollo è l'enorme espansione dello spazio di indirizzamento disponibile. Un indirizzo IPv6 è composto da valori di 128 bit anziché dei tradizionali 32 bit e ciò consente una disponibilità di milioni di miliardi di indirizzi IP.

Gli indirizzi IPv6 sono tuttavia diversi da quelli della versione precedente del protocollo non solo per quanto riguarda la lunghezza, ma anche per la struttura interna che può includere informazioni più specifiche sui sistemi e sulle reti a cui appartengono. Per

ulteriori informazioni sull'argomento, fare riferimento alla Sezione 38.2.2, «Tipi di indirizzi e struttura» (p. 604).

Di seguito è riportato un elenco di alcuni dei vantaggi offerti dal nuovo protocollo:

Configurazione automatica
Con IPv6 la rete diventa compatibile «Plug and Play» e ciò significa che i nuovi sistemi si integrano nella rete (locale) senza richiedere alcun intervento di configurazione manuale. Il nuovo host utilizza il proprio meccanismo di configurazione automatica per rilevare l'indirizzo dalle informazioni rese disponibili dai router vicini sulla base di un protocollo di *rilevazione del router vicino* (ND). Questo metodo non richiede l'intervento dell'amministratore, né la gestione di un server centrale per l'allocazione degli indirizzi e ciò rappresenta un ulteriore vantaggio rispetto al protocollo IPv4 per il quale l'allocazione automatica degli indirizzi richiede un server DHCP.

Mobilità
Con IPv6 è possibile assegnare contemporaneamente più indirizzi alla stessa interfaccia di rete. In questo modo gli utenti possono accedere facilmente a diverse reti, in modo analogo ai servizi di roaming internazionali offerti dalle società di telefonia cellulare. Quando si utilizza un cellulare in un altro paese, viene stabilita automaticamente la connessione a un servizio locale non appena si entra nella relativa area di copertura, consentendo quindi di ricevere ovunque chiamate allo stesso numero e di effettuare chiamate come nel proprio paese.

Comunicazione sicura
Con IPv4 la sicurezza della rete viene implementata mediante una funzione aggiuntiva, mentre tra le funzionalità di base offerte da IPv6 è disponibile IPSec che consente la comunicazione tra i sistemi attraverso un tunnel sicuro ed evita l'intercettazione dei dati su Internet.

Compatibilità con versioni precedenti
È realisticamente impossibile che sull'intera rete Internet venga effettuata una transizione in massa da IPv4 a IPv6, pertanto è fondamentale che entrambi i protocolli siano in grado di coesistere non solo su Internet, ma anche in uno stesso sistema. Questo aspetto è assicurato da indirizzi compatibili, infatti gli indirizzi IPv4 possono essere facilmente convertiti in indirizzi IPv6, e dall'uso di numerosi tunnel. Vedere la Sezione 38.2.3, «Coesistenza di IPv4 e IPv6» (p. 609). Per supportare entrambi i protocolli contemporaneamente, nei sistemi è inoltre possibile utilizzare una tecnica *IP a doppio stack*, ovvero due stack di rete mantenuti

completamente separati per evitare qualsiasi interferenza tra le due versioni del protocollo.

Servizi personalizzati mediante il multicast
Con IPv4 è necessario che alcuni servizi, ad esempio SMB, diffondano i pacchetti a tutti gli host della rete locale. IPv6 consente invece un approccio molto più granulare in quanto i server possono indirizzare i pacchetti agli host mediante il *multicast*, ovvero a più host nell'ambito di un gruppo. Questa tecnica è diversa rispetto all'indirizzamento a tutti gli host mediante la *diffusione* o a ogni singolo host mediante il *multicast*. A quali host vengano indirizzati i pacchetti nell'ambito di un gruppo dipende dall'applicazione in uso. Sono disponibili alcuni gruppi di indirizzamento predefiniti, ad esempio il *gruppo di multicast a tutti i server dei nomi* o il *gruppo di multicast a tutti i router*.

38.2.2 Tipi di indirizzi e struttura

Come accennato in precedenza, nell'attuale protocollo IP esistono due importanti aspetti negativi. La carenza di indirizzi IP aumenta costantemente, mentre la configurazione della rete e la gestione delle tabelle degli instradamenti stanno diventando task sempre più complessi e gravosi. IPv6 consente di risolvere il primo problema mediante l'espansione dello spazio di indirizzamento a 128 bit e di contrastare il secondo con l'introduzione di una struttura di indirizzamento gerarchica unita a tecniche sofisticate di allocazione degli indirizzi di rete nonché *MultiHome*, ovvero la capacità di assegnare più indirizzi a un unico dispositivo per l'accesso a più reti.

In relazione a IPv6 è inoltre utile conoscere i tre diversi tipi di indirizzi supportati:

Unicast
Gli indirizzi di questo tipo vengono associati a un'unica interfaccia di rete. I pacchetti con tale indirizzo vengono consegnati a una sola destinazione. Gli indirizzi unicast vengono di conseguenza utilizzati per il trasferimento di pacchetti a singoli host sulla rete locale o su Internet.

Multicast
Gli indirizzi di questo tipo sono correlati a un gruppo di interfacce di rete. I pacchetti con tale indirizzo vengono consegnati a tutte le destinazioni appartenenti al gruppo. Gli indirizzi multicast vengono utilizzati soprattutto da alcuni servizi di rete per comunicare con determinati gruppi di host in una maniera ben precisa.

Anycast

Gli indirizzi di questo tipo sono correlati a un gruppo di interfacce. I pacchetti con tale indirizzo vengono consegnati al membro del gruppo che si trova più vicino al mittente, in base ai principi del protocollo di instradamento sottostante. Gli indirizzi anycast vengono utilizzati per consentire agli host di individuare più facilmente i server che offrono determinati servizi in una data area della rete. Tutti i server dello stesso tipo dispongono dello stesso indirizzo anycast. Ogni volta che un host richiede un servizio, riceve una risposta dal server più vicino, secondo quanto determinato dal protocollo di instradamento. In caso di un errore qualsiasi di questo server, viene selezionato automaticamente il secondo server più vicino, quindi il terzo e così via.

Un indirizzo IPv6 è composto da otto campi di quattro cifre, ognuno dei quali rappresenta 16 bit, espressi in notazione esadecimale. I campi sono inoltre separati da due punti (`:`). Eventuali byte zero iniziali in un determinato campo possono essere scartati, mentre gli zeri all'interno o alla fine del campo devono essere mantenuti. Secondo un'ulteriore convenzione, più di quattro byte zero consecutivi possono essere rappresentati da un doppio carattere due punti. È tuttavia consentito utilizzare un solo `::` per indirizzo. Questo tipo di notazione stenografica è illustrato nell'Esempio 38.3, «Indirizzo IPv6 di esempio» (p. 605), dove le tre righe rappresentano lo stesso indirizzo.

Esempio 38.3 *Indirizzo IPv6 di esempio*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                           : 10 : 1000 : 1a4
```

A ogni parte di un indirizzo IPv6 è associata una funzione specifica. I primi byte formano il prefisso e specificano il tipo di indirizzo. La parte centrale rappresenta la porzione relativa alla rete, ma potrebbe essere inutilizzata. La parte finale dell'indirizzo è relativa all'host. Con IPv6 la maschera di rete viene definita mediante l'indicazione della lunghezza del prefisso dopo una barra alla fine dell'indirizzo. Nell'indirizzo, come illustrato nell'Esempio 38.4, «Indirizzo IPv6 che specifica la lunghezza del prefisso» (p. 605), è inclusa l'informazione che i primi 64 bit formano la parte relativa alla rete e gli ultimi 64 bit la parte relativa all'host. In altre parole, `64` indica che la maschera di rete viene completata con 64 valori di 1 bit a partire da sinistra. Come avviene per la versione IPv4, l'indirizzo IP viene combinato mediante AND con i valori della maschera di rete per determinare se l'host si trova nella stessa sottorete o in un'altra rete.

Esempio 38.4 *Indirizzo IPv6 che specifica la lunghezza del prefisso*

```
fe80::10:1000:1a4/64
```

IPv6 riconosce numerosi tipi predefiniti di prefissi, alcuni dei quali sono illustrati nella Tabella 38.4, «Vari prefissi IPv6» (p. 606).

Tabella 38.4 *Vari prefissi IPv6*

Prefisso (esadecimale)	Definizione
`00`	Indirizzi IPv4 e indirizzi di compatibilità IPv4 su IPv6. Vengono utilizzati per mantenere la compatibilità con IPv4 e richiedono comunque un router in grado di convertire i pacchetti IPv6 in pacchetti IPv4. Anche molti altri indirizzi speciali, ad esempio quello per il dispositivo di loopback, hanno questo prefisso.
`2` o `3` come prima cifra	Indirizzi unicast globali aggregabili. Come avviene per IPv4, è possibile assegnare un'interfaccia per formare una parte di una determinata sottorete. Attualmente sono disponibili gli spazi di indirizzamento seguenti: `2001::/16` (spazio di indirizzamento di qualità produzione) e `2002::/16` (spazio di indirizzamento 6to4).
`fe80::/10`	Indirizzi di collegamento locali. Non essendo necessario instradare gli indirizzi con questo prefisso, dovranno essere raggiungibili solo dall'interno della stessa sottorete.
`fec0::/10`	Indirizzi del sito locali. Possono essere instradati, ma solo all'interno della rete dell'organizzazione alla quale appartengono. Sono in effetti l'equivalente di IPv6 dell'attuale spazio di indirizzamento di rete privata, ad esempio `10.x.x.x`.
`ff`	È il prefisso per gli indirizzi multicast.

Un indirizzo unicast consiste di tre componenti di base:

Topologia pubblica
: La prima parte, che contiene inoltre uno dei prefissi sopra indicati, viene utilizzata per l'instradamento dei pacchetti su Internet e include informazioni sulla società o sull'istituzione che fornisce l'accesso a Internet.

Topologia del sito
La seconda parte contiene informazioni di instradamento relative alla sottorete alla quale deve essere consegnato il pacchetto.

ID interfaccia
La terza parte identifica l'interfaccia alla quale deve essere consegnato il pacchetto. Fornisce inoltre l'indirizzo MAC (Media Access Control) per formare parte dell'indirizzo. Poiché MAC è un identificatore univoco globale fisso codificato all'interno del dispositivo da parte del produttore dell'hardware, la procedura di installazione viene sostanzialmente semplificata. I primi 64 bit dell'indirizzo vengono infatti consolidati per formare il token `EUI-64`. Gli ultimi 48 bit corrispondono all'indirizzo MAC e i rimanenti 24 bit contengono informazioni speciali sul tipo di token. In questo modo è possibile assegnare un token `EUI-64` anche alle interfacce che non dispongono di un MAC, come quelle basate su PPP o ISDN.

Oltre a questa struttura di base, IPv6 è in grado di riconoscere cinque diversi tipi di indirizzi unicast:

`::` (non specificato)
Questo indirizzo viene utilizzato dall'host come indirizzo di origine alla prima inizializzazione dell'interfaccia, ovvero quando l'indirizzo non può ancora essere determinato con altri mezzi.

`::1` (loopback)
Indirizzo del dispositivo di loopback.

Indirizzi compatibili IPv4
L'indirizzo IPv6 è formato dall'indirizzo IPv4 e da un prefisso composto da 96 bit zero. Questo tipo di indirizzo di compatibilità viene utilizzato per il tunneling (vedere la Sezione 38.2.3, «Coesistenza di IPv4 e IPv6» (p. 609)), in modo da consentire agli host IPv4 e IPv6 di comunicare con altri sistemi operativi in un ambiente solo IPv4.

Indirizzi IPv4 mappati a IPv6
Questo tipo di indirizzo specifica un puro indirizzo IPv4 in notazione IPv6.

Indirizzi locali
Sono disponibili due tipi di indirizzi per l'uso locale:

collegamento locale
: Questo tipo di indirizzo può essere utilizzato solo nella sottorete locale. I pacchetti con un indirizzo di origine o di destinazione di questo tipo non dovranno essere instradati a Internet o ad altre sottoreti. Questi indirizzi contengono un prefisso speciale (`fe80::/10`) e l'ID interfaccia della scheda di rete, con la parte centrale formata da byte zero. Gli indirizzi di questo tipo vengono utilizzati durante la configurazione automatica per comunicare con altri host appartenenti alla stessa sottorete.

sito locale
: I pacchetti con questo tipo di indirizzo possono essere instradati ad altre sottoreti, ma non a Internet, e devono rimanere all'interno della rete dell'organizzazione. Tali indirizzi vengono utilizzati per le intranet e rappresentano un equivalente dello spazio di indirizzamento privato definito da IPv4. Contengono un prefisso speciale (`fec0::/10`), l'ID interfaccia e un campo a 16 bit che specifica l'ID della sottorete. Anche in questo caso, il resto dell'indirizzo viene completato con byte zero.

In base a una funzionalità completamente nuova introdotta con IPv6, a ogni interfaccia di rete vengono normalmente assegnati più indirizzi IP con il vantaggio di poter accedere a più reti attraverso la stessa interfaccia. Una di queste reti può essere configurata in modo completamente automatico utilizzando l'indirizzo MAC e un prefisso conosciuto, in modo da consentire l'accesso a tutti gli host della rete locale dopo aver abilitato IPv6, utilizzando l'indirizzo di collegamento locale. L'uso di MAC consente di rendere univoco sulla rete mondiale qualsiasi indirizzo IP. Le sole parti variabili dell'indirizzo sono quelle che specificano la *topologia del sito* e la *topologia pubblica*, a seconda della rete effettiva in cui l'host è attualmente funzionante.

Per consentire all'host di passare da una rete all'altra, sono necessari almeno due indirizzi. Uno di essi, l'*indirizzo home*, contiene l'ID interfaccia, oltre a un identificatore della rete interna alla quale appartiene normalmente, nonché il prefisso corrispondente. L'indirizzo home è un indirizzo statico e, come tale, di solito non viene modificato. Ciononostante tutti i pacchetti destinati all'host mobile possono continuare a essere consegnati, indipendentemente dal punto della rete, interna o esterna, in cui viene utilizzato. Ciò è reso possibile dalle funzionalità completamente nuove introdotte con IPv6, quali la *configurazione automatica stateless* e la *rilevazione del router vicino*. Oltre all'indirizzo home, un host mobile ottiene uno o più indirizzi aggiuntivi che appartengono alle reti esterne in cui viene utilizzato, e che sono definiti indirizzi *C/O*. Nella rete interna è disponibile una funzionalità per l'inoltro dei pacchetti destinati all'host quando questo viene spostato su reti esterne. In un ambiente IPv6 questo task

viene eseguito dall'*agente home*, che riceve tutti i pacchetti destinati all'indirizzo home e li inoltra attraverso un tunnel. I pacchetti destinati all'indirizzo C/O, invece, vengono trasferiti direttamente all'host mobile senza alcuna particolare deviazione.

38.2.3 Coesistenza di IPv4 e IPv6

Il processo di migrazione di tutti gli host connessi a Internet da IPv4 a IPv6 avverrà gradualmente e per un certo periodo i due protocolli dovranno coesistere. La coesistenza su uno stesso sistema è garantita, a condizione che sia implementato un *doppio stack* di entrambi i protocolli. Rimane tuttavia da chiarire come avverrà la comunicazione tra un host che supporta IPv6 e un host IPv4 e come verrà effettuato il trasporto dei pacchetti IPv6 sulle reti attuali, che sono prevalentemente basate su IPv4. Le soluzioni migliori prevedono il tunneling e indirizzi di compatibilità (vedere la Sezione 38.2.2, «Tipi di indirizzi e struttura» (p. 604)).

Gli host IPv6 più o meno isolati sulla rete IPv4 mondiale possono comunicare mediante tunnel. I pacchetti IPv6 vengono incapsulati come pacchetti IPv4 per poter essere spostati su una rete IPv4. Questa connessione tra due host IPv4 è detta *tunnel*. Per ottenere questo risultato, nei pacchetti deve essere incluso l'indirizzo di destinazione IPv6, o il prefisso corrispondente, oltre all'indirizzo IPv4 dell'host remoto all'estremità ricevente del tunnel. Previo accordo tra gli amministratori degli host, è possibile configurare manualmente un tunnel di base che viene definito anche *tunneling statico*.

L'uso della configurazione e della manutenzione di tunnel statici, tuttavia, è troppo impegnativo per le esigenze di comunicazione quotidiane. In IPv6 sono quindi disponibili tre diversi metodi di *tunneling dinamico*:

6over4
: I pacchetti IPv6 vengono incapsulati automaticamente come pacchetti IPv4 e inviati su una rete IPv4 che supporta il multicast. L'intera rete (Internet) viene vista da IPv6 come un'enorme rete locale (LAN) e ciò rende possibile la determinazione automatica dell'estremità ricevente del tunnel IPv4. La scalabilità di questo metodo non è tuttavia ottimale ed è inoltre ostacolata dal fatto che il multicast IP è tutt'altro che esteso su Internet. Rappresenta pertanto una soluzione solo per le società più piccole o per le reti istituzionali in cui è possibile abilitare il multicast. Le specifiche per questo metodo sono descritte nel documento RFC 2529.

6to4
Con questo metodo vengono generati automaticamente indirizzi IPv4 da indirizzi IPv6 in modo da consentire agli host IPv6 isolati di comunicare su una rete IPv4. Sono stati tuttavia segnalati numerosi problemi riguardanti la comunicazione tra questi host IPv6 isolati e Internet. Il metodo è descritto nel documento RFC 3056.

IPv6 Tunnel Broker
Questo metodo si basa su speciali server che forniscono tunnel dedicati per host IPv6 ed è descritto nel documento RFC 3053.

IMPORTANTE: iniziativa 6bone

Nel cuore della «tradizionale» Internet esiste già una rete distribuita globalmente di sottoreti IPv6 connesse mediante tunnel. Si tratta della rete *6bone* (`http://www.6bone.net`, in lingua inglese), un ambiente di test IPv6 che può essere utilizzato dai programmatori e dai provider Internet che desiderano sviluppare e offrire servizi basati su IPv6, in modo che possano maturare l'esperienza necessaria per l'implementazione del nuovo protocollo. Ulteriori informazioni sono disponibili sul sito Internet del progetto.

38.2.4 Configurazione di IPv6

Per configurare IPv6 non è normalmente necessario apportare modifiche alle singole workstation, nelle quali deve tuttavia essere caricato il supporto IPv6. Per eseguire questa operazione, immettere `modprobe ipv6` come `root`.

In base al concetto di configurazione automatica di IPv6, alla scheda di rete viene assegnato un indirizzo nella rete di *collegamento locale*. Di solito non vengono eseguite operazioni di gestione della tabella degli instradamenti sulle workstation. Le workstation possono inviare query ai router di rete mediante il *protocollo di dichiarazione dei router* per sapere quale prefisso e quali gateway dovranno essere implementati. Per la configurazione di un router IPv6 è possibile utilizzare il programma radvd che comunica alle workstation quale prefisso per gli indirizzi IPv6 e quali router utilizzare. In alternativa, per la configurazione automatica di indirizzi e instradamento utilizzare zebra.

Per informazioni sulla configurazione di vari tipi di tunnel mediante i file `/etc/sysconfig/network`, consultare la documentazione ifup(8).

38.2.5 Ulteriori informazioni

La panoramica precedente sull'argomento IPv6 non è esaustiva, quindi per informazioni più dettagliate sul nuovo protocollo si consiglia di fare riferimento alla documentazione in linea e ai manuali seguenti:

http://www.ngnet.it/e/cosa-ipv6.php
Una serie di articoli con una chiara introduzione alle nozioni di base di IPv6 che costituiscono un buon manuale sull'argomento (in lingua inglese).

http://www.bieringer.de/linux/IPv6/
La documentazione HOWTO di Linux su IPv6 e molti collegamenti correlati all'argomento (in lingua inglese).

http://www.6bone.net/
Da questo sito è possibile accedere a una rete IPv6 con tunnel (in lingua inglese).

http://www.ipv6.org/
Il punto di partenza per qualsiasi iniziativa riguardante IPv6 (in lingua inglese).

RFC 2640
I documenti RFC fondamentali su IPv6.

IPv6 Essentials
IPv6 Essentials di Silvia Hagen (ISBN 0-596-00125-8) è un manuale che descrive tutti gli aspetti più importanti di questo argomento.

38.3 Risoluzione del nome

DNS consente di assegnare un indirizzo IP a uno o più nomi e assegnare un nome a un indirizzo IP. In Linux questa conversione viene di solito eseguita da uno speciale tipo di software detto BIND e il computer che esegue questa conversione è definito *server dei nomi*. I nomi creano un sistema gerarchico in cui ogni componente di un nome è separato per mezzo di punti. La gerarchia dei nomi è tuttavia indipendente dalla gerarchia degli indirizzi IP descritta precedentemente.

Si consideri un nome completo, ad esempio `earth.example.com`, scritto nel formato `nome host.dominio`. Un nome completo, a cui viene fatto riferimento come *nome*

di dominio completo (FQDN), è formato da un nome host e da un nome di dominio (`example.com`). Quest'ultimo include il *dominio di livello superiore* o TLD (`com`).

L'assegnazione del TLD è diventata piuttosto confusa per motivi storici. Negli Stati Uniti vengono tradizionalmente utilizzati nomi di dominio di tre lettere, mentre nel resto del mondo vengono utilizzati i codici nazionali standard ISO di due lettere. Nel 2000 sono stati inoltre introdotti TLD più lunghi per rappresentare specifiche sfere di attività, ad esempio `.info`, `.name`, `.museum`).

Nei primi anni della diffusione di Internet, prima del 1990, per la memorizzazione dei nomi di tutti i computer rappresentati su Internet veniva utilizzato il file `/etc/hosts`. Questo approccio si rivelò ben presto di scarsa praticità a causa del numero in rapida crescita di computer connessi a Internet. Per questo motivo è stato sviluppato un database centralizzato in cui memorizzare i nomi host in modo ampiamente distribuito. In questo database, simile a un server dei nomi, non sono immediatamente disponibili i dati relativi a tutti gli host su Internet, tuttavia il database è in grado di inviare richieste ad altri server dei nomi.

Il livello più alto della gerarchi è occupato da *server dei nomi radice* che vengono utilizzati per la gestione dei domini di livello superiore e sono gestiti dal Network Information Center (NIC). Ogni server dei nomi radice dispone di informazioni sui server dei nomi responsabili di un determinato dominio di livello superiore. Le informazioni sui NIC dei domini di livello superiore sono disponibili all'indirizzo `http://www.internic.net`.

DNS è in grado di eseguire altre operazioni oltre alla risoluzione dei nomi host. Il server dei nomi può inoltre riconoscere quale host riceve i messaggi e-mail per un intero dominio, ovvero il *Mail Exchanger (MX)*.

Affinché un computer possa risolvere un indirizzo IP, deve disporre almeno delle informazioni relative a un server dei nomi e al proprio indirizzo IP. È possibile specificare facilmente un server dei nomi utilizzando YaST. Se è disponibile una connessione telefonica via modem, la configurazione manuale di un server dei nomi può non essere necessaria, in quanto il protocollo di connessione telefonica fornisce l'indirizzo del server dei nomi non appena viene stabilita la connessione. La configurazione dell'accesso al server dei nomi con SUSE Linux è descritta nel Capitolo 40, *DNS: Domain Name System* (p. 643).

Il protocollo `whois` è strettamente correlato a DNS. Con questo programma è possibile individuare velocemente il server responsabile di un determinato dominio.

38.4 Configurazione di una connessione di rete con YaST

In Linux sono supportati molti tipi di reti. La maggior parte utilizza nomi di dispositivi diversi e i file di configurazione sono distribuiti in varie posizioni nel file system. Per una panoramica dettagliata degli aspetti della configurazione manuale di rete, vedere la Sezione 38.5, «Configurazione manuale di una connessione di rete» (p. 624).

Durante l'installazione è possibile utilizzare YaST per configurare automaticamente tutte le interfacce rilevate, mentre eventuali componenti hardware aggiuntivi possono essere configurati successivamente in qualsiasi momento nel sistema installato. Nelle sezioni seguenti viene descritta la configurazione della rete per tutti i tipi supportati da SUSE Linux.

38.4.1 Configurazione della scheda di rete con YaST

Dopo aver avviato il modulo, in YaST viene visualizzata una finestra di dialogo per la configurazione generale della rete. Nella parte superiore sono elencate tutte le schede di rete ancora da configurare. Ogni scheda rilevata correttamente è elencata con il relativo nome. I dispositivi che non è stato possibile rilevare possono essere configurati mediante *Altro (non rilevato)* secondo quanto descritto nella sezione chiamata «Configurazione manuale di una scheda di rete non rilevata» (p. 613). Nella parte inferiore della finestra di dialogo è presente l'elenco dei dispositivi configurati finora, con il relativo indirizzo e tipo di rete. È possibile configurare una nuova scheda di rete oppure modificare una configurazione esistente.

Configurazione manuale di una scheda di rete non rilevata

La configurazione di una scheda di rete che non è stata rilevata, e che quindi è elencata come *Altro*, include gli elementi seguenti:

Configurazione della rete

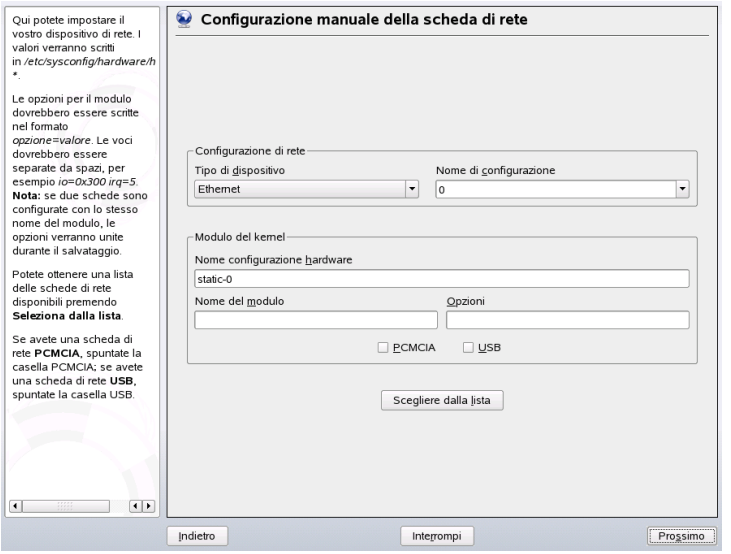
Impostare il tipo di dispositivo dell'interfaccia utilizzando le opzioni disponibili e specificare il nome di configurazione. Nella documentazione di `getcfg(8)` sono disponibili informazioni relative alle convenzioni di denominazione.

Modulo del kernel

Nome configurazione hardware consente di specificare il nome del file `/etc/sysconfig/hardware/hwcfg-*` contenente le impostazioni hardware della scheda di rete in uso. Include il nome del modulo del kernel appropriato, oltre alle opzioni necessarie per l'inizializzazione dell'hardware. In genere vengono proposti nomi utili per l'hardware PCMCIA e USB, mentre per altri tipi di hardware l'uso di `hwcfg-static-0` è solitamente adeguato solo se il nome di configurazione della scheda è impostato su `0`.

Se la scheda di rete è un dispositivo PCMCIA o USB, selezionare le rispettive caselle di controllo e scegliere *Avanti* per uscire dalla finestra di dialogo. In caso contrario, selezionare il modello di scheda di rete in uso scegliendo *Seleziona dalla lista*. Il modulo del kernel appropriato per la scheda specificata viene quindi selezionato automaticamente. Scegliere *Avanti* per uscire dalla finestra di dialogo.

Figura 38.3 *Configurazione della scheda di rete*



Impostazione dell'indirizzo di rete

Impostare il tipo di dispositivo dell'interfaccia e il nome di configurazione. Selezionare il tipo di dispositivo dall'elenco fornito. Specificare un nome di configurazione in base alle esigenze. Le impostazioni di default sono solitamente utili e possono essere accettate. Nella documentazione di `getcfg(8)` sono disponibili informazioni relative alle convenzioni di denominazione.

Se come tipo di dispositivo dell'interfaccia è stata selezionata l'opzione *Wireless*, nella finestra di dialogo successiva, *Configurazione delle schede di rete wireless*, configurare la modalità operativa, il nome di rete (ESSID) e il tipo di cifratura. Per completare la configurazione della scheda di rete, fare clic su *OK*. Nella Sezione 22.1.3, «Configurazione con YaST» (p. 314) è disponibile una descrizione dettagliata relativa alla configurazione di schede WLAN. Per tutti gli altri tipi di interfaccia, procedere con la configurazione dell'indirizzo di rete:

Impostazione automatica indirizzi (via DHCP)
: Se nella rete è presente un server DHCP, è possibile utilizzarlo per la configurazione automatica dell'indirizzo di rete. Questa opzione dovrà essere utilizzata anche per una linea DSL senza un indirizzo IP statico assegnato dall'ISP. Se si sceglie di utilizzare DHCP, selezionare *Opzioni di client DHCP*, quindi configurare i dettagli. Specificare se il server DHCP dovrà sempre soddisfare le richieste di diffusione e l'eventuale identificatore da utilizzare. Per default, i server DHCP utilizzano l'indirizzo hardware della scheda per identificare un'interfaccia. In una configurazione host virtuale nella quale più host comunicano attraverso la stessa interfaccia, è necessario utilizzare un identificatore per distinguere i vari host.

Impostazione statica dell'indirizzo
: Attivare questa opzione se si utilizza un indirizzo statico, quindi immettere l'indirizzo e la maschera di sottorete per la rete in uso. La maschera di sottorete preimpostata dovrà soddisfare i requisiti di una tipica rete domestica.

Scegliere *Avanti* per uscire da questa finestra di dialogo o procedere nella configurazione del nome host, del server dei nomi e dei dettagli di instradamento (vedere le sezioni relative a Server DNS (↑Avvio) e Instradamento (↑Avvio)).

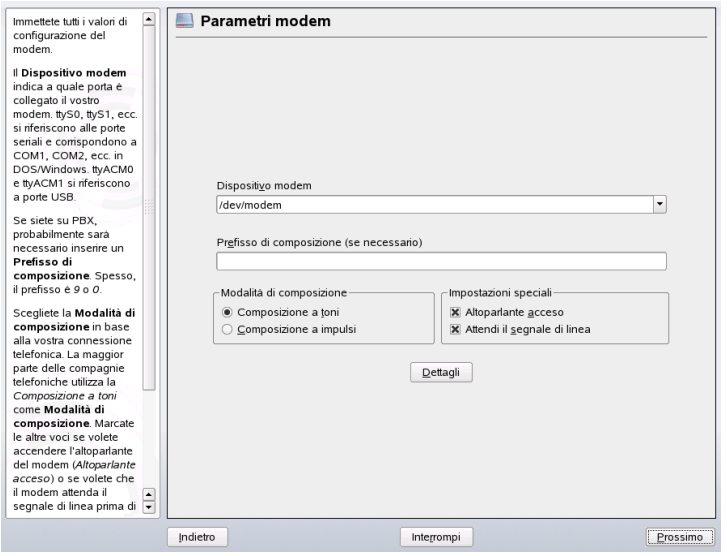
Tramite *Avanzate* è possibile specificare impostazioni più complesse. In *Impostazioni dettagliate* utilizzare *Amministrata dall'utente* per delegare il controllo della scheda di rete dall'amministratore (`root`) all'utente normale. Per un computer portatile questa configurazione consente una maggiore flessibilità di adattamento delle connessioni di

rete, che vengono modificate frequentemente, poiché è possibile controllare l'attivazione o la disattivazione dell'interfaccia. In questa finestra di dialogo è inoltre possibile impostare la MTU (Maximum Transmission Unit) e il tipo di *Attivazione dispositivo*.

38.4.2 Modem

Dal centro controllo YaST accedere alla configurazione del modem in *Dispositivi di rete*. Se il modem in uso non è stato rilevato automaticamente, aprire la finestra di dialogo per la configurazione manuale. Nella finestra di dialogo visualizzata immettere l'interfaccia alla quale è connesso il modem in *Modem*.

Figura 38.4 *Configurazione del modem*



Se la connessione viene stabilita attraverso un centralino (PBX), potrebbe essere necessario immettere un prefisso di composizione che spesso corrisponde ala cifra zero. A questo scopo, consultare le istruzioni fornite con il PBX. Selezionare inoltre se verrà utilizzata la chiamata a toni o a impulsi, se l'altoparlante dovrà essere attivato e se il modem dovrà attendere il rilevamento del segnale di linea. Se il modem è connesso a un centralino, evitare di attivare l'ultima opzione.

In *Dettagli* impostare la velocità di trasmissione e le stringhe di inizializzazione del modem. Modificare queste impostazioni solo se il modem non è stato rilevato

automaticamente o se richiede impostazioni speciali per il funzionamento della trasmissione dati, come avviene soprattutto per le schede di terminale ISDN. Fare clic su *OK* per uscire da questa finestra di dialogo. Per delegare il controllo del modem all'utente normale senza autorizzazioni root, selezionare *Amministrata dall'utente*. In questo modo un utente privo di autorizzazioni di amministratore può attivare o disattivare un'interfaccia. In *Espressione regolare del prefisso di selezione* specificare un'espressione regolare alla quale dovrà corrispondere il *Prefisso di composizione* in KInternet, che può essere modificato dall'utente normale. Se questo campo viene lasciato vuoto, l'utente non potrà impostare un *Prefisso di composizione* diverso senza autorizzazioni di amministratore.

Nella finestra di dialogo successiva selezionare l'ISP (Internet Service Provider). Per scegliere l'ISP da un elenco di provider predefiniti che operano localmente, selezionare *Nazione*. In alternativa scegliere *Nuovo* per aprire una finestra di dialogo nella quale specificare i dati relativi all'ISP, ad esempio il nome della connessione telefonica e dell'ISP, oltre al login e alla password forniti dall'ISP. Selezionare *Richiedi sempre password* se si desidera che venga richiesta l'immissione della password a ogni connessione.

Nell'ultima finestra di dialogo specificare ulteriori opzioni di connessione:

Connessione su richiesta
: Se si attiva la composizione su richiesta, impostare almeno un server dei nomi.

Modifica DNS quando connesso
: Questa opzione è abilitata per default e di conseguenza l'indirizzo del server dei nomi viene aggiornato ogni volta che si esegue la connessione a Internet.

Rilevamento automatico del DNS
: Se il provider non trasmette automaticamente il server dei nomi del dominio dopo la connessione, disattivare questa opzione e immettere manualmente i dati per DNS.

Modalità stupida
: Questa opzione è abilitata per default. In tal caso i prompt di input inviati dal server dell'ISP vengono ignorati per impedire interferenze con il processo di connessione.

Interfaccia firewall esterna* e *Riavvia firewall
: La selezione di queste opzioni abilita SUSEfirewall2 che protegge il computer in uso da attacchi esterni per tutta la durata della connessione Internet.

Periodo di inattività (secondi)

Questa opzione consente di specificare un intervallo di inattività della rete, trascorso il quale il modem si disconnette automaticamente.

Dettagli IP

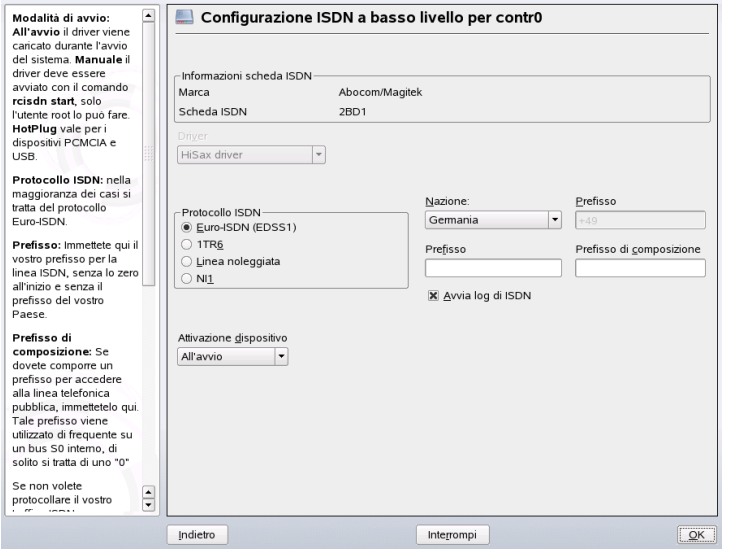
Consente di aprire la finestra di dialogo di configurazione dell'indirizzo. Se l'ISP non assegna un indirizzo IP dinamico all'host, disattivare *Indirizzo IP dinamico*, quindi immettere l'indirizzo IP locale e l'indirizzo IP remoto dell'host. Richiedere queste informazioni all'ISP. Lasciare selezionata *Route predefinita* e fare clic su *OK* per chiudere la finestra di dialogo.

Scegliendo *Avanti* viene visualizzata la finestra di dialogo originale con un riepilogo della configurazione del modem. Scegliere *Fine* per chiudere questa finestra di dialogo.

38.4.3 ISDN

Utilizzare questo modulo per la configurazione di una o più schede ISDN per il sistema in uso. Se la scheda ISDN non viene rilevata da YaST, selezionarla manualmente. Sono supportate più interfacce, tuttavia è possibile configurare più ISP per la stessa interfaccia. Nelle finestre di dialogo successive impostare le opzioni ISDN necessarie per il funzionamento corretto della scheda.

Figura 38.5 *Configurazione ISDN*

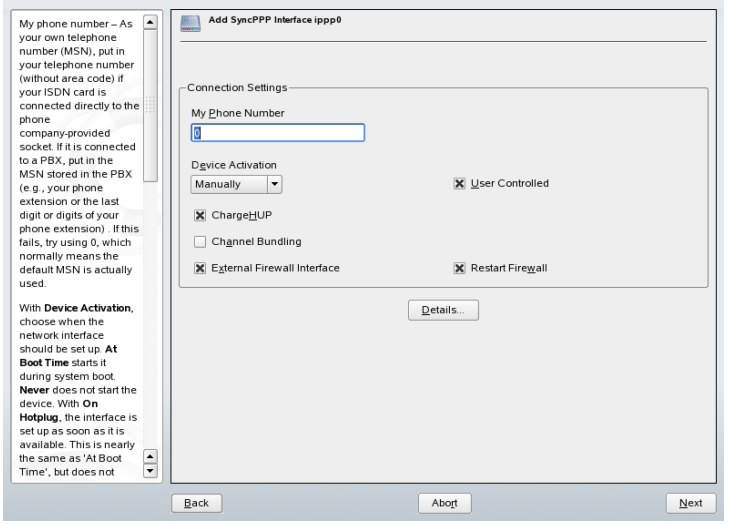


Nella finestra di dialogo successiva, illustrata nella Figura 38.5, «Configurazione ISDN» (p. 619), selezionare il protocollo da utilizzare. L'impostazione di default è *Euro-ISDN (EDSS1)*, tuttavia per i centralini meno recenti o più grandi è necessario selezionare *1TR6*. Negli Stati Uniti selezionare *NI1*. Selezionare il paese nel campo corrispondente. Il codice del paese viene visualizzato nel campo accanto. Immettere infine i valori relativi a *Prefisso* e *Prefisso di composizione*, se necessario.

Modalità di avvio consente di definire come deve essere avviata l'interfaccia ISDN: *All'avvio* attiva l'inizializzazione del driver ISDN ogni volta che viene avviato il sistema, mentre *Manuale* richiede il caricamento del driver ISDN come `root` con il comando `rcisdn start`. L'opzione *All'HotPlug* viene utilizzata per dispositivi PCMCIA o USB e consente di caricare il driver dopo il collegamento del dispositivo. Al termine, fare clic su *OK*.

NeIla finestra di dialogo successiva specificare il tipo di interfaccia per la scheda ISDN in uso e aggiungere gli ISP a un'interfaccia esistente. Le interfacce possono essere di tipo `SyncPPP` o `RawIP`, tuttavia la maggior parte degli ISP utilizza la modalità `SyncPPP` descritta di seguito.

Figura 38.6 *Configurazione dell'interfaccia ISDN*



Il numero da immettere per *Mio numero di telefono* dipende dalla particolare configurazione in uso:

Scheda ISDN connessa direttamente alla presa telefonica
: Una linea ISDN standard consente di utilizzare tre numeri di telefono, definiti numeri sottoscrittori multipli (MSN). Su richiesta del sottoscrittore i numeri possono essere un massimo di 10. Immettere uno di questi MSN in questo campo senza indicativo di località. Se si immette il numero errato, l'operatore telefonico utilizzerà automaticamente il primo MSN assegnato alla linea ISDN in uso.

Scheda ISDN connessa a un centralino
: Anche in questo caso la configurazione può variare a seconda delle apparecchiature installate:

1. I centralini (PBX) di piccole dimensioni creati per reti domestiche utilizzano principalmente il protocollo Euro-ISDN (EDSS1) per le chiamate interne. Questi centralini dispongono di un bus S0 interno e utilizzano numeri interni per gli apparecchi collegati.

   Utilizzare uno dei numeri interni come MSN. Dovrebbe essere possibile utilizzare almeno uno degli MSN del centralino abilitati per la composizione diretta dei numeri esterni. Se questa impostazione non funziona, provare a

impostare uno zero. Per ulteriori informazioni, consultare la documentazione fornita con il centralino.

2. I centralini di maggiori dimensioni progettati per le aziende utilizzano normalmente il protocollo 1TR6 per le chiamate interne. In questo caso l'MSN è detto EAZ e corrisponde di solito al numero di composizione diretta. Per la configurazione in ambiente Linux dovrebbe essere sufficiente immettere l'ultima cifra dell'EAZ. Come ultima risorsa, provare tutte le cifre nell'intervallo da 1 a 9.

Per fare in modo che la connessione venga terminata immediatamente prima del successivo scatto di tariffazione, selezionare *Disconnessione allo scatto*. Questa impostazione potrebbe tuttavia non funzionare con tutti gli ISP. Mediante la selezione dell'opzione corrispondente, è inoltre possibile abilitare il raggruppamento dei canali (connessioni multiple PPP). Infine è possibile abilitare SuSEfirewall2 sul collegamento selezionando *Interfaccia firewall esterna* e *Riavvia firewall*. Per consentire all'utente normale privo di autorizzazioni di amministratore di attivare o disattivare l'interfaccia, selezionare *Amministrata dall'utente*.

Mediante *Dettagli* è possibile aprire una finestra di dialogo per l'implementazione di schemi di connessione più complessi, che tuttavia non interessano i normali utenti privati. Fare clic su *OK* per chiudere la finestra di dialogo *Dettagli*.

Nella finestra di dialogo successiva configurare le impostazioni dell'indirizzo IP. Se il provider non ha fornito un indirizzo IP statico, selezionare *Indirizzo IP dinamico*. In caso contrario utilizzare i campi disponibili per immettere l'indirizzo IP locale e l'indirizzo IP remoto dell'host in base a quanto specificato dall'ISP. Se l'interfaccia deve corrispondere all'instradamento di default per Internet, selezionare *Route predefinita*. Per ogni host è possibile configurare una sola interfaccia come instradamento di default. Fare clic su *Avanti* per uscire da questa finestra di dialogo.

Nella finestra di dialogo successiva è possibile impostare il paese e selezionare un ISP. Gli ISP inclusi nell'elenco sono solo provider di servizi call-by-call. Se l'ISP desiderato non è incluso nell'elenco, scegliere *Nuovo*. Viene aperta la finestra di dialogo *Parametri del provider* nella quale è possibile immettere tutti i dettagli relativi all'ISP. Quando si immette il numero di telefono, evitare di inserire spazi vuoti o virgole tra le cifre. Immettere infine il login e la password forniti dall'ISP e al termine scegliere *Avanti*.

Per utilizzare *Connessione su richiesta* su una workstation autonoma, specificare anche il server dei nomi (DNS). La maggior parte degli ISP supporta il DNS dinamico e ciò

significa che l'indirizzo IP del server dei nomi viene inviato dall'ISP a ogni connessione. Per una singola workstation sarà tuttavia necessario fornire un indirizzo segnaposto, ad esempio `192.168.22.99`. Se l'ISP non supporta il DNS dinamico, specificare gli indirizzi IP del server dei nomi utilizzato dall'ISP. È possibile specificare un un timeout, ovvero il tempo massimo di inattività della rete (in secondi), scaduto il quale la connessione dovrà essere terminata automaticamente. Confermare le impostazioni scegliendo *Avanti*. In YaST viene visualizzato un riepilogo delle interfacce configurate. Per attivare queste impostazioni, scegliere *Fine*.

38.4.4 Modem via cavo

In alcuni paesi, come l'Austria e gli Stati uniti, è abbastanza comune accedere a Internet tramite le rete TV via cavo. Il sottoscrittore della TV via cavo riceve di solito un modem che viene collegato alla presa del cavo TV da un lato e alla scheda di rete del computer dall'altro mediante un cavo a doppini intrecciati 10Base-TG. Il modem via cavo fornisce una connessione Internet dedicata con un indirizzo IP fisso.

A seconda delle istruzioni fornite dall'ISP, quando si configura la scheda di rete selezionare *Impostazione automatica indirizzi (via DHCP)* o *Impostazione statica dell'indirizzo*. Quasi tutti i provider utilizzano DHCP, tuttavia viene spesso fornito un indirizzo IP statico viene spesso fornito nell'ambito di uno speciale account aziendale.

38.4.5 DSL

Per configurare il dispositivo DSL in uso, selezionare il modulo *DSL* nella sezione *Dispositivi di rete* di YaST. Questo modulo di YaST è composto da diverse finestre di dialogo nelle quali è possibile impostare i parametri dei collegamenti DSL basati su uno dei protocolli seguenti:

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoATM)
- CAPI for ADSL (schede Fritz)
- Point-to-Point Tunneling Protocol (PPTP)—Austria

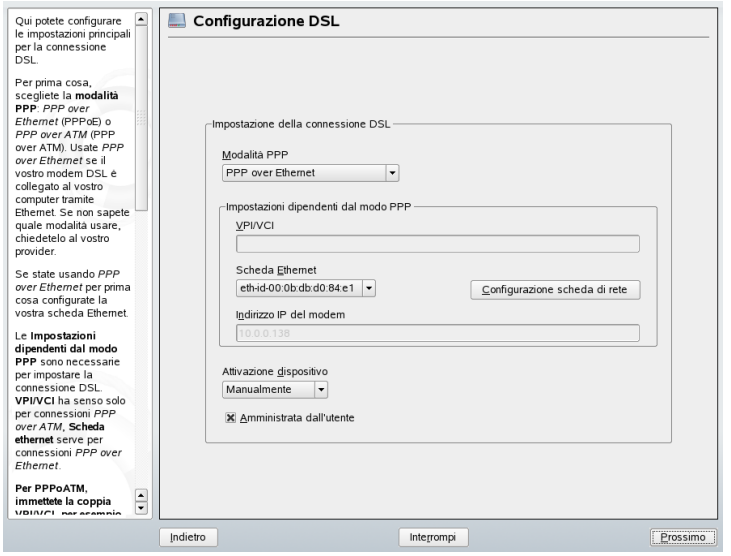
La configurazione di una connessione DSL basata sul protocollo PPPoE o PPTP richiede la preventiva configurazione corretta della scheda di rete corrispondente. Se questa

operazione non è ancora stata effettuata, selezionare *Configura scheda di rete* per configurare la scheda (vedere la Sezione 38.4.1, «Configurazione della scheda di rete con YaST» (p. 613)). Nel caso di un collegamento DSL gli indirizzi possono essere assegnati automaticamente ma non tramite DHCP, per questo è necessario evitare di selezionare l'opzione *Impostazione automatica indirizzi (via DHCP)*. Immettere invece un indirizzo statico fittizio per l'interfaccia, ad esempio `192.168.22.1`. In *Maschera di sottorete* immettere `255.255.255.0`. Se si configura una workstation autonoma, lasciare vuoto il campo *Gateway predefinito*.

SUGGERIMENTO

I valori in *Indirizzo IP* e *Maschera di sottorete* sono solo segnaposto e sono necessari solo per inizializzare la scheda di rete, ma non rappresentano il collegamento DSL come tale.

Figura 38.7 *Configurazione DSL*



Per iniziare la configurazione della connessione DSL (vedere la Figura 38.7, «Configurazione DSL» (p. 623)), selezionare innanzitutto la modalità PPP e la scheda Ethernet alla quale è connesso il modem DSL (si tratta quasi sempre di `eth0`). Utilizzare quindi *Attivazione dispositivo* per specificare se il collegamento DSL dovrà essere stabilito durante il processo di avvio. Fare clic su *Amministrata dall'utente* per consentire

all'utente normale privo di autorizzazioni root di attivare o disattivare l'interfaccia con KInternet. In questa finestra di dialogo è inoltre possibile selezionare il paese e scegliere uno dei numerosi ISP disponibili. I dettagli delle finestre di dialogo successive nella configurazione DSL dipendono dalle opzioni impostate finora, pertanto nei seguenti paragrafi vengono menzionate solo brevemente. Per informazioni sulle opzioni disponibili, leggere la guida contestuale disponibile nelle singole finestre di dialogo.

Per utilizzare *Connessione su richiesta* su una workstation autonoma, specificare anche il server dei nomi (DNS). La maggior parte degli ISP supporta il DNS dinamico, ovvero l'indirizzo IP del server dei nomi viene inviato dall'ISP a ogni connessione. Per una singola workstation fornire comunque un indirizzo segnaposto, ad esempio `192.168.22.99`. Se l'ISP non supporta il DNS dinamico, immettere l'indirizzo IP del server dei nomi fornito dall'ISP.

Periodo di inattività (secondi) consente di definire un intervallo di inattività della rete, trascorso il quale la connessione viene terminata automaticamente. Un valore di timeout adeguato è compreso tra 60 e 300 secondi. Se l'opzione *Connessione su richiesta* è disattivata, può essere utile impostare il timeout su zero per impedire la disconnessione automatica.

La configurazione T-DSL è molto simile a DSL. È sufficiente selezionare *Compagnia telefonica* come provider per visualizzare la finestra di configurazione T-DSL, nella quale immettere alcune informazioni aggiuntive necessarie per T-DSL, ovvero l'ID della linea, il numero della compagnia telefonica, il codice utente e la password. Tutti questi dati dovrebbero essere inclusi nelle informazioni ricevute dopo la sottoscrizione a T-DSL.

38.5 Configurazione manuale di una connessione di rete

L'esecuzione manuale della configurazione del software di rete dovrebbe costituire un'alternativa estrema, al contrario di YaST il cui uso è consigliato. Queste informazioni generali sulla configurazione della rete possono tuttavia essere utili anche quando si utilizza YaST.

Tutte le schede di rete incorporate e di tipo HotPlug (PCMCIA, USB e alcune schede PCI) vengono rilevate e configurate mediante la tecnologia HotPlug. Una scheda di rete viene vista dal sistema in due modi, prima come dispositivo fisico e quindi come

interfaccia. L'inserimento o il rilevamento di un dispositivo attiva un evento HotPlug, che a sua volta attiva l'inizializzazione del dispositivo mediante lo script `hwup`. Dopo l'inizializzazione della scheda di rete come una nuova interfaccia di rete, il kernel genera un altro evento HotPlug che attiva la configurazione dell'interfaccia mediante `ifup`.

I nomi di interfaccia vengono numerati dal kernel in base all'ordine temporale della relativa registrazione, mentre la sequenza di inizializzazione definisce l'assegnazione dei nomi. Se per una delle schede di rete si verifica un errore, la numerazione di tutte le schede inizializzate successivamente viene spostata. Per le schede realmente collegabili a caldo, il fattore determinante è l'ordine in cui vengono collegati i dispositivi.

Ai fini della flessibilità, la configurazione del dispositivo (hardware) e dell'interfaccia è stata separata e la mappatura delle configurazioni ai dispositivi e alle interfacce non viene più gestita in base ai nomi delle interfacce. Le configurazioni dei dispositivi si trovano nel percorso `/etc/sysconfig/hardware/hwcfg-*`, mentre quelle delle interfacce si trovano nel percorso `/etc/sysconfig/network/ifcfg-*`. I nomi delle configurazioni vengono assegnati secondo un metodo descrittivo che consente di identificare i dispositivi e le interfacce a cui sono associate. Il precedente metodo di mappatura dei driver ai nomi di interfaccia richiedeva l'uso di nomi di interfaccia statici, pertanto non può più essere utilizzato in `/etc/modprobe.conf`. Secondo il nuovo concetto, le voci alias immesse in questo file potrebbero causare effetti collaterali indesiderati.

I nomi di configurazione, ovvero la parte che segue `hwcfg-` o `ifcfg-`, possono descrivere i dispositivi per mezzo dello slot, di un ID specifico del dispositivo o del nome di interfaccia. Il nome di configurazione di una scheda PCI, ad esempio, potrebbe essere `bus-pci-0000:02:01.0` (slot PCI) o `vpid-0x8086-0x1014-0x0549` (fornitore e ID prodotto). Il nome dell'interfaccia associata potrebbe essere `bus-pci-0000:02:01.0` o `wlan-id-00:05:4e:42:31:7a` (indirizzo MAC).

Per assegnare una determinata configurazione di rete a una scheda qualsiasi di un certo tipo (di cui ne viene inserita una sola alla volta) anziché una certa scheda, selezionare nomi di configurazione meno specifici. Ad esempio, è possibile utilizzare `bus-pcmcia` per tutte le schede PCMCIA. I nomi possono essere limitati, d'altra parte, da un precedente tipo di interfaccia. Ad esempio, alle schede WLAN connesse a una porta USB verrà assegnato il nome `wlan-bus-usb`.

Il sistema utilizza sempre le configurazione che descrive meglio un'interfaccia o il dispositivo che fornisce l'interfaccia. La ricerca della configurazione più adatta viene gestita da `getcfg`. Nell'output di `getcfg` sono disponibili tutte le informazioni che

è possibile utilizzare per descrivere un dispositivo. I dettagli riguardanti la specifica dei nomi di configurazione sono disponibili nella documentazione di `getcfg`.

Con il metodo descritto è possibile configurare un'interfaccia di rete nel modo corretto anche se i dispositivi di rete non sono sempre inizializzati nello stesso ordine. Il nome dell'interfaccia continua tuttavia a dipendere dalla sequenza di inizializzazione. Sono disponibili due modi per assicurare l'accesso in maniera affidabile all'interfaccia di una determinata scheda di rete:

- `getcfg-interface` *`nome configurazione`* restituisce il nome dell'interfaccia di rete associata. In alcuni file di configurazione è quindi possibile immettere il nome della configurazione, ad esempio firewall, dhcpd, instradamento o varie interfacce di rete virtuali (tunnel), anziché il nome di interfaccia che non è permanente.

- I nomi di interfaccia permanenti possono essere assegnati a tutte le interfacce le cui configurazioni non includono nomi di interfaccia. Questa operazione può essere eseguita per mezzo di voci `PERSISTENT_NAME=`*`nomep`* nella configurazione di un'interfaccia (`ifcfg-*`). Il nome permanente *`nomep`* non dovrà tuttavia essere lo stesso nome assegnato automaticamente dal kernel, quindi `eth*`, `tr*`, `wlan*` e così via non sono consentiti. Utilizzare invece `net*` o nomi descrittivi come `external`, `internal` o `dmz`. Un nome permanente può essere assegnato a un'interfaccia solo immediatamente dopo la registrazione e ciò significa che il driver della scheda di rete deve essere ricaricato o che deve essere eseguito il comando `hwup` *`descrizione dispositivo`*. Il comando `rcnetwork restart` non è sufficiente per questo scopo.

  IMPORTANTE: uso di nomi di interfaccia permanenti

  L'uso di nomi di interfaccia permanenti non è stato testato in tutte le aree, quindi è possibile che alcune applicazioni non siano in grado di gestire nomi di interfaccia selezionati liberamente.

`ifup` richiede un'interfaccia esistente, in quanto l'hardware non viene inizializzato. L'inizializzazione dell'hardware viene gestita dal comando `hwup`, eseguito da `hotplug` o `coldplug`. Quando si inizializza un dispositivo, viene eseguito automaticamente `ifup` per la nuova interfaccia tramite `hotplug`, la quale viene configurata se la modalità di avvio è impostata su `onboot`, `hotplug` o `auto` e il servizio `network` è stato avviato. In precedenza il comando `ifup` *`nomeinterfaccia`* attivava l'inizializzazione dell'hardware, mentre ora la procedura è stata invertita. Un componente

hardware viene prima di tutto inizializzato, quindi seguono tutte le altre azioni. In questo modo è sempre possibile configurare un numero variabile di dispositivi nel modo migliore possibile mediante un set di configurazioni esistente.

Nella Tabella 38.5, «Script di configurazione manuale della rete» (p. 627) sono riassunti gli script più importanti utilizzati nella configurazione della rete. Dove possibile gli script sono distinti per hardware e interfaccia.

Tabella 38.5 *Script di configurazione manuale della rete*

Fase di configurazione	Comando	Funzione
Hardware	`hw{up,down,status}`	Gli script `hw*` vengono eseguiti dal sottosistema HotPlug per inizializzare un dispositivo, annullare l'inizializzazione o richiedere lo stato di un dispositivo. Ulteriori informazioni sono disponibili nella documentazione di `hwup`.
Interfaccia	`getcfg`	`getcfg` può essere utilizzato per richiedere il nome dell'interfaccia associata a un nome di configurazione o a una descrizione dell'hardware. Ulteriori informazioni sono disponibili nella documentazione di `getcfg`.
Interfaccia	`if{up,down,status}`	Gli script `if*` avviano le interfacce di rete esistenti o restituiscono lo stato dell'interfaccia specificata. Ulteriori informazioni sono disponibili nella documentazione di `ifup`.

Ulteriori informazioni su HotPlug e sui nomi di dispositivi permanenti sono disponibili nel Capitolo 32, *Sistema Hotplug* (p. 527) e nel Capitolo 33, *Nodi di dispositivi dinamici con* `udev` (p. 535).

38.5.1 File di configurazione

In questa sezione viene fornita una panoramica dei file di configurazione di rete e vengono descritti lo scopo e il formato utilizzato.

/etc/syconfig/hardware/hwcfg-*

Questi file contengono le configurazioni hardware delle schede di rete e di altri dispositivi, oltre ai parametri necessari, ad esempio il modulo del kernel, la modalità di avvio e le associazioni di script. Per informazioni, fare riferimento alla documentazione di `hwup`. Indipendentemente dall'hardware esistente, le configurazioni `hwcfg-static-*` vengono applicate all'avvio di coldplug.

/etc/sysconfig/network/ifcfg-*

Questi file contengono le configurazioni per l'interfaccia di rete, ad esempio la modalità di avvio e l'indirizzo IP. I parametri possibili sono descritti nella documentazione di `ifup`. Se fosse necessario utilizzare un'impostazione generale per una sola interfaccia, è inoltre possibile utilizzare tutte le variabili dai file `dhcp`, `wireless` e `config` nei file `ifcfg-*`.

/etc/sysconfig/network/config, dhcp, wireless

Il file `config` contiene impostazioni generali relative al comportamento di `ifup`, `ifdown` e `ifstatus`. `dhcp` contiene impostazioni per DHCP e `wireless` per le schede LAN wireless. Le variabili nei tre file di configurazione sono commentate e possono essere utilizzate anche nei file `ifcfg-*`, dove sono considerate con maggiore priorità.

/etc/sysconfig/network/routes,ifroute-*

In questo file viene determinato l'instradamento statico dei pacchetti TCP/IP. Tutti gli instradamenti statici necessari per i vari task di sistema possono essere immessi nel file `/etc/sysconfig/network/routes`, ovvero instradamenti a un host, a un host tramite un gateway e a una rete. Per ogni interfaccia che richiede un instradamento individuale, è necessario definire un file di configurazione aggiuntivo, `/etc/sysconfig/network/ifroute-*`. Sostituire `*` con il nome dell'interfaccia. Le voci contenute nei file di configurazione dell'instradamento hanno un aspetto analogo al seguente:

```
# Destination     Dummy/Gateway     Netmask            Device
#
127.0.0.0         0.0.0.0           255.255.255.0      lo
204.127.235.0     0.0.0.0           255.255.255.0      eth0
default           204.127.235.41    0.0.0.0            eth0
207.68.156.51     207.68.145.45     255.255.255.255    eth1
192.168.0.0       207.68.156.51     255.255.0.0        eth1
```

Nella prima colonna è indicata la destinazione dell'instradamento, ad esempio l'indirizzo IP di una rete o di un host oppure, nel caso di nomi di server *raggiungibili*, il nome completo della rete o dell'host.

Nella seconda colonna è indicato il gateway di default o un gateway attraverso il quale è possibile accedere a un host o alla rete. Nella terza colonna è indicata la maschera di rete per le reti o gli host che utilizzano un gateway. Ad esempio, `255.255.255.255` è la maschera per un host che utilizza un gateway.

La quarta colonna si riferisce solo alle reti connesse all'host locale, ad esempio un dispositivo di loopback, Ethernet, ISDN, PPP o fittizio. Il nome del dispositivo deve essere immesso in questa colonna.

È possibile utilizzare una quinta colonna facoltativa per specificare il tipo di un instradamento. Per assicurare la corretta interpretazione del comando da parte del parser, dovrà essere inserito un segno meno – nelle colonne non necessarie. Per informazioni, fare riferimento alla documentazione di `routes(5)`.

/etc/resolv.conf

In questo file (parola chiave `search`) viene specificato il dominio a cui appartiene l'host, oltre allo stato dell'indirizzo del server dei nomi (parola chiave `nameserver`).

È possibile specificare più nomi di domini. Quando viene risolto un nome non completo, viene effettuato il tentativo di generarne uno aggiungendo le singole voci di `search`. Per utilizzare più server dei nomi immettere più righe, iniziando ognuna con `nameserver`. Anteporre ai commenti segni `#`. Il server dei nomi specificato viene immesso da YaST in questo file. Nell'Esempio 38.5, «/etc/resolv.conf» (p. 630) è illustrato il possibile aspetto di `/etc/resolv.conf`.

Esempio 38.5 */etc/resolv.conf*

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

Alcuni servizi, ad esempio `pppd` (`wvdial`), `ipppd` (`isdn`), `dhcp` (`dhcpcd` e `dhclient`), `pcmcia` e `hotplug`, modificano il file `/etc/resolv.conf` mediante lo script `modify_resolvconf`. Se il file `/etc/resolv.conf` è stato modificato temporaneamente da questo script, contiene un commento predefinito con informazioni sul servizio che ha apportato la modifica, sulla posizione in cui si trova la copia di backup del file originale e sul modo per disattivare il meccanismo di modifica automatico. Se `/etc/resolv.conf` viene modificato più volte, include le modifiche in un formato nidificato. Tali modifiche possono essere ripristinate correttamente anche se l'operazione viene eseguita in un ordine diverso da quello in cui sono state immesse. I servizi che potrebbero richiedere questa flessibilità comprendono `isdn`, `pcmcia` e `hotplug`.

Se un servizio non è stato terminato in modo normale e corretto, è possibile utilizzare `modify_resolvconf` per ripristinare il file originale. All'avvio del sistema viene inoltre eseguito un controllo per verificare se, ad esempio, dopo un crash di sistema è presente un file `resolv.conf` modificato e non pulito, nel qual caso viene ripristinato il file `resolv.conf` originale (non modificato).

In YaST viene utilizzato il comando `modify_resolvconf check` per verificare se `resolv.conf` è stato modificato, quindi all'utente viene notificato che dopo il ripristino del file le modifiche andranno perse. A parte questo aspetto, `modify_resolvconf` non viene utilizzato da YaST e ciò significa che l'impatto della modifica di `resolv.conf` tramite YaST è lo stesso di qualsiasi modifica manuale. In entrambi i casi le modifiche hanno un effetto permanente, mentre le modifiche richieste dai servizi sopra indicati sono solo temporanee.

/etc/hosts

In questo file, illustrato nell'Esempio 38.6, «/etc/hosts» (p. 631), gli indirizzi IP vengono assegnati a nomi host. Se non viene implementato un server dei nomi, tutti gli host con i quali verrà stabilita una connessione IP devono essere elencati in questo file. Per ogni host immettere nel file una riga formata dall'indirizzo IP, dal nome host completo e dal nome host. L'indirizzo IP deve trovarsi all'inizio della riga e le voci devono essere separate da spazi vuoti e tabulazioni. I commenti sono sempre preceduti dal segno #.

Esempio 38.6 */etc/hosts*

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.0 earth.example.com earth
```

/etc/networks

In questo file i nomi di rete vengono convertiti in indirizzi di rete. Il formato è simile a quello del file `hosts`, ad eccezione del fatto che i nomi di rete precedono gli indirizzi. Vedere l'Esempio 38.7, «/etc/networks» (p. 631).

Esempio 38.7 */etc/networks*

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

La risoluzione del nome, ovvero la conversione dei nomi host e di rete tramite la libreria del *Resolver*, viene controllata da questo file. Questo file viene utilizzato solo per i programmi collegati a libc4 o libc5. Per gli attuali programmi glibc, fare riferimento alle impostazioni contenute nel file `/etc/nsswitch.conf`. Utilizzare una riga per ogni singolo parametro. I commenti sono preceduti da un segno #. Nella Tabella 38.6, «Parametri per /etc/host.conf» (p. 632) sono illustrati i parametri disponibili. Nell'Esempio 38.8, « /etc/host.conf » (p. 632) è riportato un esempio di file `/etc/host.conf`.

Tabella 38.6 *Parametri per /etc/host.conf*

order *hosts*, *bind*	Specifica in quale ordine viene eseguito l'accesso ai servizi per la risoluzione del nome. Gli argomenti disponibili, separati da spazi vuoti o da virgole, sono: *hosts*: cerca il file `/etc/hosts`. *bind*: accede a un server dei nomi. *nis*: utilizza NIS.
multi *on*/*off*	Definisce se un host immesso nel file `/etc/hosts` può avere più indirizzi IP.
nospoof *on* spoofalert *on*/*off*	Questi parametri hanno effetto sullo *spoofing* del server dei nomi tuttavia, a parte ciò, non hanno alcuna influenza sulla configurazione della rete.
trim *domainname*	Il nome di dominio specificato viene separato dal nome host dopo la risoluzione di quest'ultimo, a condizione che nel nome host sia incluso il nome di dominio. Questa opzione è utile se nel file `/etc/hosts` sono inclusi solo i nomi dal dominio locale, i quali devono tuttavia essere riconosciuti mediante i nomi di dominio associati.

Esempio 38.8 */etc/host.conf*

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

/etc/nsswitch.conf

L'introduzione della Libreria GNU C 2.0 è stata accompagnata dall'introduzione di *Name Service Switch* (NSS). Per informazioni, fare riferimento alla documentazione di `nsswitch.conf(5)` e a *The GNU C Library Reference Manual*.

L'ordine delle query è definito nel file `/etc/nsswitch.conf`. Nell'Esempio 38.9, «/etc/nsswitch.conf» (p. 633) è riportato un esempio di file `nsswitch.conf`. I commenti sono introdotti da segni `#`. In questo esempio la voce nel database `hosts` significa che viene inviata una richiesta a `/etc/hosts` (`files`) tramite DNS (vedere il Capitolo 40, *DNS: Domain Name System* (p. 643)).

Esempio 38.9 */etc/nsswitch.conf*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

I «database» disponibili tramite NSS sono elencati nella Tabella 38.7, «Database disponibili tramite /etc/nsswitch.conf» (p. 633). Nel prossimo futuro sono inoltre previsti `automount`, `bootparams`, `netmasks` e `publickey`. Le opzioni di configurazione per i database NSS sono elencate nella Tabella 38.8, «Opzioni di configurazione per i «database» NSS» (p. 634).

Tabella 38.7 *Database disponibili tramite /etc/nsswitch.conf*

`aliases`	Alias di posta implementati da `sendmail`; vedere `man 5 aliases`.
`ethers`	Indirizzi Ethernet.
`group`	Per gruppi di utenti, utilizzato da `getgrent`. Vedere anche la documentazione per `group`.
`hosts`	Per nomi host e indirizzi IP, utilizzato da `gethostbyname` e funzioni simili.
`netgroup`	Elenchi di utenti e host validi presenti nella rete allo scopo di controllare le autorizzazioni di accesso; vedere la documentazione di `netgroup(5)`.

networks	Nomi e indirizzi di rete, utilizzato da getnetent.
passwd	Password utente, utilizzato da getpwent; vedere la documentazione di passwd(5).
protocols	Protocolli di rete, utilizzato da getprotoent; vedere la documentazione di protocols(5).
rpc	Nomi e indirizzi di chiamate di procedura remota (RPC), utilizzato da getrpcbyname e funzioni simili.
services	Servizi di rete, utilizzato da getservent.
shadow	Password shadow di utenti, utilizzato da getspnam; vedere la documentazione di shadow(5).

Tabella 38.8 *Opzioni di configurazione per i «database» NSS*

files	Accesso diretto ai file, ad esempio /etc/aliases.
db	Accesso tramite un database.
nis, nisplus	NIS, vedere anche il Capitolo 41, *Uso di NIS* (p. 665).
dns	Può essere utilizzata solo come estensione per hosts e networks.
compat	Può essere utilizzata solo come estensione per passwd, shadow e group.

/etc/nscd.conf

Questo file viene utilizzato per configurare nscd (Name Service Cache Daemon). Vedere la documentazione di nscd(8) e di nscd.conf(5). Per default, le voci di sistema di passwd e groups vengono memorizzate nella cache da nscd. È un aspetto importante per le prestazioni dei servizi di directory, come NIS e LDAP, poiché diversamente sarebbe necessario utilizzare la connessione di rete per ogni accesso a

nomi o gruppi. `hosts` non viene memorizzato nella cache per default, in quanto il meccanismo di nscd per la memorizzazione nella cache di host non consente al sistema locale di eseguire in modo sicuro i controlli per le ricerche dirette e inverse. Anziché richiedere la memorizzazione nella cache dei nomi da parte di nscd, configurare un server DNS di caching.

Se viene attivata la funzione di caching per `passwd`, il riconoscimento di un nuovo utente locale aggiunto richiede di solito circa 15 secondi. Per ridurre questo tempo di attesa, riavviare nscd con il comando `rcnscd restart`.

/etc/HOSTNAME

Questo file contiene il nome host senza il nome di dominio associato e viene letto da numerosi script durante l'avvio del computer. Può contenere una sola riga nella quale è impostato il nome host.

38.5.2 Script di avvio

Oltre ai file di configurazione descritti in precedenza, sono disponibili diversi altri script che caricano i programmi di rete durante l'avvio del computer e che vengono avviati non appena il sistema passa a uno dei *runlevel multi-utente*. Nella Tabella 38.9, «Alcuni script di avvio per i programmi di rete» (p. 635) sono descritti alcuni di questi script.

Tabella 38.9 *Alcuni script di avvio per i programmi di rete*

`/etc/init.d/network`	Questo script gestisce la configurazione delle interfacce di rete. L'hardware deve essere già stato inizializzato da `/etc/init.d/coldplug` (tramite `hotplug`). Se il servizio `network` non è stato avviato, le interfacce di rete non verranno implementate al momento dell'inserimento tramite hotplug.
`/etc/init.d/inetd`	Avvia xinetd che può essere utilizzato per rendere disponibili i servizi server nel sistema. Ad esempio, può avviare vsftpd ogni volta che viene iniziata una connessione FTP.

`/etc/init.d/portmap`	Avvia il portmapper necessario per il server RPC, ad esempio un server NFS.
`/etc/init.d/nfsserver`	Avvia il server NFS.
`/etc/init.d/sendmail`	Controlla il processo sendmail.
`/etc/init.d/ypserv`	Avvia il server NIS.
`/etc/init.d/ypbind`	Avvia il client NIS.

38.6 smpppd come assistente di connessione remota

Molti utenti privati non dispongono di una linea dedicata per la connessione a Internet ma utilizzano connessioni telefoniche. A seconda del metodo utilizzato (ISDN o DSL), la connessione telefonica viene controllata da ipppd o pppd. Per connettersi in rete è sufficiente avviare questi programmi nel modo corretto.

Se si dispone di una connessione a tariffa fissa che non genera costi aggiuntivi per la connessione telefonica, avviare semplicemente il rispettivo daemon. Controllare la connessione telefonica con un'applet KDE o un'interfaccia della riga di comando. Se il gateway Internet non corrisponde all'host in uso, si consiglia di controllare la connessione telefonica mediante un host di rete.

In questo caso, utilizzare smpppd che dispone di un'interfaccia uniforme per i programmi ausiliari e funziona in due direzioni. Programma innanzitutto il servizio pppd o ipppd necessario e controlla le proprietà di connessione telefonica, quindi rende disponibili vari provider per i programmi utente e trasmette informazioni sullo stato corrente della connessione. Poiché smpppd può essere controllato anche attraverso la rete, è adatto per il controllo delle connessioni telefoniche a Internet da una workstation in una sottorete privata.

38.6.1 Configurazione di smpppd

Le connessioni fornite da smpppd vengono configurate automaticamente da YaST. Vengono inoltre configurati gli effettivi programmi di connessione telefonica KInternet e cinternet, mentre le impostazioni manuali sono necessarie solo per la configurazione di funzionalità aggiuntive di smpppd, ad esempio il controllo remoto.

Il file di configurazione di smpppd, `/etc/smpppd.conf`, non abilita il controllo remoto di default. Di seguito sono descritte le opzioni più importanti di questo file di configurazione:

open-inet-socket = ***yes|no***
: Per controllare smpppd attraverso al rete, impostare questa opzione su `yes`. smpppd è in ascolto sulla porta `3185`. Se questo parametro viene impostato su `yes`, impostare di conseguenza anche i parametri `bind-address`, `host-range` e `password`.

bind-address = ***ip***
: Se a un host sono assegnati più indirizzi IP, utilizzare questo parametro per determinare a quale indirizzo IP devono essere accettate le connessioni da parte di smpppd.

host-range = ***min ip max ip***
: Il parametro `host-range` definisce un intervallo di rete. Agli host con indirizzi IP inclusi in questo intervallo è consentito l'accesso a smpppd. L'accesso viene invece negato a tutti gli host che non rientrano in questo intervallo.

password = ***password***
: Mediante l'assegnazione di una password è possibile limitare l'accesso dei client agli host autorizzati. Per questa password viene utilizzato testo normale, quindi è opportuno non sopravvalutare la sicurezza che consente di applicare. Se non viene assegnata una password, tutti i client possono accedere a smpppd.

slp-register = ***yes|no***
: Con questo parametro è possibile annunciare il servizio smpppd in rete tramite SLP.

Ulteriori informazioni su smpppd sono disponibili nella documentazione di `smpppd(8)` e di `smpppd.conf(5)`.

38.6.2 Configurazione di KInternet, cinternet e qinternet per l'uso remoto

KInternet, cinternet e qinternet possono essere utilizzate per controllare un servizio smpppd locale o remoto. cinternet costituisce la controparte della riga di comando dell'utilità grafica KInternet. qinternet è fondamentalmente uguale a KInternet, ma non utilizza le librerie KDE, quindi non richiede l'uso di KDE e deve essere installata separatamente. Per preparare queste utilità in modo che possano essere utilizzate con un servizio smpppd remoto, modificare il file di configurazione `/etc/smpppd-c.conf` manualmente o tramite KInternet. In questo file vengono utilizzate solo tre opzioni:

sites = ***list of sites***
: In questo parametro viene indicato ai front-end dove cercare smpppd. Il test delle opzioni viene eseguito dai front-end nell'ordine specificato in questo parametro. L'opzione `local` ordina l'esecuzione di una connessione al servizio smpppd locale. `gateway` punta a un servizio smpppd sul gateway. La connessione dovrà essere stabilita come specificato alla voce `server` in `config-file`. `slp` ordina ai front-end di connettersi a un smpppd individuato tramite SLP.

server = ***server***
: Specificare l'host sul quale è in esecuzione smpppd.

password = ***password***
: Inserire la password selezionata per smpppd.

Se smpppd è attivo, è possibile provare ad accedervi, ad esempio con `cinternet --verbose --interface-list`. In caso di difficoltà, fare riferimento alla documentazione di `smpppd-c.conf(5)` e di `cinternet(8)`.

39 Servizi SLP in rete

Service Location Protocol (SLP) è stato sviluppato per semplificare la configurazione dei client connessi in una rete locale. Per configurare un client di rete, inclusi tutti i servizi necessari, l'amministratore deve in genere disporre di informazioni dettagliate relative ai server disponibili nella rete. Con SLP è possibile comunicare la disponibilità di un determinato servizio a tutti i client nella rete locale. Le applicazioni che supportano SLP possono quindi utilizzare le informazioni distribuite ed essere configurate automaticamente.

SUSE Linux supporta l'installazione mediante origini di installazione rese disponibili tramite SLP e include molti servizi di sistema con supporto integrato per SLP. Sia in YaST che in Konqueror sono disponibili front-end appropriati per SLP. È possibile utilizzare SLP per fornire ai client di rete funzioni centrali, ad esempio un server di installazione, un server YOU, un file server o un server di stampa in SUSE Linux.

39.1 Registrazione dei servizi personalizzati

Molte applicazioni in ambiente SUSE Linux dispongono già del supporto integrato per SLP mediante l'uso della libreria `libslp`. Se un servizio non è stato compilato con il supporto SLP, utilizzare una delle procedure seguenti per renderlo disponibile con SLP:

Registrazione statica tramite `/etc/slp.reg.d`
Creare un file di registrazione separato per ogni nuovo servizio. Di seguito è riportato un esempio di file per la registrazione di un servizio scanner:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

La riga più importante di questo file è l'*URL del servizio* che inizia con `service:`. Contiene il tipo di servizio (`scanner.sane`) e l'indirizzo al quale è disponibile il servizio sul server. *`$HOSTNAME`* viene sostituito automaticamente con il nome host completo. Segue il nome della porta TCP, separata da una virgola, tramite la quale è accessibile il servizio corrispondente. Viene quindi immessa la lingua che dovrà essere utilizzata per la visualizzazione del servizio e la durata della registrazione, espressa in secondi. Questi valori devono essere separati dall'URL del servizio mediante virgole. Impostare la durata della registrazione su un valore compreso tra `0` e `65535`. `0` impedisce la registrazione, mentre `65535` rimuove qualsiasi restrizione.

Nel file di registrazione sono inoltre presenti due variabili `watch-tcp-port` e `description`. La prima collega l'annuncio del servizio SLP allo stato attivo del servizio corrispondente che viene controllato da slpd. La seconda variabile contiene una descrizione più precisa del servizio visualizzato nei browser applicabili.

Registrazione statica con `/etc/slp.reg`
La sola differenza rispetto alla procedura descritta in precedenza è il raggruppamento di tutti i servizi in un file centrale.

Registrazione dinamica con slptool
Se è necessario registrare un servizio per SLP da script proprietari, utilizzare il front-end della riga di comando slptool.

39.2 Front-end SLP in SUSE Linux

In SUSE Linux sono disponibili numerosi front-end che consentono il controllo e l'uso delle informazioni relative a SLP attraverso una rete:

slptool
slptool è un semplice programma della riga di comando che può essere utilizzato per annunciare richieste SLP presenti nella rete o per annunciare servizi proprietari.

Con `slptool --help` è possibile visualizzare un elenco di tutte le opzioni e le funzioni disponibili. slptool può inoltre essere chiamato da script che elaborano le informazioni su SLP.

Browser SLP di YaST
YaST include un browser SLP separato che consente di elencare tutti i servizi presenti nella rete locale, annunciati tramite SLP, in un diagramma ad albero in *Servizi di rete → Browser SLP*.

Konqueror
Quando viene utilizzato come browser di rete, Konqueror è in grado di visualizzare tutti i servizi SLP disponibili nella rete locale in `slp:/`. Fare clic sulle icone nella finestra principale per visualizzare informazioni più dettagliate sul servizio corrispondente. Se si utilizza Konqueror con `service:/`, fare clic sulla relativa icona nella finestra del browser per configurare una connessione con il servizio selezionato.

39.3 Attivazione di SLP

Se si desidera che vengano offerti servizi, slpd deve essere in esecuzione nel sistema in uso. Non è necessario avviare questo daemon semplicemente per creare richieste di servizio. Come la maggior parte dei servizi di sistema in SUSE Linux, il daemon slpd viene controllato per mezzo di uno script init separato. Il daemon è inattivo di default. Per attivarlo per la durata di una sessione, eseguire `rcslpd start` come `root` per avviarlo e `rcslpd stop` per interromperlo. Eseguire un riavvio o un controllo dello stato con `restart` o `status`. Se slpd deve essere attivo di default, eseguire una volta il comando `insserv slpd` come `root`. In questo modo slpd viene incluso automaticamente nel set di servizi avviati all'avvio del sistema.

39.4 Ulteriori informazioni

Nel materiale di consultazione seguente sono disponibili ulteriori informazioni su SLP:

RFC 2608, 2609, 2610
RFC 2608 tratta in generale la definizione di SLP. RFC 2609 descrive in dettaglio la sintassi degli URL dei servizi utilizzati, mentre RFC 2610 descrive DHCP mediante SLP.

http://www.openslp.com (in lingua inglese)
Home page del progetto OpenSLP.

file:/usr/share/doc/packages/openslp/*
In questa directory è contenuta tutta la documentazione disponibile relativa a SLP, incluso un file `README.SuSE` contenente i dettagli per SUSE Linux, le RFC sopra descritte e due documenti HTML introduttivi. I programmatori che desiderano utilizzare le funzioni di SLP devono installare il pacchetto `openslp-devel` per consultare la *guida per programmatori*.

40 DNS: Domain Name System

Compito del DNS Domain Name System è di risolvere i nomi di dominio e host in indirizzi IP. In tal modo l'indirizzo IP 192.168.0.0 viene assegnato ad esempio all'host `earth`. Prima di configurare un proprio server dei nomi, leggete le informazioni generali riguardanti il DNS che trovate nella Sezione 38.3, «Risoluzione del nome» (p. 611). L'esempio di configurazione riportato si riferische a BIND

40.1 Nozioni di base su DNS

40.2 Configurazione con YaST

Il modulo DNS di YaST vi consente di configurare un server DNS proprio nella rete locale. Questo modulo funziona in due modi. Al primo avvio del modulo l'amministratore deve prendere delle decisioni fondamentali. Una volta portata a termine la configurazione iniziale il server è preconfigurato e pronto ad essere impiegato. Il modo per esperti consente di eseguire interventi configurativi più complessi.

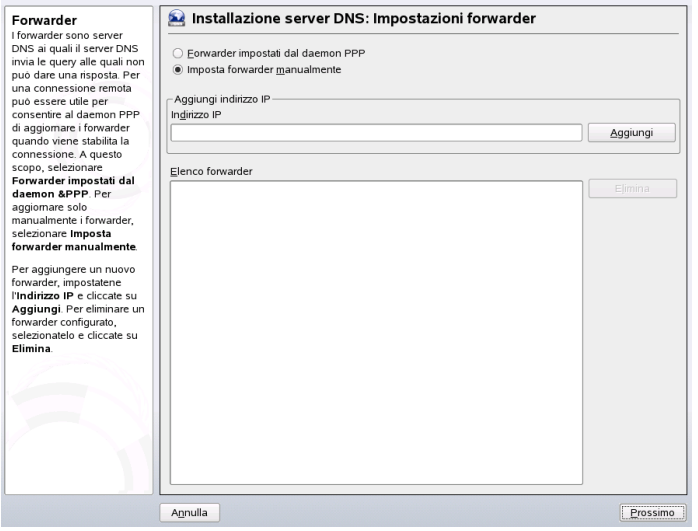
40.2.1 Configurazione guidata (Wizard)

Il wizard si compone di tre parti, che vi permettono di passare nel modo di configurazione per esperti.

Installazione del server DNS: impostazioni forwarder

Al primo avvio del modulo si avrà questa finestra (si veda la Figura 40.1, «Installazione del server DNS: forwarder» (p. 644). Stabilite se volete il demone PPP debba fornire un elenco di forwarder durante il processo di composizione tramite DSL o ISDN (*PPP Daemon stabilisce i forwarder*) o se preferite di eseguire l'immissione voi stessi (*Stabilire forwarder manualmente*).

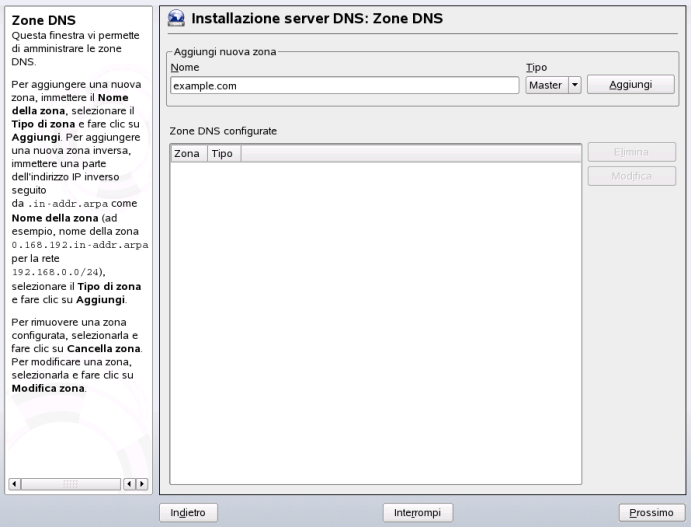
Figura 40.1 *Installazione del server DNS: forwarder*



Installazione del server DNS: zone DNS

Le registrazioni di questo modulo vengono spiegate nel modo di installazione da esperti (si veda la Sezione 40.5, «Struttura di un file zona» (p. 658)). Per una nuova zona va impostato un nome in *Nome zona*. Per aggiungere una zona inversa, il nome deve terminare in `.in-addr.arpa`. Selezionate infine il *Tipo di zona* (master o slave). Si veda la Figura 40.2, «Installazione del server DNS: zone DNS» (p. 645). Cliccate su *Modifica zona* per configurare altre impostazioni di una data zona. Per cancellare una zona cliccate su *Elimina zona*.

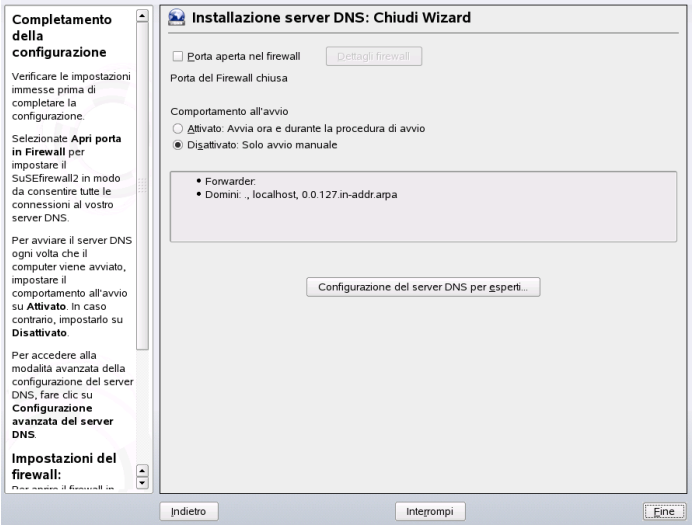
Figura 40.2 *Installazione del server DNS: zone DNS*



Installazione del server DNS: chiudere il wizard

Visto che durante l'installazione viene abilitato un firewall, potete aprire la porta DNS nel firewall (Porta `53`) con *Apri porta nel firewall* impostare il comportamento di avviamento del server DNS (*On* o *Off*). Si veda la Figura 40.3, «Installazione del server DNS: chiudere il wizard» (p. 646).

Figura 40.3 *Installazione del server DNS: chiudere il wizard*



40.2.2 Configurazione da esperti

Al primo avvio del modulo, YaST visualizza una finestra con diverse possibilità di configurazione. In seguito, il server DNS è in linea di massima pronto ad essere utilizzato:

Server DNS: avvio
Sotto *Avvio del sistema* è possibile scegliere se avviare il server DNS all'avvio del sistema o manualmente. Tramite il bottone *Avviare il server DNS ora* potete avviare il server DNS immediatamente e fermarlo tramite *Fermare server DNS ora*; salvare le impostazioni attuali vi è *Salva impostazioni e riavvia il server DNS ora*. Potete anche aprire la porta DNS (*Apri porta nel firewall*) e tramite *Dettagli firewall* intervenire in modo mirato sulle impostazioni del firewall.

Server DNS: forwarder
Questa finestra è identica a quella che ottenete all'avvio del configurazione guidata wizard (si veda Installazione del server DNS: impostazioni forwarder (p. 644)).

Server DNS: file di protocollo
Qui stabilite cosa e dove il server DNS debba protocollare.

Sotto *Tipo di protocollo* specificate dove il server DNS debba protocollare i suoi messaggi. Potete lasciare mano libera al sistema (*Protocollare nel protocollo di sistema* in `/var/log/messages`) oppure indicare esplicitamente un file (*Protocollare nel file*). In quest'ultimo caso, potete indicare anche la dimensione massima del file in megabyte ed il numero dei file di protocollo.

Sotto *Protocollare in aggiunta* potete impostare ulteriori opzioni. Con *Registra tutte le query DNS* verrà protocollata *ogni* richiesta. Il file di protocollo raggiungere una notevole dimensione. Questa opzione si dovrebbe abilitare solo per eseguire il debug. Per eseguire un aggiornamento delle zone sul server DHCP e server DNS, selezionate *Protocollare aggiornamento delle zone*. Per protocollare il traffico di dati durante il transfer dei dati zone (transfer delle zone) dal master allo slave abilitate l'opzione *Protocollare transfer di zone* (si veda la Figura 40.4, «Server DNS: attività di log» (p. 647)).

Figura 40.4 *Server DNS: attività di log*

Server DNS: zone DNS

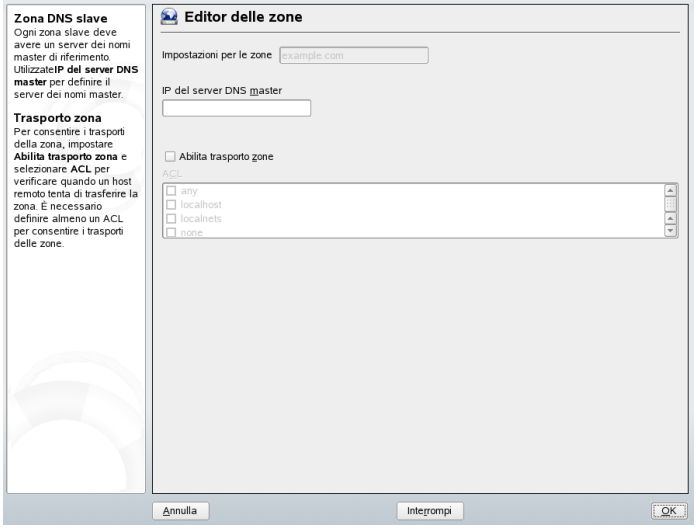
Questa sezione è suddivisa in diverse finestre e tramite essa vengono amministrati i file zona (si veda la Sezione 40.2.1, «Configurazione guidata (Wizard)» (p. 643).

Server DNS: editor delle zone slave

Arrivate a questa finestra se sotto Server DNS: zone DNS (p. 647) avete selezionato *Slave* come tipo zona. Sotto *Server DNS master* indicate il server master a cui debba

rivolgersi lo slave. Se intendete restringere l'accesso, potete selezionare le ACL definite in precedenza dall'elenco (si veda la Figura 40.5, «Server DNS: editor delle zone slave» (p. 648)).

Figura 40.5 *Server DNS: editor delle zone slave*



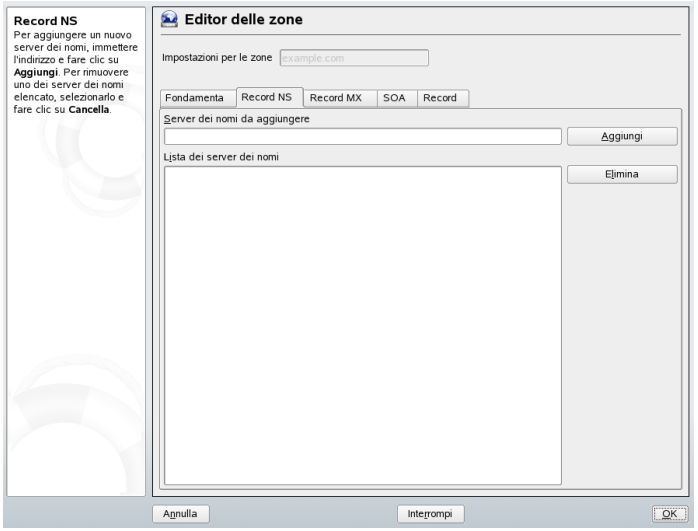
Server DNS: editor delle zone master

Arrivate a questa finestra se sotto Server DNS: zone DNS (p. 647) avete selezionato come tipo di zona *Master*. Potete visualizzare: Le *basi* (la pagina attualmente visualizzata), *Registrazioni NS*, *Registrazioni MX*, *SOA* e *Registrazioni*. Segue una breve illustrazione.

Server DNS: editor delle zone (registrazioni NS)

Qui potete stabilire dei server dei nomi alternativi per queste zone. Dovete badare al fatto che il proprio server dei nomi sia contenuto nell'elenco. Per aggiungere una nuova registrazione, indicate sotto *Server dei nomi da aggiungere* il rispettivo nome e confermate con *Aggiungi* (si veda la Figura 40.6, «Server DNS: editor delle zone (registrazioni NS)» (p. 649)).

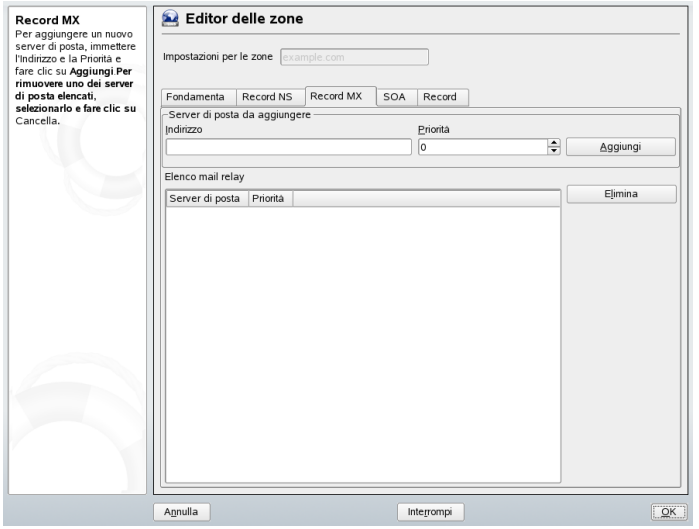
Figura 40.6 *Server DNS: editor delle zone (registrazioni NS)*



Server DNS: editor delle zone (registrazioni MX)

Per aggiungere un nuovo server di posta per la zona attuale all'elenco esistente, indicate il rispettivo indirizzo e la priorità. Confermate con *Aggiungi* (si veda la Figura 40.7, «Server DNS: editor delle zone (registrazioni MX)» (p. 650)).

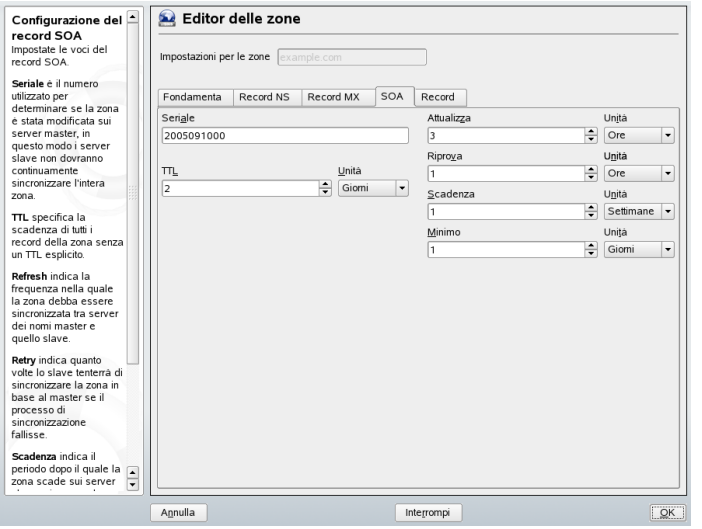
Figura 40.7 *Server DNS: editor delle zone (registrazioni MX)*



Server DNS: editor delle zone (SOA)

Tramite SOA Record Configuration (si veda la Figura 40.8, «Server DNS: editor delle zone (SOA)» (p. 651)) si generano registrazioni SOA (*Start of Authority*). Il significato delle singole opzioni può essere evinto dall'Esempio 40.6, «File /var/lib/named/mondo.zone» (p. 658).

Figura 40.8 *Server DNS: editor delle zone (SOA)*



Server DNS: editor delle zone (Registrazioni)

Questa finestra amministra un elenco di coppie nomi e indirizzi IP. Nel campo di immissione sotto *Chiave della registrazione* inserite il nome dell'host e selezionate il tipo (menu a tendina omonimo). *A-Record* è la registrazione principale; *CNAME* è un alias. Usate i tipi *NS* e *MX* per registrazioni dettagliati o parziali che si basano sulle informazioni fornite in *Recordi NS* e *Record MX* . Vi sono tra modi di risolvere una record A esistente. *PTR* per le zone inverse è il contrario di una record A.

40.3 Inizializzare il server dei nomi BIND

In SUSE Linux, il server dei nomi BIND (*Berkeley Internet Name Domain*) è già preconfigurato in modo da poter essere avviato subito dopo l'installazione. Se siete già collegati ad Internet ed immettete in `/etc/resolv.conf` l'indirizzo `127.0.0.1` come server dei nomi per `localhost` avrete solitamente già una risoluzione dei nomi correttamente funzionante, senza dover conoscere il DNS del provider. BIND eseguirà la risoluzione dei nomi tramite i server dei nomi root – cosa che però richiede un pò di tempo. Per ottenere una risoluzione del nome sicura ed effettiva, immettete nel file di configurazione `/etc/named.conf`, sotto `forwarders`, il DNS del provider con

indirizzo IP. Se tutto è andato per il verso giusto, il server dei nomi girerà nella modalità «caching-only». Solo dopo l'impostazione delle zone diventa un DNS a tutti gli effetti. Un esempio a riguardo è reperibile nella directory di documentazione `/usr/share/doc/packages/bind/sample-config`.

SUGGERIMENTO: Adattamenti automatici dell'allocazione dei nomi

A secondo del tipo di accesso ad Internet o ambiente di rete dato, l'allocazione dei nomi può essere adatta alla situazione attuale. A tal fine impostate la variabile `MODIFY_NAMED_CONF_DYNAMICALLY` nel file `/etc/sysconfig/network/config` su `yes`.

Non si dovrebbe impostare un dominio ufficiale, finché l'autorità competente – per `.it` si tratta dell' ITNIC non ve ne assegni uno. Anche se avete un dominio personale, amministrato da un provider, non conviene utilizzarlo, dato che BIND non inoltrerebbe richieste indirizzate a questo dominio, e il server Web del provider risulterebbe irraggiungibile per il proprio dominio.

Per avviare il server dei nomi, si immette come `root` di comando `rcnamed start`. Se sulla destra appare in verde «done», `named`, così si chiama il processo del server dei nomi, è stato inizializzato correttamente. Sul sistema locale si potrà subito verificare se il server dei nomi funziona nel modo dovuto tramite i programmi `host` oppure `dig`. Come server di default deve venire indicato `localhost` con l'indirizzo `127.0.0.1`. Altrimenti in `/etc/resolv.conf` si trova probabilmente un server dei nomi sbagliato, o questo file non esiste. Per un primo test, inserite `host 127.0.0.1`; questo dovrebbe funzionare in ogni caso. Se invece ricevete una comunicazione di errore, controllate, con il seguente comando, se il `named` è in esecuzione con `rcnamed status`. Se il server dei nomi non parte o mostra qualche disfunzione, il motivo viene protocollato nella maggioranza dei casi sotto `/var/log/messages`.

Per usare come «forwarder» il server dei nomi del provider oppure un server dei nomi che gira all'interno della propria rete, bisogna registrarlo o registrarli nella sezione `options` sotto `forwarders`. Gli indirizzi IP utilizzati nel file Esempio 40.1, «Opzioni di forwarding in named.conf» (p. 653) sono stati scelti a caso, dovrete adattarli in base ai vostri dati effettivi.

Esempio 40.1 *Opzioni di forwarding in named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.0.99; };
        allow-query { 127/8; 192.168.0/24; };
        notify no;
        };
```

Dopo `options`, seguono le registrazioni per le zone, `localhost`, `0.0.127.in-addr.arpa` e il «.» di «type hint» che dovrebbero essere presenti in ogni caso. I file corrispondenti non dovranno essere modificati, dal momento che funzionano benissimo così come sono. Non dimenticate di porre un «;» alla fine di ogni riga e di digitare correttamente le parentesi graffe. Dopo aver apportato delle modifiche al file di configurazione `/etc/named.conf` o ai file zona, BIND dovrà rileggerle, immettete dunque il comando `rcnamed reload`. Alternativamente, riavviate il server dei nomi con il comando `rcnamed restart`. E per terminare il server dei nomi, usate `rcnamed stop`.

40.4 Il file di configurazione /etc/named.conf

Tutte le impostazioni riguardanti il server dei nomi BIND devono venire eseguite nel file `/etc/named.conf`. Anche i dati delle zone, cioè i nomi degli host, gli indirizzi IP, etc. per i domini da amministrare, devono venire archiviati in file separati nella directory `/var/lib/named`. Trattateremo questo tema più avanti.

L' `/etc/named.conf` si suddivide grosso modo in due settori: una sezione `options` per le impostazioni generali ed una per le registrazioni `zone` per i singoli domini. Inoltre è anche possibile definire un'area `logging`, come pure registrazioni del tipo `acl` (ingl.Access Control List). Le righe di commento iniziano con il carattere `#`, alternativamente è permesso anche `//`. Il file Esempio 40.2, «File /etc/named.conf di base» (p. 654) vi mostra un esempio di un `/etc/named.conf` minimale.

Esempio 40.2 *File /etc/named.conf di base*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

40.4.1 Le opzioni di configurazione principali

directory "*nomefile*";
indica la directory in cui BIND trova i file con i dati delle zone, di solito `/var/lib/named`.

forwarders { *indirizzo ip*; };
viene usato per indicare uno o più server dei nomi (nella maggioranza dei casi quelli del provider) ai quali vengono inoltrate le richieste DNS a cui non è possibile rispondere direttamente. Al posto di *`indirizzo ip`* utilizzato un indirizzo IP del tipo `10.0.0.1`.

forward first;
fa in modo che le richieste DNS vengano inoltrate `forwarded`, prima che si cercare di risolverle tramite i server dei nomi root. Invece di `forward first` è anche possibile scrivere `forward only`; in questo caso, tutte le richieste vengono inoltrate ed i server dei nomi root non vengono più indirizzati. Può essere conveniente in configurazioni firewall.

listen-on port 53 {127.0.0.1; *indirizzo ip*; };

comunica a BIND, su quali interfacce di rete e su quale porta mettersi in ascolto di eventuali richieste dei client. L'indicazione `port 53` può venire omessa, poiché `53` è la porta standard. Con `127.0.0.1` si ammettono richieste di localhost. Omettendo completamente questa registrazione, vengono usate di default tutte le interfacce.

listen-on-v6 port 53 { any; };
indica a BIND su quale porta mettersi in ascolto di richieste da parte di client che utilizzano IPv6. Oltre a `any` è consentito come alternativa solo `none`, dato che il server si mette in ascolto sull'indirizzo wildcard IPv6.

query-source address * port 53;
questa registrazione è necessaria se il firewall blocca richieste DNS esterne. In questo modo BIND viene indotto ad inviare delle richieste verso l'esterno dalla porta 53 e non dalle porte con un numero elevato (> 1024).

query-source-v6 address * port 53;
qui si indica a BIND quale porta utilizzare per richieste IPv6.

allow-query {127.0.0.1; *net*; };
definisce le reti da cui i client possono inviare delle richieste DNS. Al posto di *net* si immettete un indirizzo del tipo `192.168.1/24`; laddove `/24` è un'abbreviazione per la maschera di rete, in questo caso `255.255.255.0`.

allow-transfer {! *; };
regola quali sistemi possano richiedere il trasferimento delle zone; in questo esempio ciò viene completamente impedito da `! *`. Senza questa registrazione, il trasferimento delle zone può venire richiesto da ovunque.

statistics-interval 0;
senza questa registrazione, BIND archivia ogni ora diverse righe di messaggi di natura statistica in `/var/log/messages`. Il valore 0 determina che questi messaggi vengano completamente soppressi; l'intervallo viene indicato in minuti.

cleaning-interval 720;
questa opzione stabilisce l'intervallo di tempo, scaduto il quale BIND svuota la sua cache. Ogni volta questa attività genera una registrazione in `/var/log/messages`. L'indicazione del tempo avviene in minuti: sono preconfigurati 60 minuti.

interface-interval 0;
BIND verifica regolarmente se vi sono delle nuove interfacce di rete o se ne sono state rimosse alcune. Se questo valore è impostato su `0`, si rinuncia a tale verifica, e BIND si mette in ascolto solo sulle interfacce rilevate all'avvio. Si può indicare questo l'intervallo in minuti. 60 minuti è il valore preconfigurato.

notify no;
Con `no` non viene avvisato nessun altro server dei nomi nel caso si siano apportate delle modifiche ai dati delle zone o se il server dei nomi viene riavviato.

40.4.2 Attività di logging

BIND permette di configurare in modo flessibile l'attività di logging. Normalmente, le preimpostazioni dovrebbero rilevarsi sufficienti. Il file Esempio 40.3, «Il logging viene soppresso» (p. 656) vi mostra la variante più semplice di una tale registrazione, e sopprime completamente il «logging»:

Esempio 40.3 *Il logging viene soppresso*

```
logging {
        category default { null; };
};
```

40.4.3 Struttura delle registrazioni delle zone

Esempio 40.4 *L'indicazione zone per mio-dominio.it*

```
zone "mio-dominio.it" in {
       type master;
       file "mio-dominio.zone";
       notify no;
};
```

Dopo `zone` si indica il nome del dominio da amministrare, nel nostro esempio abbiamo scelto un nome a caso `mio-dominio.it` seguito da un `in` ed un blocco compreso tra parentesi graffe con le relative opzioni; cfr. Esempio 40.4, «L'indicazione zone per mio-dominio.it» (p. 656). Se si desidera definire una *zona slave*, cambia solo il `type` che diventa `slave`, e si deve indicare il server dei nomi che amministra questa zona

come `master` (può, a sua volta essere uno «slave»); si veda l'Esempio 40.5, «L'indicazione zone per altro-dominio.it» (p. 657).

Esempio 40.5 *L'indicazione zone per altro-dominio.it*

```
zone "altro-dominio.it" in {
      type slave;
        file "slave/altro-dominio.zone";
        masters { 10.0.0.1; };
};
```

Le opzioni di zone:

type master;
`master` stabilisce che questa zona venga amministrata su questo server di nome. Premessa per questa opzione: un file di zone corretto.

type slave;
Questa zona viene trasferita da un altro server dei nomi. Deve venire usata assieme a `masters`.

type hint;
La zona `.` del tipo `hint` viene impiegata per l'indicazione dei server dei nomi root. Questa definizione di zona può rimanere invariata.

file `mio-dominio.zone` o file «slave/altro-dominio.zone»;
Questa registrazione indica il file in cui sono registrati i dati delle zone per il dominio. Con uno slave, il file non è necessario, poiché il suo contenuto viene preso da un altro server dei nomi. Per distinguere fra file master e file slave, si indica la directory `slave` per i file slave.

masters {*`indirizzo_ip_server`*; };
Questa impostazione è necessaria solo per zone slave ed indica da quale server dei nomi debba venire trasferito il file delle zone.

allow-update {! *; };
Questa opzione regola l'accesso in scrittura ai dati delle zone dall'esterno. Se l'accesso fosse indiscriminato, ogni client potrebbe registrarsi nel DNS del tutto autonomamente, cosa non auspicabile da un punto di vista della sicurezza. Senza questa opzione, non sono permessi gli aggiornamenti delle zone. La registrazione riportata nell'esempio non cambierebbe nulla, dal momento che la definizione `! *` proibisce, anch'essa, ogni accesso.

40.5 Struttura di un file zona

Servono due tipi di file zona: uno per attribuire un indirizzo IP al nome di un host e l'altro per fare l'esatto contrario, cioè allocare un nome host ad un determinato indirizzo IP.

SUGGERIMENTO: Il punto (.) nei file zona

D'importanza fondamentale è il `.` nei file zona. A nomi di host senza il punto finale viene sempre aggiunta automaticamente la zona. E' quindi necessario porre un `.` alla fine di nomi completi, già provvisti di dominio completo, per evitare che il dominio venga aggiunto una seconda volta. La mancanza di questo punto alla fine o la sua posizione errata sono sicuramente gli errori più comuni nella configurazione di server dei nomi.

Osserviamo ora il file zona `mondo.zone` responsabile per il dominio Domain `mondo.all` mostrato nell'Esempio 40.6, «File /var/lib/named/mondo.zone» (p. 658).

Esempio 40.6 *File /var/lib/named/mondo.zone*

```
$TTL 2D
mondo.all IN SOA      gateway  root.mondo.all.(
              2003072441  ; serial
              1D          ; refresh
              2H          ; retry
              1W          ; expiry
              2D )        ; minimum

             IN NS       gateway
             IN MX       10 sole

 gateway     IN A        192.168.0.1
             IN A        192.168.1.1
 sole        IN A        192.168.0.2
 luna        IN A        192.168.0.3
 terra       IN A        192.168.1.2
 marte       IN A        192.168.1.3
 www         IN CNAME    luna
```

Rigo 1:

`$TTL` definisce il TTL standard (ingl. Time To Live), ovvero la scandenza valida per l'intero contenuto di questo file: due giorni, in questo caso `2D`= 2 days)..

Rigo 2:

Ha inizio qui il `SOA control record` (SOA = Start of Authority):

- Al primo posto vi è il nome del dominio da amministrare `mondo.all`, con un `.` alla fine, per evitare che venga aggiunta la zona una seconda volta. Alternativamente, si può digitare una chiocciola `@`, in questo caso la zona viene evinta dalla rispettiva registrazione in `/etc/named.conf`.

- Dopo l'`IN SOA`, abbiamo il nome del server dei nomi, responsabile per questa zona in funzione di master. In questo caso, il nome `gateway`, diventa automaticamente `gateway.mondo.all`, perché non seguito da un `.`.

- Segue l'indirizzo e-mail della persona responsabile per il server dei nomi. Dal momento che la chiocciola `@` possiede già un significato particolare, si aggiungerà semplicemente un `.`, di modo che, al posto di `root@mondo.all` avremo `root.mondo.all.`; non dimenticate il punto alla fine, altrimenti viene aggiunta la zona una seconda volta.

- Alla fine abbiamo una `(`, per includere i righi seguenti fino alla seconda `)` nella istruzione SOA.

Rigo 3:

Il `numero di serie` è una cifra arbitraria, da aumentare ogni volta che si modifica questo file. Questa cifra serve ad informare server dei nomi secondari (server slave) che sono state effettuate delle modifiche. Di solito, si usa un numero di dieci cifre composto da una data e da un numero progressivo, nella forma `AAAAMMGGNN`.

Rigo 4:

Il `refresh rate` indica l'intervallo di tempo trascorso il quale i server dei nomi secondari verificano il `numero di serie` della zona. In questo caso, si ha 1 giorno (1D = 1 day).

Rigo 5:

Il `retry rate` indica l'intervallo di tempo trascorso il quale un name server secondario, in caso di errore, cerca di ristabilire il contatto con il server primario. In questo caso, due ore (2H = 2 hours).

Rigo 6:

L'`expiration time` indica quanto tempo debba passare prima che il server dei nomi secondario espelli i dati dalla cache, se non riesce a ristabilire il contatto con il server primario. In questo caso, una settimana (1W = 1 week).

Rigo 7:

Con `negative caching TTL` si conclude l'SOA, che indica per quanto tempo i risultati delle richieste DNS di altri server irrisolte debbano restare nella cache.

Rigo 9:

L'`IN NS` indica il server dei nomi responsabile per questo dominio. Anche in questo caso, `gateway` diventa automaticamente `gateway.mondo.all`, poiché non vi è un `.` alla fine. Vi possono essere diverse righe del genere: una per il server dei nomi primario e una per ogni server dei nomi secondario. Se per questa zona `notify` in `/etc/named.conf` non è impostato su `no`, verranno informati tutti i server dei nomi qui elencati delle modifiche apportate ai dati delle zone.

Rigo 10:

La registrazione MX indica il server di posta che accetta le e-mail per il dominio `mondo.all`, per poi elaborarle o inoltrarle. In quest'esempio, si tratta dell'host `sole.mondo.all`. Il numero davanti al server dei nomi è il valore di preferenza: se vi sono più indicazioni MX, si prenderà per primo il server di posta con il valore minore; se la consegna a questo server fallisce, si prova con il prossimo valore.

Righe 12-17:

Le registrazioni degli indirizzi (ingl. Address Records), dove il nome dell'host viene attribuito ad uno o più indirizzi IP. In questo caso, i nomi vengono riportati senza un punto alla fine, dal momento che sono registrati senza il relativo dominio e che in questo caso è possibile aggiungere a tutti `mondo.all`. A `gateway` sono stati attribuiti due indirizzi IP, dacché dispone di due schede di rete. `A` sta per un indirizzo host tradizionale; con `A6` si immettono indirizzi IPv6 e `AAAA` è il formato ormai superato per indirizzi IPv6.

Rigo 18:

Impostare un alias per `www`, p.es `luna` (`CNAME` = *canonical name* ovvero nome canonico).

Per la risoluzione inversa (ingl. reverse lookup) degli indirizzi IP in nomi di host si ricorre allo pseudo-dominio `in-addr.arpa` che viene aggiunto all'indirizzo scritto

alla rovescia. Quindi, `192.168.1` diventa `1.168.192.in-addr.arpa`. Si veda l'Esempio 40.7, «Risoluzione inversa dell'indirizzo» (p. 661).

Esempio 40.7 *Risoluzione inversa dell'indirizzo*

```
 $TTL 2D
 1.168.192.in-addr.arpa. IN SOA gateway.mondo.all. root.mondo.all. (
                         2003072441     ; serial
                         1D              ; refresh
                         2H              ; retry
                         1W              ; expiry
                         2D )            ; minimum

                         IN NS           gateway.mondo.all.

1                      IN PTR          gateway.mondo.all.
2                      IN PTR          terra.mondo.all.
3                      IN PTR          marte.mondo.all.
```

Rigo 1:
$TTL definisce il TTL di default valido per tutte le voci.

Rigo 2:
Questo file permette il «reverse lookup» per la rete `192.168.1.0`. Dal momento che la zona del caso è `1.168.192.in-addr.arpa` , non la si vorrà aggiungere al nome del server: per questo motivo, i nomi sono tutti completi di dominio e punto finale. Il resto corrisponde all'esempio dato per `mondo.all`.

Righe 3-7:
si veda l'esempio di `mondo.all`.

Rigo 9:
Questa riga indica nuovamente il server dei nomi responsabile per questa zona. Questa volta, però, il nome viene riportato completo di dominio e punto finale.

Righe 11-13:
Le registrazioni pointer (puntatore) puntano sull' indirizzo IP del relativo host. All'inizio della riga trovate solo la parte finale dell'indirizzo, senza `.` finale. Se ora aggiungete la zona e togliete `.in-addr.arpa`, avrete l'indirizzo IP completo, scritto alla rovescia.

Il trasferimento di zone tra le diverse versioni di BIND di solito non dovrebbe creare dei problemi.

40.6 Aggiornamento dinamico dei dati di zona

Con aggiornamento dinamico (ingl. dynamic update) si intende l'aggiunta, la modifica e l'eliminazione di registrazioni nei dati zona di un master. Questo meccanismo viene descritto nell'RFC 2136. L'aggiornamento dinamico delle zone si configura tramite le opzioni `allow-update` o `update-policy` nelle registrazioni delle zone. Le zone che vengono aggiornate dinamicamente non dovrebbero venir impostate manualmente.

Con `nsupdate` le registrazioni da aggiornare vengono trasmesse al server; per la corretta sintassi si veda la pagina di manuale di nsupdate (`man 8 nsupdate`). L'aggiornamento deve avvenire assolutamente, per motivi di sicurezza, tramite transazioni sicure (TSIG); cfr. la Sezione 40.7, «Transazioni sicure» (p. 662).

40.7 Transazioni sicure

Grazie alle «Transaction SIGnatures» (TSIG) si realizza una transazione sicura. Vengono utilizzate delle chiavi di transazione (ingl. transaction keys) e firme di transazione (ingl. transaction signatures). Nella seguente sezione spiegheremo come generarle ed utilizzarle.

Una transazione sicura è richiesta per la comunicazione tra server e l'aggiornamento dinamico dei dati di zona. Il controllo degli accessi basato su chiave offre maggior sicurezza rispetto ad un controllo basato sugli indirizzi IP.

Con il seguente comando potete generare una chiave di transazione (per avere ulteriori informazioni si veda la pagina di manuale `man dnssec-keygen`):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Il risultato sono due file che per esempio portano il seguente nome:

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

La chiave è contenuta in entrambi i file (p.es. `ejIkuCyyGJwwuN3xAteKgg==`). In seguito `Khost1-host2.+157+34265.key` dovrebbe venir copiato in modo sicuro (p.es. con `scp`) su host remoti e lì essere inserito in `/etc/named.conf` per realizzare una comunicazione sicura tra `host1` e `host2`:

```
key host1-host2. {
 algorithm hmac-md5;
 secret ";ejIkuCyyGJwwuN3xAteKgg==;
};
```

AVVERTIMENTO: Permessi di accesso di `/etc/named.conf`

Assicuratevi che i permessi di accesso per `/etc/named.conf` rimangono limitati; il valore di default è `0640` per `root` ed il gruppo `named`; alternativamente potete archiviare la chiave in un file protetto ed includerlo in seguito.

Affinché sul server `host1` venga utilizzata la chiave per `host2` con l'indirizzo esempio `192.168.2.3` il file `/etc/named.conf` sul server deve contenere:

```
server 192.168.2.3 {
  keys { host1-host2. ;};
};
```

Il file di configurazione di `host2` deve essere adattato di conseguenza.

Oltre alle ACL che si basano sugli indirizzi IP e area degli indirizzi si dovrebbero aggiungere delle chiavi TSIG per avere delle transazioni sicure; ecco un esempio:

```
allow-update { key host1-host2. ;};
```

Per ulteriori informazioni consultate nel manuale di amministrazione di BIND (*BIND Administrator Reference Manual*) la parte intitolata `update-policy`.

40.8 DNSSEC

DNSSEC (DNS Security) viene illustrato nell'RFC 2535; gli strumenti disponibili per l'utilizzo di DNSSEC sono descritti nella manuale di BIND.

Una zona per dirsi sicura deve avere una o più chiavi zona; questo tipo di chiave viene generato - come nel caso di chiavi per host - con `dnssec-keygen`. Ai fini della cifratura al momento si usa DSA. Le chiavi pubbliche (public keys) dovrebbero essere integrate nei file zona con `$INCLUDE`.

Tutte le chiavi possono essere riunite in un set di chiavi tramite `dnssec-makekeyset` da trasmettere in modo sicuro alla zona superiore (parent zone), per essere firmati con

`dnssec-signkey`. I file creati durante questo processo, vanno utilizzati ai fini della firma delle zone assieme a `dnssec-signzone` e i file generati da questo processo vanno quindi integrati in `/etc/named.conf` nella zona corrispondente.

40.9 Ulteriori informazioni

Rimandiamo al *BIND Administrator Reference Manual* che trovate sotto `/usr/share/doc/packages/bind/`; segnaliamo inoltre gli RFC ricordati enl manuale e le pagine di manuale di BIND. `/usr/share/doc/packages/bind/README.SuSE` offre delle informazioni aggiornate su BIND in SUSE Linux.

41 Uso di NIS

Quando più sistemi UNIX in una rete richiedono l'accesso a risorse comuni, è essenziale che tutte le identità di utenti e gruppi siano le stesse per tutti i computer nella rete. L'accesso alla rete deve essere trasparente agli utenti, in modo che si trovino sempre esattamente nello stesso ambiente indipendentemente dai computer utilizzati. Questa configurazione è resa possibile dai servizi NIS e NFS. NFS consente la distribuzione dei file system in una rete e viene descritto nel Capitolo 42, *Condivisione di file system con NFS* (p. 673).

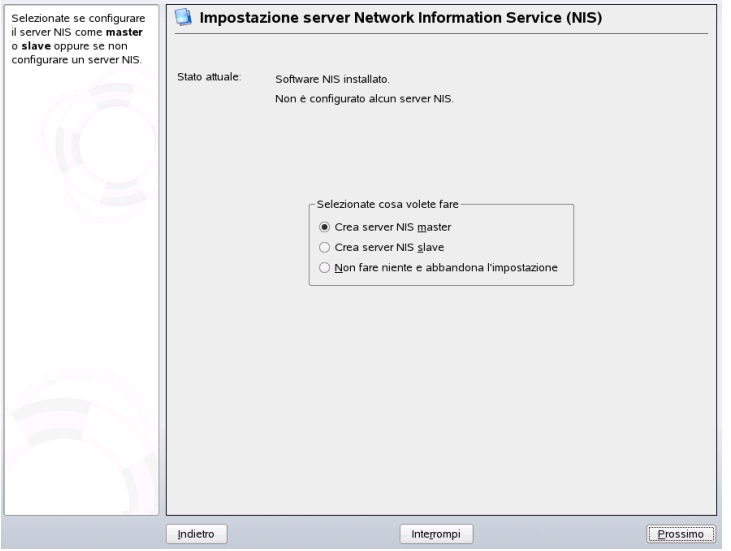
NIS (Network Information Service) può essere descritto come un servizio di tipo database che offre l'accesso al contenuto di `/etc/passwd`, `/etc/shadow` e `/etc/group` attraverso più reti. NIS può inoltre essere utilizzato per altri scopi, ad esempio per rendere disponibile il contenuto di file come `/etc/hosts` o `/etc/services`, tuttavia questo aspetto non rientra nell'ambito di questa introduzione. NIS viene spesso definito *YP (Yellow Pages)* in quanto funziona come le pagine gialle «»della rete.

41.1 Configurazione di un server NIS con YaST

Per la configurazione selezionare *Server NIS* dal modulo YaST *Servizi di rete*. Se nella rete non è ancora presente un server NIS, selezionare *Installa e imposta un server NIS master* nella schermata successiva. I pacchetti necessari verranno installati immediatamente da YaST.

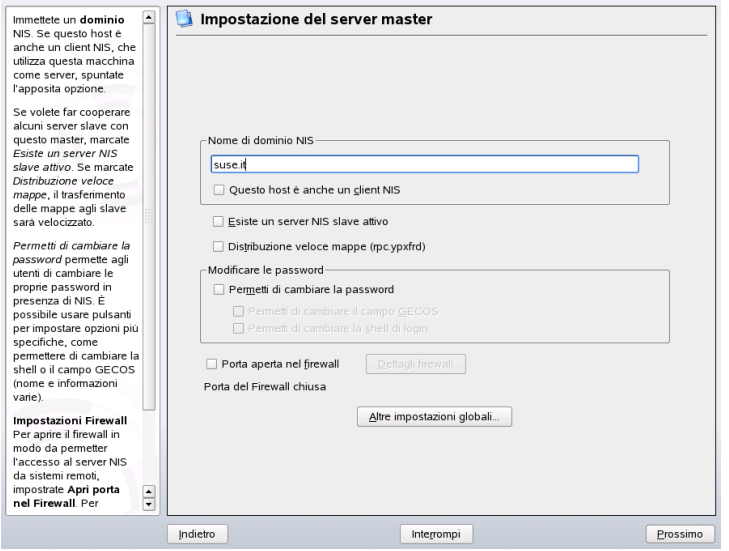
Se il software per NIS è già stato installato, fare clic su *Crea server NIS master*. Se nella rete è già disponibile un server NIS (*master*), è possibile aggiungere un server slave NIS, ad esempio se si desidera configurare una nuova sottorete. Viene innanzitutto descritta la configurazione del server master. Se si fa clic su *Non fare niente e abbandona l'impostazione*, si torna al centro controllo YaST senza salvare le modifiche.

Figura 41.1 *Configurazione del server NIS.*



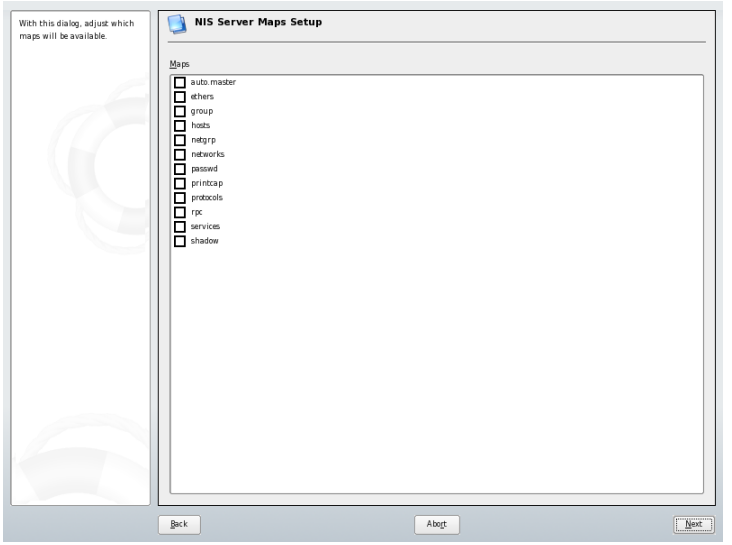
Dopo aver installato tutti i pacchetti, immettere il nome di dominio NIS nella parte superiore della finestra di dialogo di configurazione illustrata nella Figura 41.1, «Configurazione del server NIS.» (p. 666). Tramite la casella di controllo definire se l'host dovrà essere anche un client NIS, in modo da consentire agli utenti di eseguire il login e accedere ai dati dal server NIS. Selezionare le caselle delle opzioni che si desidera applicare, inclusa l'opzione *Modificare le password*. Per la configurazione di ulteriori opzioni, fare clic su *Altre impostazioni globali*. Viene visualizzata una schermata nella quale è possibile cambiare la directory di origine, fondere le password e impostare gli ID utente e di gruppo minimi. Fare clic su *OK* per tornare alla finestra di dialogo principale. Fare clic su *Avanti* per continuare la configurazione.

Figura 41.2 *Configurazione del server master.*



Nella schermata successiva specificare quali mappe dovranno essere disponibili. Se si fa clic su *Avanti*, viene visualizzata la schermata successiva nella quale è possibile determinare a quali host è consentito inviare query al server NIS. Gli host possono essere aggiunti, eliminati e modificati. Per salvare le modifiche e chiudere la finestra di dialogo di configurazione, fare clic su *Fine*.

Figura 41.3 *Configurazione delle mappe del server NIS.*



Per configurare server NIS aggiuntivi nella rete (*server slave*), selezionare *Installa e imposta un server NIS slave*. Se il software per NIS è già stato installato, fare clic su *Crea server NIS slave*, quindi fare clic su *Avanti* per continuare. Nella schermata successiva immettere il nome di dominio NIS e selezionare le caselle di controllo applicabili.

Per consentire agli utenti della rete, sia locali sia gestiti tramite il server NIS, di cambiare le password sul server NIS mediante il comando `yppasswd`, selezionare l'opzione corrispondente. In questo modo diventano disponibili le opzioni *Permetti di cambiare il campo GECOS* e *Permetti di cambiare la shell di login*. «GECOS» significa che gli utenti possono utilizzare il comando `ypchfn` per modificare anche le impostazioni relative ai nomi e agli indirizzi. «SHELL» consente agli utenti di modificare la relativa shell di default utilizzando il comando `ypchsh`, ad esempio per passare da bash a sh.

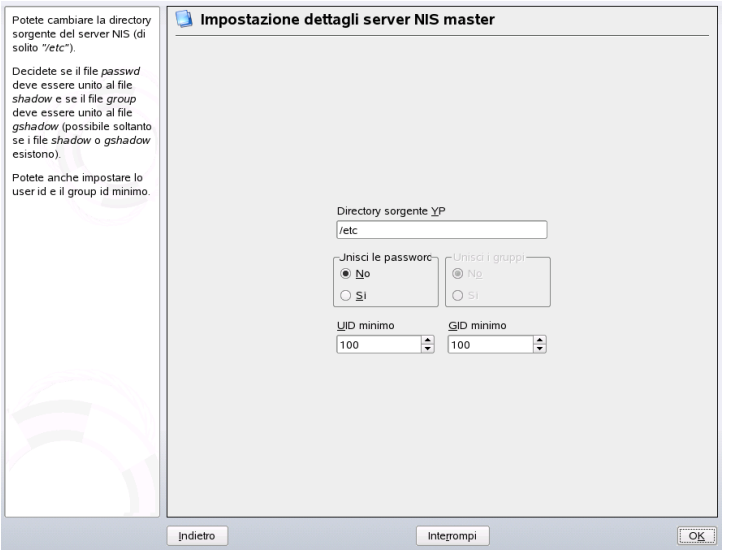
Per impostare ulteriori opzioni, fare clic su *Altre impostazioni globali*. Viene visualizzata la schermata, illustrata nella Figura 41.4, «Cambio di directory e sincronizzazione di file per un server NIS.» (p. 669), nella quale è possibile cambiare la directory di origine del server (di default `/etc`). Sempre in questa schermata è inoltre possibile fondere password e gruppi. Impostare *Sì* per consentire la sincronizzazione dei file `/etc/passwd`, `/etc/shadow` ed `/etc/group`. Determinare inoltre l'ID di gruppo e

utente minimo, quindi fare clic su *OK* per confermare le impostazioni e tornare alla schermata precedente.

Dopo aver definito le impostazioni, fare clic su *Avanti* per passare alla schermata successiva. Nella finestra di dialogo visualizzata selezionare le mappe che saranno disponibili, quindi fare clic su *Avanti* per continuare. Nell'ultima schermata immettere gli host ai quali è consentito inviare query al server NIS. Gli host possono essere aggiunti, modificati o eliminati mediante i pulsanti appropriati. Per salvare le modifiche e uscire dalla configurazione, fare clic su *Fine*.

Fare quindi clic su *Avanti*.

Figura 41.4 *Cambio di directory e sincronizzazione di file per un server NIS.*



Se è stata selezionata l'opzione *Esiste un server NIS slave attivo*, immettere i nomi host utilizzati come slave, quindi fare clic su *Avanti*. Se non si utilizzano server slave, la relativa configurazione viene ignorata e si passa direttamente alla finestra di dialogo per la configurazione del database, nella quale è necessario specificare le *mappe*, ovvero i database parziali da trasferire dal server NIS al client. Le impostazioni di default sono in genere appropriate.

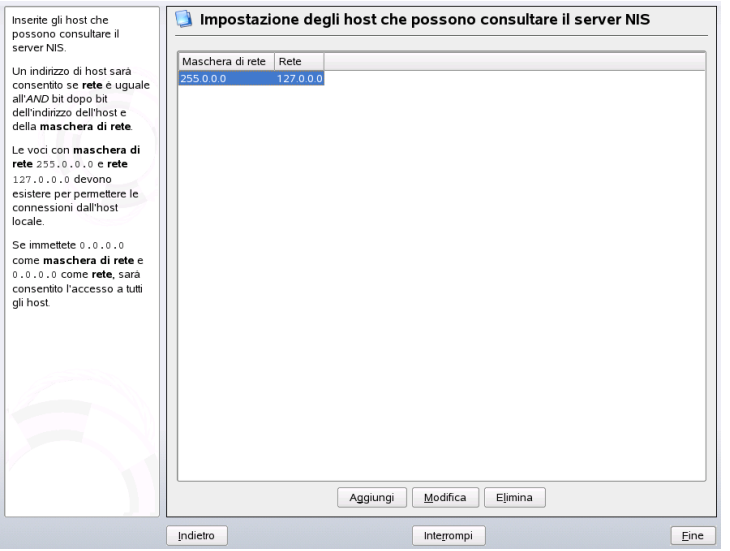
Fare clic su *Avanti* per passare all'ultima finestra di dialogo, illustrata nella Figura 41.5, «Impostazione delle autorizzazioni per le richieste a un server NIS.» (p. 670). Specificare

da quali reti possono essere inviate richieste al server NIS. In genere viene indicata la rete interna. In questo caso dovranno essere presenti le due voci seguenti:

```
255.0.0.0       127.0.0.0
0.0.0.0         0.0.0.0
```

La prima voce abilita le connessioni dall'host che corrisponde al server NIS. La seconda voce consente a tutti gli host che dispongono dell'accesso alla stessa rete di inviare richieste al server.

Figura 41.5 *Impostazione delle autorizzazioni per le richieste a un server NIS.*



IMPORTANTE: configurazione automatica del firewall

Se nel sistema in uso è attivo un firewall (SuSEfirewall2), YaST ne adatta la configurazione per il server NIS mediante l'abilitazione del servizio `portmap` quando è selezionata l'opzione *Porta aperta nel firewall*.

41.2 Configurazione dei client NIS

Utilizzare questo modulo per configurare un client NIS. Dopo aver scelto di utilizzare NIS e l'automounter, in determinate circostanze, viene aperta questa finestra di dialogo.

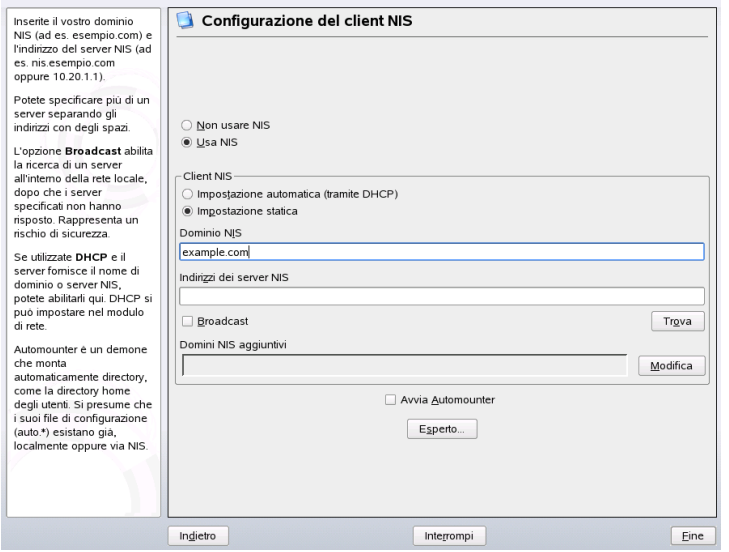
Specificare se l'host dispone di un indirizzo IP statico o se ne riceve uno generato da DHCP. Anche il dominio NIS e il server NIS vengono forniti da DHCP. Per ulteriori informazioni su DHCP, vedere il Capitolo 43, *DHCP* (p. 679). Se viene utilizzato un indirizzo IP statico, specificare manualmente il dominio NIS e il server NIS. Vedere Figura 41.6, «Impostazione del dominio e dell'indirizzo di un server NIS.» (p. 671). *Trova* consente di attivare la ricerca automatica di un server NIS attivo nella rete locale. *Broadcast* abilita la ricerca di un server nella rete locale se i server specificati non rispondono.

È inoltre possibile specificare più server mediante l'immissione dei relativi indirizzi separati da spazi nella casella *Indirizzi dei server NIS*.

Nelle impostazioni avanzate disattivare *Rispondi a host remoti* se si desidera impedire che altri host siano in grado di identificare quale server viene utilizzato dal client. Se si seleziona *Server malfunzionante*, il client viene abilitato a ricevere risposte da un server che comunica attraverso una porta senza privilegi. Per ulteriori informazioni, vedere `man ypbind`.

Dopo aver completato le impostazioni, fare clic su *Fine* per applicare le modifiche e tornare al centro controllo YaST.

Figura 41.6 *Impostazione del dominio e dell'indirizzo di un server NIS.*



42 Condivisione di file system con NFS

Come accennato nel Capitolo 41, *Uso di NIS* (p. 665), NFS interagisce con NIS per creare una rete trasparente per l'utente e consente la distribuzione di file system nella rete. Indipendentemente dal terminale al quale è stato eseguito il login, l'utente potrà sempre accedere allo stesso ambiente.

Come NIS, anche NFS è un servizio asimmetrico con il quale vengono utilizzati server NFS e client NFS. Un computer può essere l'uno e l'altro, distribuire file system in rete (esportazione) e montare file system da altri host (importazione). In genere si tratta di server con una capacità del disco rigido particolarmente elevata i cui file system sono montati da altri client.

IMPORTANTE: esigenza dell'uso del DNS

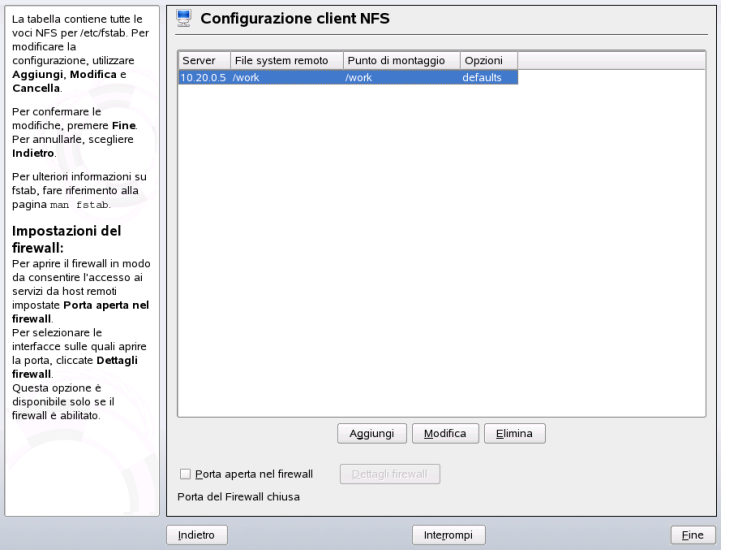
In linea di massima tutte le esportazioni possono essere effettuate solo mediante indirizzi IP. Per evitare timeout, è tuttavia necessario disporre di un sistema DNS funzionante, almeno ai fini della registrazione poiché il daemon mountd esegue ricerche inverse.

42.1 Importazione di file system con YaST

Gli utenti autorizzati possono montare directory NFS da un server NFS negli alberi di file locali. Questa operazione può essere eseguita molto facilmente mediante il modulo YaST *Client NFS* con l'immissione del nome host del server NFS, della directory da

importare e del punto di montaggio locale per la directory. Per eseguire queste operazioni, fare clic su *Aggiungi* nella prima finestra di dialogo. Fare clic su *Porta aperta nel firewall* per aprire il firewall e consentire l'accesso al servizio da computer remoti. Lo stato del firewall viene visualizzato accanto alla casella di controllo. Fare clic su *OK* per salvare le modifiche. Vedere la Figura 42.1, «Configurazione del client NFS con YaST» (p. 674).

Figura 42.1 *Configurazione del client NFS con YaST*



42.2 Importazione manuale di file system

I file system possono essere facilmente importati da un server NFS. Il solo prerequisito è l'esecuzione di un portmapper RPC che può essere avviato mediante il comando `rcportmap start` come `root`. Dopo aver soddisfatto questo prerequisito, i file system remoti esportati sui rispettivi computer possono essere montati nel file system come dischi rigidi locali utilizzando il comando `mount` con la sintassi seguente:

```
mount host:remote-path local-path
```

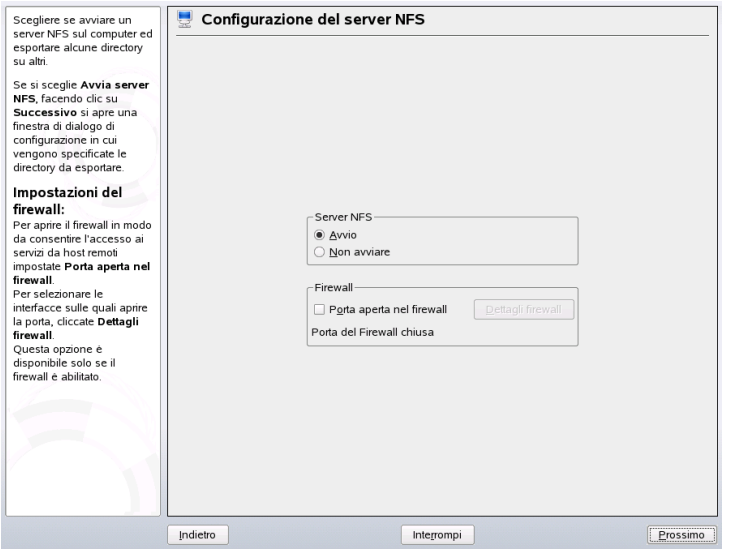
Se è necessario importare, ad esempio, directory utente da un computer Sun, utilizzare il comando seguente:

```
mount sun:/home /home
```

42.3 Esportazione di file system con YaST

Mediante YaST è possibile trasformare un host della rete in un server NFS, ovvero un server in grado di esportare directory e file a tutti gli host autorizzati ad accedervi. Questa configurazione può essere scelta per rendere accessibili applicazioni particolari a tutti i membri di un gruppo senza installarle localmente in ogni singolo host. Per installare un server NFS, avviare YaST e selezionare *Servizi di rete* → *Server NFS*. Viene aperta la finestra di dialogo illustrata nella Figura 42.2, «Strumento di configurazione del server NFS» (p. 675).

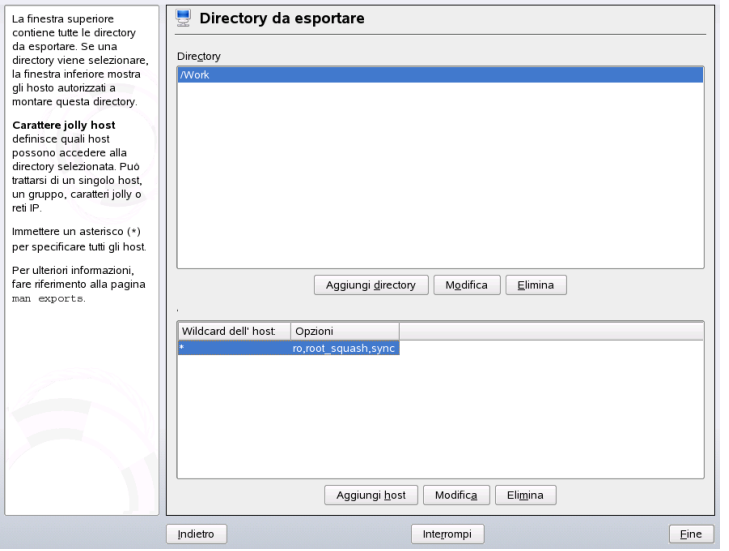
Figura 42.2 *Strumento di configurazione del server NFS*



Selezionare quindi *Avvia server NFS* e scegliere *Avanti*. Nel campo di testo superiore immettere le directory da esportare. Nel campo sottostante immettere gli host che dispongono delle autorizzazioni di accesso alle directory. Questa finestra di dialogo è

illustrata nella Figura 42.3, «Configurazione di un server NFS con YaST» (p. 676). Per ogni host è possibile impostare quattro opzioni: `single host`, `netgroups`, `wildcards` e `IP networks`. Per una spiegazione più dettagliata di queste opzioni, vedere `man exports`. Scegliere *Esci* per completare la configurazione.

Figura 42.3 *Configurazione di un server NFS con YaST*



IMPORTANTE: configurazione automatica del firewall

Se nel sistema in uso è attivo un firewall (SuSEfirewall2), YaST ne adatta la configurazione per il server NFS mediante l'abilitazione del servizio `nfs` quando è selezionata l'opzione *Porta aperta nel firewall*.

42.4 Esportazione manuale di file system

Se non si desidera utilizzare YaST, verificare che i sistemi seguenti siano in esecuzione sul server NFS:

- Portmapper RPC (portmap)

- Daemon di montaggio RPC (rpc.mountd)
- Daemon NFS RPC (rpc.nfsd)

Per consentire l'avvio di questi servizi mediante gli script `/etc/init.d/portmap` e `/etc/init.d/nfsserver` all'avvio del sistema, immettere i comandi `insserv /etc/init.d/nfsserver` e `insserv /etc/init.d/portmap`. Nel file di configurazione `/etc/exports` definire inoltre quali file system dovranno essere esportati e i relativi host di destinazione.

Per ogni directory da esportare è necessario inserire una riga per l'impostazione dei computer a cui è consentito accedere alla directory con determinate autorizzazioni. Vengono esportate automaticamente anche tutte le sottodirectory della directory. I computer autorizzati vengono solitamente specificati con nomi completi (incluso il nome di dominio), tuttavia è possibile utilizzare caratteri jolly, ad esempio `*` o `?` (con la stessa modalità di espansione della shell bash). Se non si specificano computer, l'importazione di questo file system con le autorizzazioni date sarà consentita a qualsiasi computer.

Impostare le autorizzazioni per il file system da esportare racchiudendole tra parentesi dopo il nome del computer. Le opzioni più importanti sono illustrate nella Tabella 42.1, «Autorizzazioni per il file system esportato» (p. 677).

Tabella 42.1 *Autorizzazioni per il file system esportato*

Opzione	Descrizione
`ro`	Il file system viene esportato con l'autorizzazione Sola lettura (default).
`rw`	Il file system viene esportato con l'autorizzazione Lettura/scrittura.
`root_squash`	Assicura che all'utente `root` di un computer di importazione non siano assegnate autorizzazioni `root` su questo file system. Per ottenere questo risultato, assegnare l'ID utente `65534` agli utenti con ID utente `0` (`root`). Questo ID utente dovrà essere impostato su `nobody` (che corrisponde all'impostazione di default).

Opzione	Descrizione
`no_root_squash`	Non assegna l'ID utente `0` all'ID utente `65534`, mantenendo la validità delle autorizzazioni `root`.
`link_relative`	Converte i collegamenti assoluti, ovvero quelli che iniziano con `/`, in una sequenza di `../`. Questa opzione è utile solo se viene montato l'intero file system di un computer (default).
`link_absolute`	I collegamenti simbolici rimangono invariati.
`map_identity`	Gli ID utente sono esattamente gli stessi sul client e sul server (default).
`map_daemon`	Gli ID utente sul client e sul server non sono corrispondenti. Questa opzione indica a nfsd di creare una tabella di conversione per gli ID utente. Per l'esecuzione di questa operazione è necessario il daemon ugidd.

Il file `exports` potrebbe essere analogo a quello riportato nell'Esempio 42.1, «/etc/exports» (p. 678). Il file `/etc/exports` viene letto da mountd e da nfsd. Se il contento di questo file viene modificato, riavviare mountd e nfsd per rendere effettive le modifiche. Questa operazione può essere eseguita facilmente mediante `rcnfsserver restart`.

Esempio 42.1 */etc/exports*

```
#
# /etc/exports
#
/home             sun(rw)    venus(rw)
/usr/X11          sun(ro)    venus(ro)
/usr/lib/texmf    sun(ro)    venus(rw)
/                 earth(ro,root_squash)
/home/ftp         (ro)
# End of exports
```

43

DHCP

Il protocollo DHCP (*Dynamic Host Configuration Protocol*) viene utilizzato allo scopo di assegnare le impostazioni della rete da un server centrale anziché su ogni singola workstation locale. Un host configurato per l'uso del protocollo DHCP non mantiene il controllo del proprio indirizzo statico, ma è abilitato all'autoconfigurazione completa e automatica in base alle indicazioni del server.

Il protocollo DHCP viene utilizzato, tra l'altro, per identificare ogni client che utilizza l'indirizzo hardware della relativa scheda di rete, che nella maggior parte dei casi è fisso, e per fornire quindi al client impostazioni identiche ogni volta che si connette al server. Può inoltre essere configurato in modo che gli indirizzi vengano assegnati dal server a ogni client interessato in maniera dinamica da un pool di indirizzi configurato per lo scopo specifico. In quest'ultimo caso, il server DHCP tenta di assegnare lo stesso indirizzo al client ogni volta che questo invia una richiesta al server, anche per periodi più lunghi. Questa impostazione funziona, naturalmente, a condizione che nella rete non vi sia un numero di client maggiore di quello degli indirizzi.

Date queste possibilità, il protocollo DHCP può facilitare l'amministrazione del sistema in due modi. Tutte le modifiche, anche quelle più estese, correlate agli indirizzi e alla configurazione della rete in generale possono essere implementate a livello centrale mediante la modifica del file di configurazione del server, una soluzione sicuramente molto più pratica rispetto alla riconfigurazione di numerose workstation. È inoltre molto più facile integrare computer nella rete, specialmente quelli nuovi, poiché possono ricevere un indirizzo IP dal pool. La possibilità di recuperare le impostazioni di rete appropriate da un server DHCP può risultare molto utile nel caso di computer portatili utilizzati in reti diverse.

Un server DHCP fornisce non solo l'indirizzo IP e la maschera di rete, ma anche gli indirizzi del nome host, del nome di dominio, del gateway e del server dei nomi che verranno utilizzati dal client. Oltre a ciò, DHCP consente la configurazione centrale di numerosi altri parametri, ad esempio un server dell'orario dal quale i client possono effettuare il polling dell'ora corrente o anche un server di stampa.

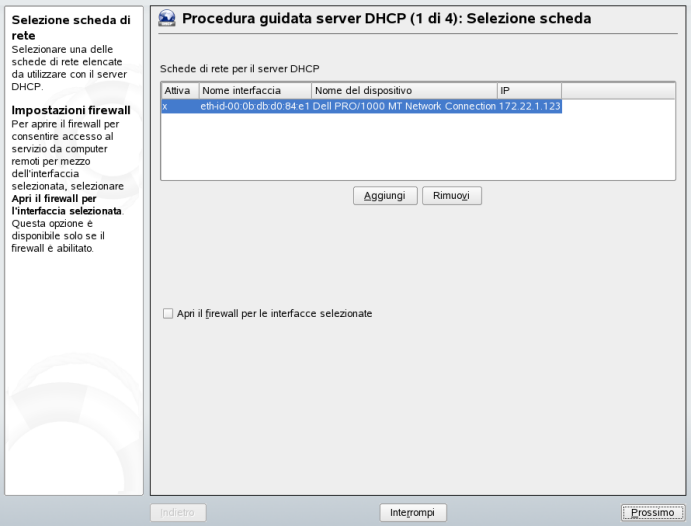
43.1 Configurazione di un server DHCP con YaST

Quando si avvia il modulo per la prima volta viene avviata una procedura guidata che richiede l'assunzione di alcune decisioni di base riguardanti l'amministrazione del server. Il completamento di questa procedura iniziale genera una configurazione del server molto elementare che dovrebbe consentire il funzionamento degli aspetti essenziali, mentre con la modalità di configurazione avanzata è possibile gestire task di configurazione più sofisticati.

Selezione della scheda

Nel primo passaggio della procedura guidata di YaST vengono cercate e visualizzate in un elenco le interfacce di rete disponibili nel sistema. Selezionare dall'elenco l'interfaccia sulla quale il server DHCP dovrà essere in ascolto, quindi fare clic su *Aggiungi* e selezionare *Apri il firewall per l'interfaccia selezionata* per aprire il firewall dell'interfaccia corrente. Vedere la Figura 43.1, «Server DHCP: Selezione scheda» (p. 681).

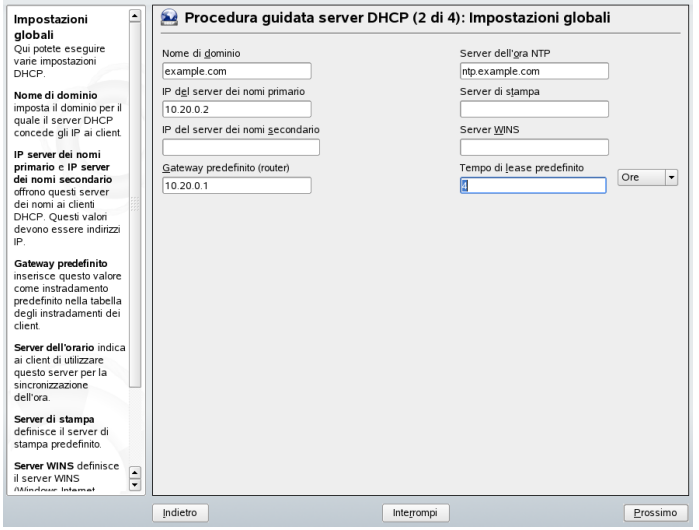
Figura 43.1 *Server DHCP: Selezione scheda*



Impostazioni globali

Nei campi di immissione definire le specifiche della rete per tutti i client gestiti dal server DHCP, ovvero nome del dominio, indirizzo di un server dell'orario, indirizzi dei server dei nomi primario e secondario, indirizzi di un server di stampa e di un server WINS (per una rete mista con client Windows e Linux), indirizzo del gateway e durata del lease. Vedere la Figura 43.2, «Server DHCP: Impostazioni globali» (p. 682).

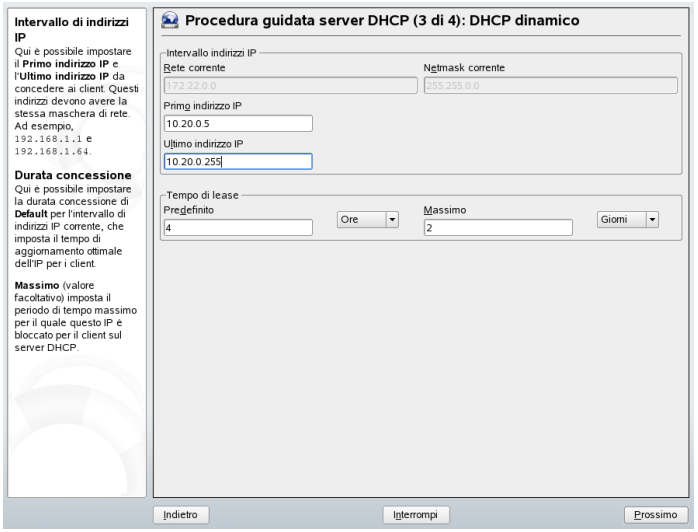
Figura 43.2 *Server DHCP: Impostazioni globali*



DHCP dinamico

In questo passaggio è necessario configurare la modalità di assegnazione degli indirizzi IP dinamici ai client. Per effettuare questa operazione, specificare un intervallo IP dal quale il server può assegnare indirizzi ai client DHCP. Tutti gli indirizzi devono avere una maschera di rete comune. Specificare inoltre la durata del lease, ovvero l'intervallo di tempo durante il quale un client può mantenere lo stesso indirizzo IP senza richiedere un'estensione del lease stesso. È inoltre possibile specificare la durata massima del lease per indicare il periodo in cui un indirizzo IP viene riservato dal server a un client particolare. Vedere la Figura 43.3, «Server DHCP: DHCP dinamico» (p. 683).

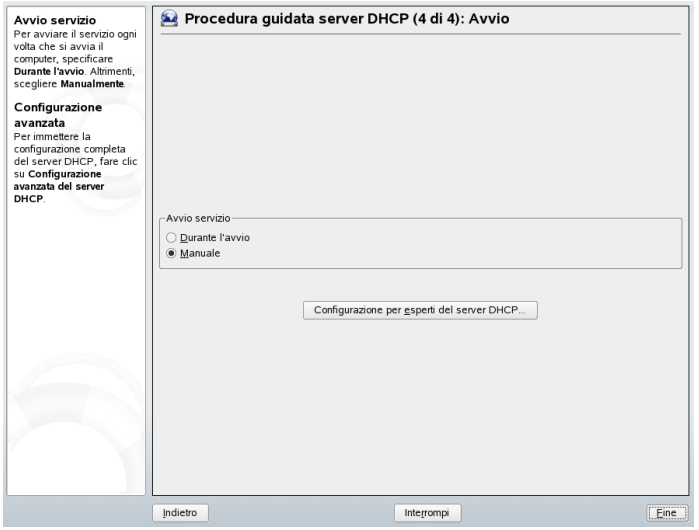
Figura 43.3 *Server DHCP: DHCP dinamico*



Completamento della configurazione e impostazione della modalità di avvio

Dopo il terzo passaggio della procedura di configurazione guidata viene visualizzata l'ultima finestra di dialogo nella quale è possibile definire la modalità di avvio del server DHCP. Specificare se il server dovrà essere avviato automaticamente all'avvio del sistema oppure manualmente quando necessario, ad esempio per l'esecuzione di test. Per completare la configurazione del server, fare clic su *Fine*. Vedere la Figura 43.4, «Server DHCP: Avvio» (p. 684).

Figura 43.4 *Server DHCP: Avvio*



43.2 Pacchetti software DHCP

Per SUSE Linux sono disponibili sia un server DHCP che client DHCP. Il server DHCP disponibile è denominato dhcpd ed è pubblicato da Internet Software Consortium (ISC). Sul lato client è possibile scegliere tra due diversi programmi client DHCP, dhclient, anch'esso pubblicato da ISC, e il daemon del client DHCP incluso nel pacchetto `dhcpcd`.

In SUSE Linux dhcpcd viene installato per default. Il programma è molto semplice da gestire e viene avviato automaticamente a ogni avvio del sistema per il controllo di un server DHCP. Non richiede un file di configurazione per effettuare questa operazione e funziona automaticamente nella maggior parte delle configurazioni standard. Per le situazioni più complesse, utilizzare dhclient di ISC che viene controllato mediante il file di configurazione `/etc/dhclient.conf`.

43.3 Server DHCP dhcpd

Il daemon del protocollo DHCP costituisce la base di qualsiasi sistema DHCP. Questo server assegna gli indirizzi in *lease* e ne controlla l'uso in base alle impostazioni definite nel file di configurazione `/etc/dhcpd.conf`. I parametri e i valori contenuti in questo file possono essere modificati dall'amministratore del sistema per modificare di conseguenza il comportamento dei programmi in vari modi. Nell'Esempio 43.1, «File di configurazione /etc/dhcpd.conf» (p. 685) è riportato un esempio di base del file `/etc/dhcpd.conf`.

Esempio 43.1 *File di configurazione /etc/dhcpd.conf*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

Questo semplice file di configurazione dovrebbe essere sufficiente per consentire al server DHCP di assegnare indirizzi IP nella rete. Verificare che alla fine di ogni riga sia inserito un punto e virgola, perché diversamente dhcpd non verrà avviato.

Il file di esempio precedente può essere diviso in tre sezioni. La prima definisce, per default, la durata in secondi di assegnazione del lease di un indirizzo IP a un client richiedente (`default-lease-time`) prima della richiesta di rinnovo. Nella seconda sezione è inclusa un'istruzione relativa alla durata massima di mantenimento di un indirizzo IP assegnato dal server DHCP da parte di un computer senza richiederne il rinnovo (`max-lease-time`).

Nella seconda parte sono definiti alcuni parametri di rete di base a livello globale:

- La riga `option domain-name` definisce il dominio di default della rete.

- Tramite la voce `option domain-name-servers` vengono specificati fino a tre valori utilizzabili dal server DNS per risolvere gli indirizzi IP in nomi host e viceversa. Prima di configurare il server DHCP, è consigliabile configurare un server dei nomi nel computer in uso o in un altro computer della rete, il quale dovrà inoltre definire un nome host per ogni indirizzo dinamico e viceversa. Per informazioni sulla configurazione del server dei nomi, leggere il Capitolo 40, *DNS: Domain Name System* (p. 643).

- La riga `option broadcast-address` definisce l'indirizzo di diffusione utilizzato dal client richiedente.

- Mediante la riga `option routers` viene indicata al server la destinazione dei pacchetti di dati che non possono essere consegnati a un host nella rete locale, in base agli indirizzi host di origine e di destinazione e alla maschera di sottorete specificati. Nella maggior parte dei casi, specialmente nelle reti di piccole dimensioni, questo router corrisponde al gateway Internet.

- Mediante la riga `option subnet-mask` viene specificata la maschera di rete assegnata ai client.

L'ultima sezione del file è riservata alla definizione di una rete e della maschera di sottorete. Per completare il file, è necessario specificare l'intervallo di indirizzi che dovrà essere utilizzato dal daemon DHCP per l'assegnazione degli indirizzi IP ai client interessati. In questo esempio è possibile assegnare ai client un indirizzo compreso nell'intervallo tra `192.168.1.10` e `192.168.1.20` e nell'intervallo tra `192.168.1.100` e `192.168.1.200`.

Dopo la modifica di queste poche righe, dovrebbe essere possibile utilizzare il comando `rcdhcpd start` per attivare il daemon DHCP che sarà immediatamente disponibile all'uso. Per un breve controllo della sintassi, utilizzare il comando `rcdhcpd check-syntax`. In caso di problemi di configurazione imprevisti, ad esempio un errore che causa l'interruzione del server o la mancata restituzione di `Fatto` all'avvio, dovrebbe essere possibile individuare la causa dell'errore leggendo le informazioni contenute nel log di sistema principale `/var/log/messages` o in console 10 (Ctrl + Alt + F10).

In un sistema SUSE Linux di default il daemon DHCP viene avviato in un ambiente chroot per motivi di sicurezza. Per consentirne l'individuazione da parte del daemon, è necessario copiare i file di configurazione nell'ambiente chroot. In genere la copia dei file viene eseguita automaticamente mediante il comando `rcdhcpd start`.

43.3.1 Client con indirizzi IP fissi

Come accennato in precedenza, è possibile utilizzare DHCP per assegnare un indirizzo statico predefinito a un client specifico per ogni richiesta. Gli indirizzi assegnati in modo esplicito hanno sempre la priorità rispetto agli indirizzi dinamici assegnati da un pool. Un indirizzo statico, inoltre, non scade mai come invece avviene per un indirizzo dinamico, ad esempio quando non è disponibile un numero sufficiente di indirizzi e questi devono essere ridistribuiti dal server tra i client.

Per identificare un client configurato con un indirizzo *statico*, in dhcpd viene utilizzato l'indirizzo hardware, ovvero un codice numerico fisso univoco globale formato da sei coppie di ottetti che consente l'identificazione di tutti i dispositivi di rete, ad esempio `00:00:45:12:EE:F4`. Se si aggiungono le rispettive righe, come quelle contenute nell'Esempio 43.2, «Aggiunte al file di configurazione» (p. 687), al file di configurazione dell'Esempio 43.1, «File di configurazione /etc/dhcpd.conf» (p. 685), il daemon DHCP assegnerà sempre lo stesso set di dati al client corrispondente in qualsiasi circostanza.

Esempio 43.2 *Aggiunte al file di configurazione*

```
host earth {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

Il nome del rispettivo client (`host` *`nomehost`*, in questo caso `earth`) viene immesso sulla prima riga e l'indirizzo MAC sulla seconda. Sugli host Linux questo indirizzo può essere determinato con il comando `ifstatus` seguito dal dispositivo di rete, ad esempio `eth0`. Attivare prima la scheda di rete, se necessario, mediante `ifup eth0`. L'output dovrebbe essere analogo a quanto segue

```
link/ether 00:00:45:12:EE:F4
```

Nell'esempio precedente a un client dotato di una scheda di rete con l'indirizzo MAC `00:00:45:12:EE:F4` viene assegnato automaticamente l'indirizzo IP `192.168.1.21` e il nome host earth. Il tipo di hardware da immettere è quasi sempre `ethernet`, benché sia supportato anche `token-ring`, un tipo spesso presente nei sistemi IBM.

43.3.2 Versione di SUSE Linux

Per migliorare la sicurezza, la versione SUSE del server DHCP di ISC è dotata della patch non root/chroot di Ari Edelkind, in modo da consentire l'esecuzione di dhcpd con l'ID utente `nobody` e in un ambiente chroot (`/var/lib/dhcp`). A questo scopo è necessario che il file di configurazione `dhcpd.conf` si trovi nel percorso `/var/lib/dhcp/etc`. Il file viene copiato automaticamente in questa directory all'avvio dello script init.

Per controllare il comportamento del server in relazione a questa funzionalità, utilizzare le voci contenute nel file `/etc/sysconfig/dhcpd`. Per l'esecuzione di dhcpd in ambiente non chroot, impostare la variabile `DHCPD_RUN_CHROOTED` in `/etc/sysconfig/dhcpd` su «no».

Al fine di consentire la risoluzione dei nomi host da parte di dhcpd anche all'interno dell'ambiente chroot, è necessario copiare anche altri file di configurazione:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Questi file vengono copiati in `/var/lib/dhcp/etc/` all'avvio dello script init. Se tali file vengono modificati automaticamente da script, ad esempio `/etc/ppp/ip-up`, apportare le modifiche eventualmente necessarie anche a queste copie. Se nel file di configurazione sono specificati solo indirizzi IP, anziché nomi host, non sarà necessario effettuare di tali modifiche.

Qualora nella configurazione siano presenti file aggiuntivi che devono essere copiati nell'ambiente chroot, specificarli nella variabile `DHCPD_CONF_INCLUDE_FILES` nel file `/etc/sysconfig/dhcpd`. Per assicurare il funzionamento della registrazione DHCP anche dopo un riavvio del daemon syslog, è necessario aggiungere l'opzione `"-a /var/lib/dhcp/dev/log"` in `SYSLOGD_PARAMS` nel file `/etc/sysconfig/syslog`.

43.4 Ulteriori informazioni

Ulteriori informazioni relative a DHCP sono disponibili sul sito Web di *Internet Software Consortium* (`http://www.isc.org/products/DHCP/`, in lingua inglese). oltre che nella documentazione di `dhcpd`, `dhcpd.conf`, `dhcpd.leases` e `dhcp-options`.

44 Sincronizzazione dell'ora con xntp

Il meccanismo NTP (network time protocol) è un protocollo per la sincronizzazione dell'ora del sistema attraverso la rete. In primo luogo, una macchina può ottenere l'ora da un server che è una time source attendibile. Secondariamente, una macchina può fungere da time source per gli altri computer in rete. L'obiettivo è duplice—mantenere l'ora assoluta e sincronizzare l'ora del sistema di tutte le macchine all'interno di una rete.

In molte situazioni, mantenere l'ora esatta del sistema è importante. L'orologio hardware inserito (BIOS) spesso non risponde ai requisiti di applicazioni come i database. La correzione manuale dell'ora del sistema porterebbe a seri problemi, ad esempio, un balzo all'indietro può provocare il malfunzionamento di applicazioni critiche. All'interno di una rete, generalmente, è necessario sincronizzare l'ora del sistema di tutte le macchine, ma la regolazione manuale non è un metodo corretto. xntp fornisce un meccanismo in grado di risolvere questi problemi che regola continuamente l'ora del sistema con l'ausilio di server orari attendibili presenti in rete. Il meccanismo abilita la gestione di orologi di riferimento locali, ad esempio quelli controllati via radio.

44.1 Configurazione di un client NTP con YaST

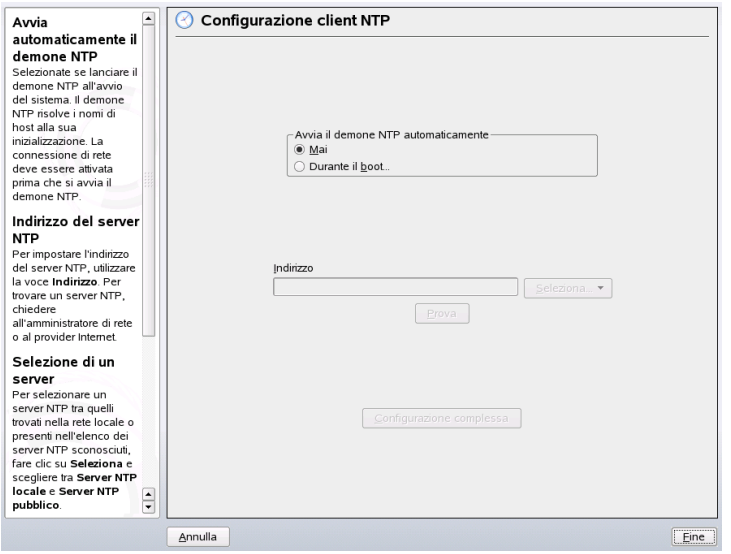
xntp è predisposto per l'utilizzo dell'orologio del computer locale come riferimento temporale. L'utilizzo dell'orologio (BIOS), funge solo da rimedio nel caso in cui non sia disponibile nessuna time source più precisa. In SUSE Linux la configurazione di un client NTP con YaST è facilitata. Utilizzare la configurazione rapida o quella

complessa per i client sui quali non è possibile eseguire SuSEfirewall perché fanno parte di una intranet protetta. La descrizione di entrambi è riportata qui di seguito.

44.1.1 Configurazione rapida di un client NTP

La configurazione facile del client NTP(*Network Services → NTP Client*) comprende due finestre di dialogo. Impostare la modalità di avvio di xntpd e il server da interrogare nella prima finestra di dialogo. Per avviare automaticamente xntpd all'avvio del sistema, cliccare su *All'avvio*. Quindi cliccare su *Seleziona* per accedere a una seconda finestra di dialogo nella quale è possibile selezionare un'ora del server adatta alla propria rete.

Figura 44.1 *YaST: Configurazione di un client NTP*



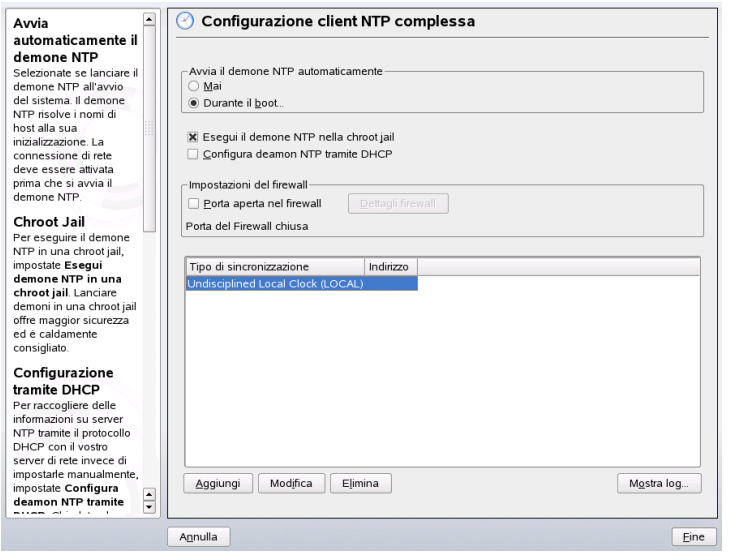
Nell'apposita finestra di dialogo di selezione del server, indicare se implementare la sincronizzazione dell'ora con un server temporale preso dalla rete locale (*Local NTP Server*) o da un server temporale su Internet corrispondente al proprio fuso orario. (*Public NTP Server*). Per il server temporale locale, cliccare su *Cerca* per avviare un'interrogazione SLP relativa ai server temporali disponibili sulla rete. Selezionare il server temporale più idoneo dalla lista dei risultati della ricerca e uscire dalla finestra di dialogo con *OK*. Per un server temporale pubblico, selezionare il paese (fuso orario)

e un server adatto dalla lista *Public NTP Server*, quindi uscire dalla finestra di dialogo con *OK*. Nella finestra di dialogo principale, provare la disponibilità del server selezionato con *Prova* e uscire con *Termina*.

44.1.2 Configurazione complessa di un client NTP

È possibile accedere alla configurazione complessa di un client NTP in*Configurazione complessa* dalla finestra di dialogo principale del modulo *Client NTP*, rappresentato in Figura 44.1, «YaST: Configurazione di un client NTP » (p. 692), dopo aver selezionato la modalità di avvio come descritto nella configurazione rapida.

Figura 44.2 *YaST: Configurazione complessa di un client NTP*



In *Configurazione complessa client NTP*, indicare se xntpd deve essere avviato in una chroot jail. Questo aumenta la sicurezza in caso di attacco tramite xntpd, dato che impedisce all'aggressore di compromettere l'intero sistema. Tramite la *Configurazione del daemon NTP via DHCP* è possibile impostare il client NTP in modo tale da ottenere una lista dei server NTP disponibili in rete tramite DHCP.

Il server e le altre time source che il client deve interrogare sono elencate nella parte inferiore. È possibile modificare questa lista in base alle necessità con *Aggiungi*, *Modifica* e *Cancella*. *Visualizza log* consente di visualizzare i file di log del client.

Cliccare su *Aggiungi* per aggiungere una nuova sorgente di informazioni temporali. Nella finestra di dialogo riportata qui di seguito, selezionare il tipo di sorgente con il quale deve essere effettuata la sincronizzazione. Sono disponibili le seguenti opzioni:

Server
Un'altra finestra di dialogo consente di selezionare un server NTP (come descritto nella Sezione 44.1.1, «Configurazione rapida di un client NTP» (p. 692)). Attivare *Usa per sincronizzazione iniziale* per avviare la sincronizzazione delle informazioni relative all'ora tra il server e il client all'avvio del sistema. Un campo di input consente di indicare altre opzioni per xntpd. Per informazioni dettagliate, consultare `/usr/share/doc/packages/xntp-doc` (parte del pacchetto `xntp-doc`).

Peer
Un peer è una macchina con la quale viene stabilita una relazione simmetrica: funge da server temporale e da client. Per utilizzare un peer all'interno della stessa rete anzichè un server, immettere l'indirizzo del sistema. La parte rimanente della finestra di dialogo è identica a quella del*Server*.

Orologi radio
Per utilizzare un orologio radio per la sincronizzazione dell'ora all'interno del sistema, immettere il tipo di orologio, il numero dell'unità, il nome del dispositivo e altre opzioni in questa finestra di dialogo. Fare clic su*Calibrazione driver* per la messa a punto del driver. Informazioni dettagliate sul funzionamento degli orologi radio locali sono disponibili in `/usr/share/doc/packages/xntp-doc/html/refclock.htm`.

Trasmissione in uscita
È possibile trasmettere le informazioni relative all'ora e le interrogazioni con la trasmissione in rete. In questa finestra di dialogo, immettere l'indirizzo al quale tali trasmissioni devono essere inviate. Non attivare la trasmissione a meno di non avere una time source affidabile, ad esempio un orologio controllato tramite radio.

Trasmissione in entrata
Se si vuole che il client riceva le informazioni per mezzo della trasmissione, immettere in questo campo l'indirizzo dal quale devono essere accettati i rispettivi pacchetti.

44.2 Configurazione xntp in rete

Il modo più facile di utilizzare un server temporale in rete consiste nell'impostare i parametri del server. Ad esempio, se un server temporale chiamato `ntp.example.com` è raggiungibile dalla rete, aggiungere il nome al file `/etc/ntp.conf` aggiungendo la riga `server ntp.example.com`. Per aggiungere altri server temporali, immettere altre righe con il server della parola chiave. Dopo aver inizializzato xntpd con il comando`rcxntpd start` , le operazioni di stabilizzazione dell'ora e creazione della direttiva drift file per la correzione dell'orologio del computer locale saranno effettuate in un'ora circa. Con drift file è possibile calcolare l'errore sistematico dell'orologio dell'hardware non appena il computer viene acceso. La correzione viene utilizzata immediatamente, ottenendo in questo modo una maggiore stabilità dell'ora del sistema.

Esistono due modi possibili per utilizzare il meccanismo NTP come client: Primo, il client può chiedere l'ora da un server noto a intervalli regolari. Con molti client, questo metodo può provocare un elevato carico sul server. Secondo, il client può aspettare le trasmissioni NTP inviate dai server di trasmissione dell'ora nella rete. Lo svantaggio di questo metodo è dato dal fatto che non si conosce la qualità del server e, un server che trasmette informazioni sbagliate, può creare seri problemi.

Se si ottiene l'ora con la trasmissione, il nome del server non è necessario. IIn questo caso, immettere la riga `broadcastclient` nel file di configurazione`/etc/ntp.conf`. Per utilizzare uno o più server temporali in modo esclusivo, immettere i nomi nella riga iniziando con `server`.

44.3 Impostazione di un orologio di riferimento locale

Il pacchetto software xntp contiene i driver per la connessione a orologi di riferimento locali. Nel pacchetto`xntp-doc` all'interno del file `/usr/share/doc/packages/`

xntp-doc/html/refclock.htm, è disponibile una lista degli orologi supportati. Ogni driver è associato a un numero. In xntp, la configurazione corrente avviene tramite pseudo IP. Gli orologi vengono inseriti nel file /etc/ntp.conf come erano in rete. A tal fine, agli orologi vengono assegnati indirizzi IP speciali nel formato 127.127.t.u dove t indica il tipo di orologio e il driver utilizzato e u l'unità che determina l'interfaccia.

Normalmente, i singoli driver hanno parametri speciali che riportano i dettagli relativi alla configurazione. Il file /usr/share/doc/packages/xntp-doc/html/driverNN.htm (dove NN indica il numero del driver) fornisce informazioni sul tipo particolare di orologio. Ad esempio, l'orologio«tipo 8» (orologio radio tramite interfaccia seriale) richiede una modalità aggiuntiva che indica l'orologio in modo più preciso. Il modulo del ricevitore Conrad DCF77, ad esempio, ha modalità 5. Per utilizzare questo orologio come riferimento preferito, indicare la parola chiave prefer. La riga completa del server per il modulo di un ricevitore Conrad DCF77 sarà:

```
server 127.127.8.0 mode 5 prefer
```

Lo stesso modello viene seguito anche per altri orologi. Per quanto riguarda l'installazione del pacchetto xntp-doc, la documentazione di xntp è disponibile nella directory /usr/share/doc/packages/xntp-doc/html. Il file /usr/share/doc/packages/xntp-doc/html/refclock.htm fornisce dei collegamenti alle pagine del driver nelle quali sono descritti i parametri.

45 LDAP - Un servizio directory

LDAP (Lightweight Directory Access Protocol) è un gruppo di protocolli progettato per l'accesso e la gestione di directory di informazioni. LDAP può essere utilizzato per diversi obiettivi, ad esempio per la gestione di utenti e gruppi, della configurazione dei sistemi o degli indirizzi. In questo capitolo vengono fornite alcune nozioni di base su OpenLDAP e sulla gestione di dati LDAP con YaST. Sebbene esistano diverse implementazioni del protocollo LDAP, questo capitolo si concentra esclusivamente sull'implementazione OpenLDAP.

In un ambiente di rete è fondamentale mantenere le informazioni importanti strutturate e prontamente disponibili. Questo obiettivo può essere conseguito con un servizio directory che, come le comuni Pagine Gialle, raccolga le informazioni disponibili in una forma ben strutturata e facile da cercare.

L'opzione ideale è un server centrale che conservi i dati in una directory e li distribuisca a tutti i client mediante un determinato protocollo. I dati sono strutturati in modo da consentirne l'accesso a una vasta gamma di applicazioni. In questo modo non è necessario gestire un database per ogni strumento calendario e client e-mail: è sufficiente accedere a un repository centrale. Ciò riduce notevolmente l'impegno per la gestione delle informazioni. L'utilizzo di un protocollo aperto e standardizzato come LDAP garantisce l'accesso a tali informazioni da parte del maggior numero possibile di applicazioni client.

In questo contesto, una directory è un tipo di database ottimizzato per una rapida ed efficace lettura e ricerca:

- Per rendere possibili numerosi accessi in lettura concomitanti, l'accesso in scrittura è limitato a un numero ridotto di aggiornamenti eseguiti dall'amministratore. I

database convenzionali sono ottimizzati per l'accettazione del massimo volume di dati possibile in un periodo di tempo breve.

- Dato che gli accessi in scrittura possono essere eseguiti solo con delle limitazioni, un servizio directory viene per lo più impiegato per l'amministrazione di informazioni non variabili e statiche. Di norma, i dati contenuti in un database convenzionale vengono modificati molto spesso (dati *dinamici*). I numeri di telefono di un elenco aziendale non cambiano con la stessa frequenza delle cifre amministrate in contabilità, ad esempio.

- L'amministrazione di dati statici implica aggiornamenti dei dati esistenti molto rari. Quando si gestiscono dati dinamici, specialmente set di dati come conti bancari o informazioni contabili, la coerenza dei dati è di fondamentale importanza. Se un importo deve essere sottratto da una cifra e sommato a un'altra, le due operazioni devono essere eseguite contemporaneamente, nell'ambito di una *transazione*, per garantire un saldo corretto. I database supportano tali transazioni. Le directory no. Incoerenze dei dati a breve termine sono abbastanza accettabili nelle directory.

Un servizio directory come LDAP non è progettato per supportare meccanismi di query o aggiornamenti complessi. Tutte le applicazioni devono poter accedere al servizio in modo semplice e rapido.

Molti servizi directory sono esistiti ed esistono tuttora in ambiente Unix e non. Novell NDS, Microsoft ADS, Street Talk di Banyan e lo standard OSI X.500 sono solo alcuni esempi. LDAP è stato originariamente progettato come semplificazione di DAP, il protocollo di accesso alle directory sviluppato per l'accesso a X.500. Lo standard X.500 regola l'organizzazione gerarchica delle voci di directory.

LDAP è una versione ridotta di DAP. Senza perdere la gerarchia delle voci di X.500, LDAP offre funzionalità multipiattaforma e consente di risparmiare risorse. L'utilizzo del protocollo TCP/IP rende sostanzialmente più semplice la definizione di interfacce tra un'applicazione docking e il servizio LDAP.

Nel frattempo, LDAP si è evoluto e viene sempre più impiegato come soluzione indipendente senza supporto X.500. LDAP supporta *riferimenti* con LDAPv3 (la versione di protocollo in pacchetto `openldap2`); ciò consente di avere database distribuiti. Un'ulteriore novità è l'utilizzo del Simple Authentication and Security Layer (SASL).

LDAP non si limita alla ricerca di dati da server X.500 come previsto in origine. Un server slapd open source può memorizzare informazioni sugli oggetti in un database

locale. È inoltre presente un'estensione denominata slurpd, responsabile della replica di più server LDAP.

Il pacchetto `openldap2` è costituito dai seguenti elementi:

slapd
Un server LDAPv3 indipendente che amministra le informazioni sugli oggetti in un database basato su BerkeleyDB.

slurpd
Questo programma consente di replicare le modifiche apportate ai dati del server LDAP locale su altri server LDAP installati nella rete.

ulteriori strumenti per la gestione del sistema
`slapcat`, `slapadd`, `slapindex`

45.1 LDAP rispetto a NIS

L'amministratore di sistema Unix utilizza tradizionalmente il servizio NIS per la risoluzione del nome e la distribuzione dei dati su una rete. I dati di configurazione contenuti nei file in `/etc` e nelle directory `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` e `services` vengono distribuiti dai client su tutta la rete. Questi file possono essere gestiti senza particolari difficoltà in quanto si tratta di semplici file di testo. La gestione di grandi quantità di dati, tuttavia, diventa sempre più difficile a causa della mancanza di una struttura. NIS è progettato solo per piattaforme Unix; ciò rende impossibile il suo impiego come amministratore dati centrale in un ambiente di rete eterogeneo.

A differenza di NIS, il servizio LDAP non è limitato alle reti esclusivamente Unix. I server Windows (a partire dalla versione 2000) supportano LDAP come servizio directory. Anche Novell offre un servizio LDAP. I task applicativi citati in precedenza sono anche supportati in sistemi non Unix.

Il principio LDAP può essere applicato a qualunque struttura di dati da amministrare a livello centrale. Alcuni esempi di applicazione sono i seguenti:

- Impiego a sostituzione del servizio NIS
- Instradamento della posta (postfix, sendmail)

- Rubriche per client di posta come Mozilla, Evolution e Outlook
- Amministrazione di descrizione di zone per un server BIND9
- Autenticazione utenti con Samba in reti eterogenee

Questo elenco può essere esteso in quando LDAP è espandibile, a differenza di NIS. La chiara struttura gerarchica dei dati semplifica l'amministrazione di elevate quantità di dati, in quanto offre migliori funzionalità di ricerca.

45.2 Struttura di un albero di directory LDAP

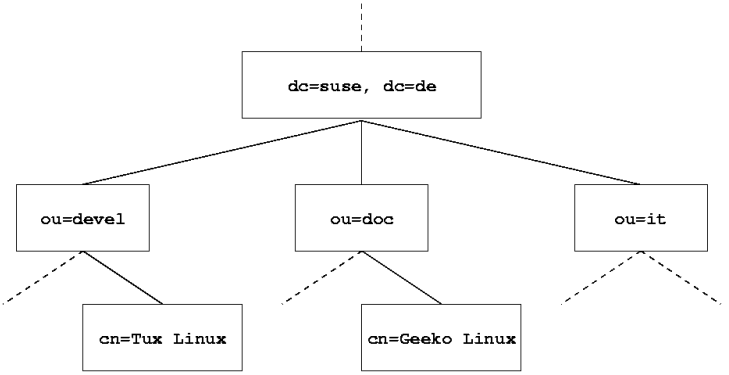
Una directory LDAP presenta una struttura ad albero. Tutte le voci (denominate oggetti) della directory hanno una posizione definita all'interno di questa gerarchia. La gerarchia è denominata *directory information tree* (DIT). Il percorso completo che identifica univocamente la voce desiderata è denominato *nome distinto* o DN. Un nodo sul percorso di questa voce è denominato *nome distinto relativo* o RDN. Gli oggetti possono di norma essere associati a uno dei due seguenti tipi:

container
: Questi oggetti possono a loro volta contenere altri oggetti. Queste classi di oggetti sono `root` (l'elemento radice dell'albero, non realmente esistente), `c` (country, Paese), `ou` (organizational unit, unità organizzativa) e `dc` (domain component, componente dominio). Questo modello è paragonabile alle directory (cartelle) di un file system.

foglia
: Questi oggetti si trovano alla fine di una diramazione e non presentano oggetti subordinati. Esempi sono `person`, `InetOrgPerson` o `groupofNames`.

La parte più alta di una gerarchia di directory dispone di un elemento radice `root`. Questo può contenere `c` (country), `dc` (domain component) o `o` (organization) come elementi subordinati. Le relazioni all'interno di un albero di directory LDAP diventano più evidenti nel seguente esempio, mostrato nella Figura 45.1, «Struttura di una directory LDAP» (p. 701).

Figura 45.1 *Struttura di una directory LDAP*



Lo schema completo comprende un DIT (directory information tree) di fantasia. Sono rappresentate voci su tre livelli. Ciascuna voce corrisponde a un riquadro nell'immagine. Il *nome distinto* completo valido per il dipendente SUSE di fantasia `Geeko Linux` è, in questo caso, `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Viene composto aggiungendo l'RDN `cn=Geeko Linux` al DN della voce precedente `ou=doc,dc=suse,dc=de`.

La definizione globale dei tipi di oggetti da memorizzare nel DIT viene eseguita seguendo uno *schema*. Il tipo di oggetto viene determinato dalla *classe oggetto*. La classe oggetto determina gli attributi obbligatori o facoltativi per l'oggetto interessato. Uno schema, pertanto, deve contenere definizioni di tutte le classi e gli attributi oggetto utilizzati nello scenario applicativo desiderato. Esistono alcuni schemi comuni (vedere RFC 2252 e 2256). È tuttavia possibile creare schemi personalizzati o utilizzare più schemi complementari, se ciò è richiesto dall'ambiente nel quale verrà impiegato il server LDAP.

La Tabella 45.1, «Classi e attributi oggetto comunemente usati» (p. 702) offre una breve panoramica delle classi oggetto degli schemi `core.schema` e `inetorgperson.schema` utilizzati nell'esempio, inclusi gli attributi obbligatori e i valori di attributo validi.

Tabella 45.1 *Classi e attributi oggetto comunemente usati*

Classe oggetto	Significato	Voce di esempio	Attributi obbligatori
dcObject	*domainComponent* (componenti del nome del dominio)	suse	dc
organizationalUnit	*organizationalUnit* (unità organizzativa)	doc	ou
inetOrgPerson	*inetOrgPerson* (dati correlati alla persona per Intranet o Internet)	Geeko Linux	sn e cn

L'Esempio 45.1, «Estratto di schema.core » (p. 702) mostra un estratto di una direttiva di schema con spiegazioni (righe numerate per scopi illustrativi).

Esempio 45.1 *Estratto di schema.core*

```
#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) )
...
```

Il tipo di attributo `organizationalUnitName` e la classe oggetto corrispondente `organizationalUnit` servono come esempio in questo caso. La riga 1 presenta il nome dell'attributo, il suo OID (*identificatore oggetto*) univoco (numerico) e l'abbreviazione dell'attributo stesso.

La riga 2 fornisce una descrizione sintetica dell'attributo con `DESC`. Viene anche indicato l'RFC corrispondente su cui si basa la definizione. `SUP` nella riga 3 indica un tipo di attributo superordinato cui appartiene questo attributo.

La definizione della classe oggetto `organizationalUnit` inizia alla riga 4, come nella definizione dell'attributo con un OID e il nome della classe oggetto. La riga 5 presenta una breve descrizione della classe oggetto. La riga 6, con la sua voce `SUP top`, indica che questa classe oggetto non è subordinata a un'altra. La riga 7, che inizia con `MUST`, elenca tutti i tipi di attributo che *devono* essere utilizzati con un oggetto di tipo `organizationalUnit`. La riga 8, che inizia con `MAY`, elenca tutti i tipi di attributo consentiti con questa classe oggetto.

Un'ottima introduzione all'utilizzo di schemi può essere reperita nella documentazione di OpenLDAP. Se installato, il percorso è `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

45.3 Configurazione del server con slapd.conf

Il sistema installato contiene un file di configurazione completo per il server LDAP nel percorso `/etc/openldap/slapd.conf`. Questo file descrive brevemente le singole voci e le necessarie modifiche. Le voci precedute da cancelletto (#) sono inattive. Per l'attivazione è necessario rimuovere questo carattere di commento.

45.3.1 Direttive globali in slapd.conf

Esempio 45.2 *slapd.conf: Direttiva di inclusione per schemi*

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/rfc2307bis.schema
include         /etc/openldap/schema/yast.schema
```

La prima direttiva del file `slapd.conf`, mostrata nell'Esempio 45.2, «slapd.conf: Direttiva di inclusione per schemi» (p. 703), specifica lo schema in base al quale è organizzata la directory LDAP. La voce `core.schema` è obbligatoria. A questa

direttiva sono aggiunti ulteriori schemi obbligatori. Per informazioni in merito, consultare la documentazione OpenLDAP allegata.

Esempio 45.3 *slapd.conf: pidfile e argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Questi due file contengono il PID (ID processo) e alcuni degli argomenti con cui viene avviato il processo `slapd`. Non sono necessarie modifiche.

Esempio 45.4 *slapd.conf: Controllo dell'accesso*

```
# 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!
```

L'Esempio 45.4, «slapd.conf: Controllo dell'accesso» (p. 704) è un estratto di `slapd.conf` che regola le autorizzazioni di accesso per la directory LDAP sul server. Le impostazioni specificate qui nella sezione globale di `slapd.conf` sono valide finché non vengono dichiarate regole di accesso personalizzate nella sezione specifica del database. Tali regole sovrascriveranno le dichiarazioni globali. Nell'esempio, tutti gli utenti dispongono di accesso in lettura alla directory, ma solo l'amministratore (`rootdn`) può eseguire operazioni di scrittura. La regolamentazione del controllo dell'accesso in LDAP è un processo altamente complesso. Può essere di aiuto quanto segue:

- Ogni regola di accesso presenta la seguente struttura:

  ```
  accesso a <cosa> da <chi> <accesso>
  ```

- *`cosa`* è il segnaposto dell'oggetto o attributo cui è consentito accedere. Le singole diramazioni della directory possono essere esplicitamente protette con regole distinte. È anche possibile elaborare aree dell'albero della directory con una regola utilizzando espressioni regolari. `slapd` valuta tutte le regole nell'ordine in cui sono elencate nel file di configurazione. Le regole più generiche devono essere elencate

dopo quelle più specifiche; la prima regola che `slapd` considera valida viene valutata e tutte le voci successive ignorate.

- *`chi`* definisce a chi consentire l'accesso alle aree specificate con *`cosa`*. È possibile utilizzare espressioni regolari. Ancora una volta, `slapd` interromperà la valutazione di `chi` dopo la prima corrispondenza, pertanto le regole più specifiche dovranno essere specificate prima di quelle più generiche. Sono possibili le voci mostrate nella Tabella 45.2, «Gruppi di utenti e autorizzazioni di accesso» (p. 705).

Tabella 45.2 *Gruppi di utenti e autorizzazioni di accesso*

Tag	Ambito
`*`	Tutti gli utenti senza eccezioni
`anonymous`	Utenti non autenticati («anonimi»)
`users`	Utenti autenticati
`self`	Utenti collegati all'oggetto di destinazione
`dn.regex=<regex>`	Tutti gli utenti corrispondenti all'espressione regolare

- *`accesso`* specifica il tipo di accesso. Utilizzare le opzioni elencate nella Tabella 45.3, «Tipi di accesso» (p. 705).

Tabella 45.3 *Tipi di accesso*

Tag	Ambito di accesso
`none`	Nessun accesso
`auth`	Per contattare il server
`compare`	Confronto con oggetti per accesso tramite confronto
`search`	Per l'impiego di filtri di ricerca

Tag	Ambito di accesso
`read`	Accesso in lettura
`write`	Accesso in scrittura

`slapd` confronta il diritto di accesso richiesto dal client con quelli concessi in `slapd.conf`. Il client è autorizzato ad accedere se le regole consentono un diritto uguale o superiore a quello richiesto. Se il client richiede diritti superiori a quelli dichiarati nelle regole, l'accesso verrà negato.

L'Esempio 45.5, «slapd.conf: Esempio di controllo dell'accesso» (p. 706) mostra un controllo dell'accesso semplice che può essere sviluppato mediante espressioni regolari.

Esempio 45.5 *slapd.conf: Esempio di controllo dell'accesso*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
by user read
by * none
```

Questa regola dichiara che solo il relativo amministratore ha l'accesso in scrittura a una singola voce `ou`. Gli altri utenti autenticati hanno l'accesso in lettura; tutti gli altri non hanno accesso.

SUGGERIMENTO: Definizione di regole di accesso

Se non esistono regole `access to` (accesso a) o direttive `by` (da) corrispondenti, l'accesso verrà negato. Vengono concessi solo i diritti di accesso esplicitamente dichiarati. Se non vengono dichiarate regole, il principio di default è l'accesso in scrittura per l'amministratore e l'accesso in lettura per tutti gli altri utenti.

Per informazioni dettagliate e un esempio di configurazione per i diritti di accesso LDAP, consultare la documentazione in linea del pacchetto `openldap2` installato.

Oltre alla possibilità di amministrare le autorizzazioni di accesso con il file di configurazione server centrale (`slapd.conf`), esiste l'ACI (Access Control Information). Consente di memorizzare informazioni di accesso per singoli oggetti all'interno dell'albero LDAP. Questo tipo di controllo dell'accesso non è ancora comune

ed è ancora considerato sperimentale dagli sviluppatori. Per informazioni, consultare http://www.openldap.org/faq/data/cache/758.html.

45.3.2 Direttive specifiche del database in slapd.conf

Esempio 45.6 *slapd.conf: Direttive specifiche del database*

```
database bdb
checkpoint      1024    5
cachesize       10000
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
```

Questo tipo di database, un database Berkeley in questo caso, è definito nella prima riga di questa sezione (vedere l'Esempio 45.6, «slapd.conf: Direttive specifiche del database» (p. 707)). `checkpoint` determina la quantità di dati (in Kb) conservati nel registro transazioni prima di essere scritti nel database vero e proprio e il tempo (in minuti) tra due azioni di scrittura. `cachesize` imposta il numero di oggetti conservati nella cache del database. `suffix` determina la parte dell'albero LDAP di cui questo server deve essere responsabile. Il `rootdn` successivo determina il possessore di diritti di amministratore per questo server. Non è necessario che l'utente dichiarato qui disponga di una voce LDAP o esista come utente normale. La parola d'ordine dell'amministratore viene impostata con `rootpw`. Invece di utilizzare `secret`, è possibile immettere l'hash della parola d'ordine dell'amministratore creato da `slappasswd`. La direttiva `directory` indica la directory (nel file system) in cui sono memorizzate le directory di database sul server. L'ultima direttiva, `index objectClass eq`, comporta la manutenzione di un indice di tutte le classi oggetto. Gli attributi cercati più di frequente dagli utenti possono essere aggiunti qui in base alla propria esperienza. Le regole di `accesso` personalizzate definite qui per il database verranno utilizzate al posto delle regole di `accesso` globali.

45.3.3 Avvio e arresto dei server

Una volta che il server LDAP è configurato e sono state specificate tutte le voci desiderate in base al modello descritto nella Sezione 45.4, «Gestione dei dati nella directory LDAP» (p. 708), avviare il server LDAP come `root` immettendo `rcldap start`. Per arrestare il server manualmente, immettere il comando `rcldap stop`. Richiedere lo stato del server LDAP in esecuzione con `rcldap status`.

L'editor runlevel di YaST, descritto nella Sezione 28.2.3, «Configurazione dei servizi di sistema (runlevel) con YaST» (p. 457), può essere utilizzato per far sì che il server venga avviato e arrestato automaticamente all'avvio e all'arresto del sistema. È anche possibile creare i relativi collegamenti agli script di avvio e arresto con il comando `insserv` da un prompt dei comandi come descritto nella Sezione 28.2.2, «Script di init» (p. 452).

45.4 Gestione dei dati nella directory LDAP

OpenLDAP offre una serie di strumenti per l'amministrazione dei dati nella directory LDAP. I quattro strumenti più importanti per l'aggiunta, l'eliminazione, la ricerca e la modifica dei dati sono spiegati sinteticamente di seguito.

45.4.1 Inserimento dati in una directory LDAP

Una volta completata la configurazione del server LDAP in `/etc/openldap/lsapd.conf` (con le voci corrette per `suffix`, `directory`, `rootdn`, `rootpw` e `index`), procedere all'inserimento dei record. Per questa attività, OpenLDAP offre il comando `ldapadd`. Se possibile, aggiungere gli oggetti al database in gruppi per ragioni di ordine pratico. LDAP è in grado di elaborare il formato LDIF (LDAP data interchange format) a questo scopo. Un file LDIF è un semplice file di testo che può contenere un numero qualsiasi di coppie di attributo e valore. Per le classi e gli attributi oggetto disponibili, consultare i file di schema dichiarati in `slapd.conf`. Il file LDIF per la creazione di una struttura approssimativa per l'esempio della Figura 45.1, «Struttura di

una directory LDAP» (p. 701) corrisponderà a quello dell'Esempio 45.7, «Esempio di file LDIF» (p. 709).

Esempio 45.7 *Esempio di file LDIF*

```
# The SUSE Organization
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG dc: suse

# The organizational unit development (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

IMPORTANTE: Codifica di file LDIF

LDAP funziona con UTF-8 (Unicode). Le dieresi devono essere codificate correttamente. Utilizzare un editor che supporti UTF-8, come Kate o le versioni recenti di Emacs. In caso contrario, evitare le dieresi o altri caratteri speciali, oppure utilizzare `recode` per ricodificare l'input in UTF-8.

Salvare il file con il suffisso `.ldif`, quindi passarlo al server con il seguente comando:

```
ldapadd -x -D <dn dell'amministratore> -W -f <file>.ldif
```

`-x` disattiva in questo caso l'autenticazione con SASL. `-D` dichiara l'utente che chiama l'operazione. Il DN valido dell'amministratore viene immesso qui così come è stato configurato in `slapd.conf`. Nell'esempio corrente, si tratta di `cn=admin,dc=suse,dc=de`. `-W` consente di evitare l'immissione della parola d'ordine sulla riga di comando (in chiaro) e attiva un prompt separato per la parola d'ordine. Questa parola d'ordine è stata definita in precedenza in `slapd.conf` con `rootpw`. `-f` passa il nome del file. Per dettagli sull'esecuzione di `ldapadd`, vedere l'Esempio 45.8, «ldapadd con example.ldif» (p. 710).

Esempio 45.8 *ldapadd con example.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f example.ldif

Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

I dati dei singoli utenti possono essere preparati in file LDIF distinti. L'Esempio 45.9, «Dati LDIF per Tux» (p. 710) aggiunge `Tux` alla nuova directory LDAP.

Esempio 45.9 *Dati LDIF per Tux*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
uid: tux
telephoneNumber: +49 1234 567-8
```

Un file LDIF può contenere un numero qualunque di oggetti. È possibile passare al server tutte le diramazioni della directory oppure parti di essa come mostrato nell'esempio dei singoli oggetti. Se è necessario modificare alcuni dati con relativa frequenza, si consiglia una precisa suddivisione di singoli oggetti.

45.4.2 Modifica dei dati nella directory LDAP

Lo strumento `ldapmodify` consente di modificare i dati. Il modo più semplice per eseguire questa operazione è modificare il file LDIF corrispondente, quindi passarlo al server LDAP. Per modificare il numero di telefono del collega Tux da `+49 1234 567-8` a `+49 1234 567-10`, modificare il file LDIF come nell'Esempio 45.10, «File LDIF tux.ldif modificato» (p. 711).

Esempio 45.10 *File LDIF tux.ldif modificato*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Importare il file modificato nella directory LDAP con il seguente comando:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

In alternativa, passare gli attributi da modificare direttamente a `ldapmodify`. La relativa procedura è descritta di seguito:

1. Avviare `ldapmodify` e immettere la propria parola d'ordine:

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W
   Enter LDAP password:
   ```

2. Immettere le modifiche rispettando rigorosamente la sintassi nell'ordine esposto di seguito:

   ```
   dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +49 1234 567-10
   ```

Informazioni dettagliate su `ldapmodify` e la relativa sintassi sono presenti nella manpage ldapmodify(1).

45.4.3 Ricerca o lettura di dati da una directory LDAP

Con `ldapsearch`, OpenLDAP fornisce uno strumento di riga di comando per la ricerca e la lettura di dati all'interno di una directory LDAP. Un'interrogazione semplice avrà la seguente sintassi:

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

L'opzione `-b` determina la base di ricerca, ovvero la sezione dell'albero all'interno della quale dovrà essere eseguita la ricerca. Nel caso corrente, si tratta di `dc=suse,dc=de`. Per eseguire una ricerca avanzata in sottosezioni specifiche della directory LDAP (ad

esempio solo all'interno del reparto `devel`), passare questa sezione a `ldapsearch` con `-b`. `-x` richiede l'attivazione dell'autenticazione semplice. `(objectClass=*)` dichiara che devono essere letti tutti gli oggetti contenuti nella directory. Questa opzione di comando può essere utilizzata dopo la creazione di un nuovo albero di directory per verificare che tutte le voci siano state registrate correttamente e che il server risponda come desiderato. Ulteriori informazioni sull'utilizzo di `ldapsearch` sono disponibili nella manpage corrispondente (ldapsearch(1)).

45.4.4 Eliminazione di dati da una directory LDAP

Eliminare le voci superflue con `ldapdelete`. La sintassi è simile a quella dei comandi descritti in precedenza. Ad esempio, per eliminare l'intera voce relativa a `Tux Linux` specificare il seguente comando:

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

45.5 Client LDAP YaST

YaST comprende un modulo per la configurazione della gestione utenti basata su LDAP. Se questa funzionalità non è stata abilitata durante l'installazione, avviare il modulo selezionando *Servizi di rete → Client LDAP*. YaST abilita automaticamente qualunque modifica correlata a PAM e NSS come richiesto da LDAP (descrizione di seguito) e installa i file necessari.

45.5.1 Procedura standard

La conoscenza dei processi che si svolgono in background sui client aiuta a comprendere il funzionamento del modulo client LDAP di YaST. Se viene attivato LDAP per l'autenticazione di rete oppure richiamato il modulo YaST, verranno installati i pacchetti `pam_ldap` e `nss_ldap` e i due file di configurazione corrispondenti modificati. `pam_ldap` è il modulo PAM responsabile della negoziazione tra processi di login e LDAP directory come origine dei dati di autenticazione. Il modulo dedicato `pam_ldap.so` viene installato e la configurazione PAM modificata (vedere l'Esempio 45.11, «pam_unix2.conf modificato per LDAP» (p. 713)).

Esempio 45.11 *pam_unix2.conf modificato per LDAP*

```
auth:       use_ldap
account:    use_ldap
password:   use_ldap
session:    none
```

Quando si configurano manualmente altri servizi per l'utilizzo di LDAP, inserire il modulo LDAP PAM nel file di configurazione PAM corrispondente al servizio in `/etc/pam.d`. File di configurazione già modificati per i singoli servizi sono disponibili in `/usr/share/doc/packages/pam_ldap/pam.d/`. Copiare i necessari file in `/etc/pam.d`.

La risoluzione del nome `glibc` mediante il meccanismo `nsswitch` viene modificata per l'utilizzo di LDAP con `nss_ldap`. Un nuovo file modificato `nsswitch.conf` verrà creato in `/etc/` con l'installazione di questo pacchetto. Per ulteriori informazioni sul funzionamento di `nsswitch.conf`, vedere la Sezione 38.5.1, «File di configurazione» (p. 628). Le seguenti righe devono essere presenti in `nsswitch.conf` per l'amministrazione e l'autenticazione degli utenti con LDAP. Vedere Esempio 45.12, «Modifiche in nsswitch.conf» (p. 713).

Esempio 45.12 *Modifiche in nsswitch.conf*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

Queste righe indicano alla libreria del Resolver di `glibc` in primo luogo di valutare i file corrispondenti in `/etc`, quindi di accedere al server LDAP come origine per l'autenticazione e i dati degli utenti. Verificare questo meccanismo, ad esempio, leggendo il contenuto del database utenti con il comando `getent passwd`. Il set restituito deve contenere la rilevazione degli utenti locali del sistema e tutti gli utenti memorizzati sul server LDAP.

Per impedire che gli utenti normali gestiti mediante LDAP accedano al server con `ssh` o `login`, i file `/etc/passwd` e `/etc/group` devono entrambi presentare un'ulteriore riga. Si tratta della riga `+:::::::/sbin/nologin` in `/etc/passwd` e `+:::` in `/etc/group`.

45.5.2 Configurazione del client LDAP

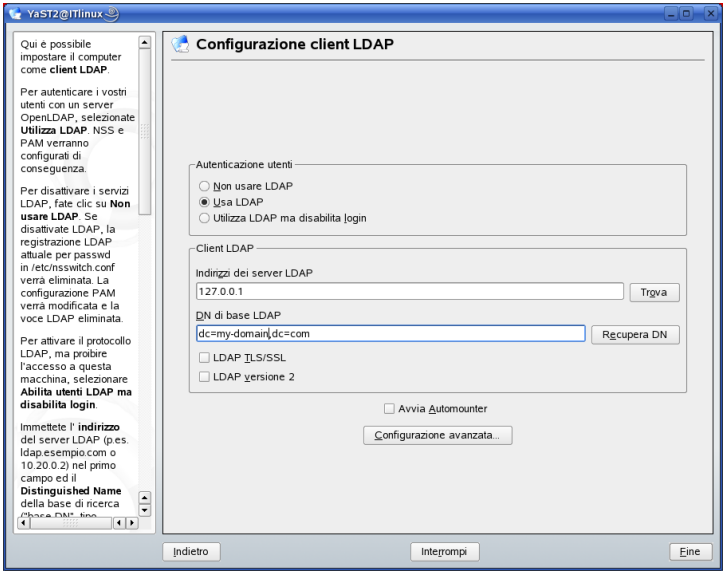
Dopo che YaST avrà apportato le modifiche iniziali a `nss_ldap`, `pam_ldap`, `/etc/passwd` e `/etc/group`, è possibile semplicemente connettersi con il client al server; la gestione degli utenti mediante LDAP verrà eseguita da YaST. Questa configurazione di base è descritta nella sezione chiamata «Configurazione di base» (p. 714).

Utilizzare il client LDAP YaST per configurare ulteriormente i moduli di configurazione utenti e gruppi di YaST. Ciò comprende la manipolazione di impostazioni di default per nuovi utenti e gruppi e la manipolazione del numero e della natura degli attributi assegnati a un utente o a un gruppo. La gestione utenti LDAP consente di assegnare molti più attributi diversi a utenti e gruppi rispetto alle soluzioni tradizionali di gestione utenti o gruppi. Per la relativa descrizione, vedere la sezione chiamata «Configurazione dei moduli di amministrazione utenti e gruppi YaST» (p. 717).

Configurazione di base

La finestra di dialogo di configurazione di base del client LDAP (Figura 45.2, «YaST: Configurazione del client LDAP» (p. 715)) viene visualizzata durante l'installazione se si sceglie la gestione utenti LDAP oppure quando si seleziona *Servizi di rete* → *Client LDAP* nel Centro controllo YaST del sistema installato.

Figura 45.2 *YaST: Configurazione del client LDAP*



Per autenticare gli utenti del computer rispetto a un server OpenLDAP e consentire la gestione utenti mediante OpenLDAP, procedere come segue:

1. Fare clic su *Utilizza LDAP* per abilitare l'uso di LDAP. Selezionare *Utilizza LDAP ma disabilita login* se invece si desidera utilizzare LDAP per l'autenticazione, ma si vuole impedire che altri utenti accedano a questo client.

2. Immettere l'indirizzo IP del server LDAP da utilizzare.

3. Immettere il *DN di base LDAP* per selezionare la base di ricerca sul server LDAP.

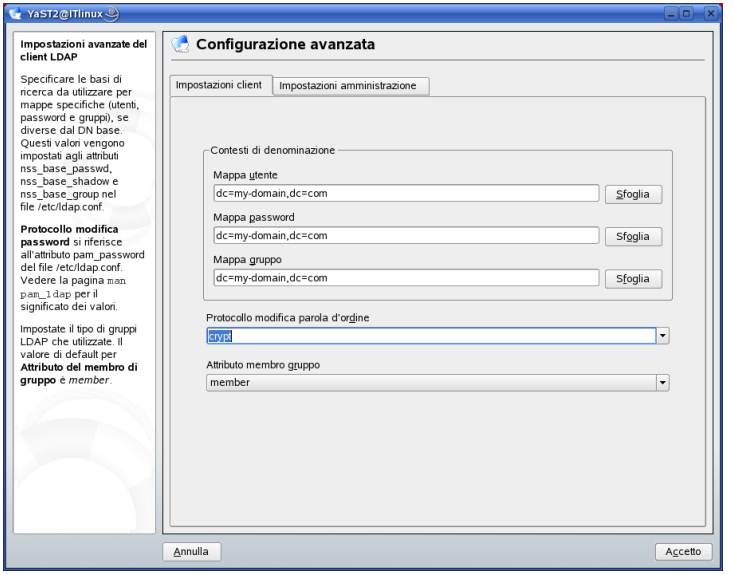
4. Se è necessaria una comunicazione con il server con protezione TLS o SSL, selezionare *LDAP TLS/SSL*.

5. Se il server LDAP utilizza ancora LDAPv2, abilitare esplicitamente l'utilizzo di questa versione di protocollo selezionando *LDAP Versione 2*.

6. Selezionare *Start Automounter (Avvia automounter)* per montare le directory remote sul client, ad esempio la directory `/home` gestita in remoto.

7 Fare clic su *Fine* per rendere effettive le impostazioni.

Figura 45.3 *YaST: Configurazione avanzata*



Per modificare i dati sul server in qualità di amministratore, fare clic su *Configurazione avanzata*. La finestra di dialogo successiva è divisa in due schede. Vedere la Figura 45.3, «YaST: Configurazione avanzata» (p. 716).

1 Nella scheda *Impostazioni client*, modificare le seguenti impostazioni in base alle esigenze:

   a Se la base di ricerca per utenti, parole d'ordine e gruppi differisce dalla base di ricerca globale specificata in *DN di base LDAP*, immettere questi diversi contesti di denominazione in *Mappa utente*, *Mappa password* e *Mappa gruppo*.

   b Specificare il protocollo di modifica password. Il metodo standard da utilizzare quando viene modificata una parola d'ordine è `crypt`, a indicare che vengono utilizzati hash di parola d'ordine generati da `crypt`. Per dettagli in merito a questa e altre opzioni, consultare la manpage `pam_ldap`.

c Specificare il gruppo LDAP da utilizzare con *Group Member Attribute (Attributo membri gruppo)*. Il valore di default è `member`.

2 In *Impostazioni di amministrazione*, definire le seguenti impostazioni:

a Impostare la base per la memorizzazione dei dati di gestione utenti mediante *Configuration Base DN (DN di base configurazione)*.

b Immettere il valore corretto per *DN di amministrazione*. Questo DN deve essere identico al valore `rootdn` specificato in `/etc/openldap/slapd.conf` per consentire a questo utente specifico di manipolare i dati memorizzati sul server LDAP.

c Selezionare *Create Default Configuration Objects (Crea oggetti di configurazione di default)* per creare gli oggetti di configurazione di base sul server per consentire la gestione utenti mediante LDAP.

d Se il computer client dovrà fungere da server file per home directory nella rete, selezionare *Home directory su questa macchina*.

e Fare clic su *Accetta* per uscire dalla finestra *Configurazione avanzata*, quindi su *Fine* per rendere effettive le impostazioni.

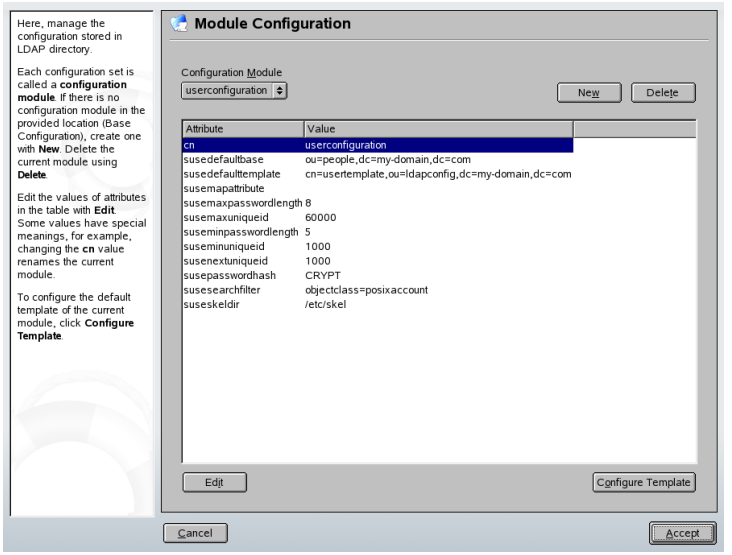
Utilizzare *Configure User Management Settings (Configura impostazioni gestione utenti)* per modificare voci sul server LDAP. L'accesso ai moduli di configurazione sul server verrà quindi concesso in base agli ACL e agli ACI memorizzati sul server. Seguire la procedura descritta nella sezione chiamata «Configurazione dei moduli di amministrazione utenti e gruppi YaST» (p. 717).

Configurazione dei moduli di amministrazione utenti e gruppi YaST

Utilizzare il client LDAP YaST per modificare i moduli YaST per l'amministrazione di utenti e gruppi ed espanderli in base alle necessità. Definire modelli con valori di default per i singoli attributi per semplificare la registrazione dei dati. Le preimpostazioni create qui vengono memorizzate come oggetti LDAP nella directory LDAP. La registrazione dei dati dell'utente viene comunque eseguita con i normali moduli YaST

per la gestione di utenti e gruppi. I dati registrati vengono memorizzati come oggetti LDAP sul server.

Figura 45.4 *YaST: Configurazione dei moduli*



La finestra di dialogo per la configurazione dei moduli (Figura 45.4, «YaST: Configurazione dei moduli» (p. 718)) consente la creazione di nuovi moduli, la selezione e modifica di moduli di configurazione esistenti e la progettazione e modifica di modelli per tali moduli.

Per creare un nuovo modulo di configurazione, procedere come segue:

1. Fare clic su *Nuovo* e selezionare il tipo di modulo da creare. Per un modulo di configurazione utenti selezionare `suseuserconfiguration`; per un modulo di configurazione gruppi scegliere `susegroupconfiguration`.

2. Specificare un nome per il nuovo modello.

   Verrà quindi visualizzata una tabella che elenca tutti gli attributi consentiti in questo modulo con i relativi valori. Oltre a tutti gli attributi impostati, l'elenco contiene anche tutti gli altri attributi consentiti dallo schema corrente, ma attualmente non in uso.

3 Accettare i valori preimpostati oppure modificare i valori di default da utilizzare nella configurazione di utenti e gruppi selezionando il relativo attributo, facendo clic su *Modifica* e immettendo il nuovo valore. Rinominare un modulo modificando semplicemente il suo attributo `cn`. Facendo clic su *Cancella* verrà eliminato il modulo selezionato.

4 Dopo aver fatto clic su *OK*, il nuovo modulo verrà aggiunto al menu di selezione.

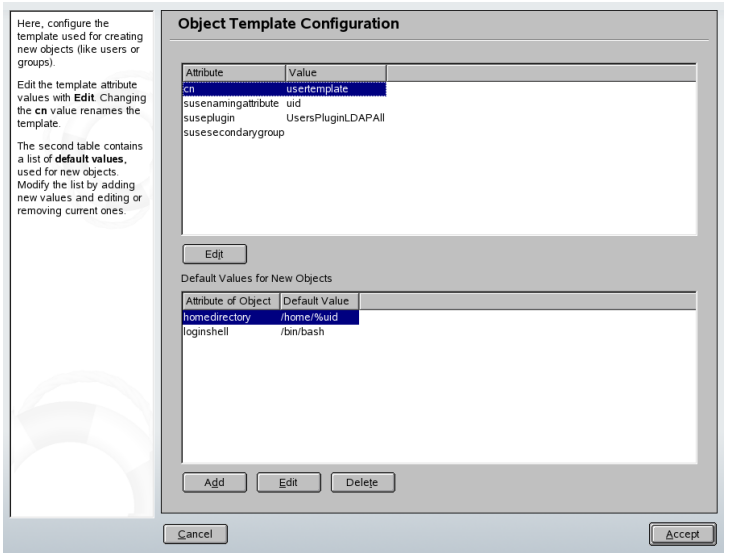
I moduli YaST per l'amministrazione di utenti e gruppi comprendono modelli con valori standard sensibili. Per modificare un modello associato a un modulo di configurazione, procedere come segue:

1 Nella finestra di dialogo *Configurazione dei moduli*, fare clic su *Configure Template (Configura modello)*.

2 Definire i valori degli attributi generali assegnati a questo modello in base alle esigenze, oppure lasciarne alcuni vuoti. Gli attributi vuoti verranno eliminati sul server LDAP.

3 Modificare, eliminare o aggiungere nuovi valori di default per i nuovi oggetti (oggetti di configurazione utenti o gruppi nell'albero LDAP).

Figura 45.5 *YaST: Configurazione di un modello di oggetti*



Collegare il modello al relativo modulo impostando il valore dell'attributo `susedefaulttemplate` del modulo sul DN del modello modificato.

SUGGERIMENTO

I valori di default di un attributo possono essere creati da altri attributi utilizzando uno stile variabile al posto di un valore assoluto. Ad esempio, quando si crea un nuovo utente, `cn=%sn %givenName` viene creato automaticamente dai valori di attributo per `sn` e `givenName`.

Una volta che tutti i moduli e i modelli sono configurati correttamente e pronti per l'esecuzione, è possibile registrare nuovi utenti e gruppi nella modalità consueta con YaST.

45.6 Configurazione di utenti e gruppi LDAP in YaST

La registrazione effettiva di dati di utenti e gruppi differisce solo leggermente dalla procedura eseguita quando non si utilizza LDAP. Le seguenti istruzioni sintetiche si riferiscono all'amministrazione di utenti. La procedura per l'amministrazione di gruppi è simile.

1. Accedere all'amministrazione utenti di YaST con *Sicurezza& Utenti → User Administration (Amministrazione utenti)*.

2. Utilizzare *Imposta filtro* per visualizzare solo gli utenti LDAP e immettere la parola d'ordine per Root DN.

3. Fare clic su *Aggiungi* e specificare la configurazione di un nuovo utente. Verrà visualizzata una finestra di dialogo con quattro schede:

   a. Specificare nome utente, login e parola d'ordine nella scheda *User Data (Dati utente)*.

   b. Utilizzare la scheda *Dettagli* per l'appartenenza ai gruppi, la shell di login e la home directory del nuovo utente. Se necessario, sostituire i valori di default con valori più rispondenti alle proprie esigenze. I valori di default, come quelli delle impostazioni della parola d'ordine, possono essere definiti

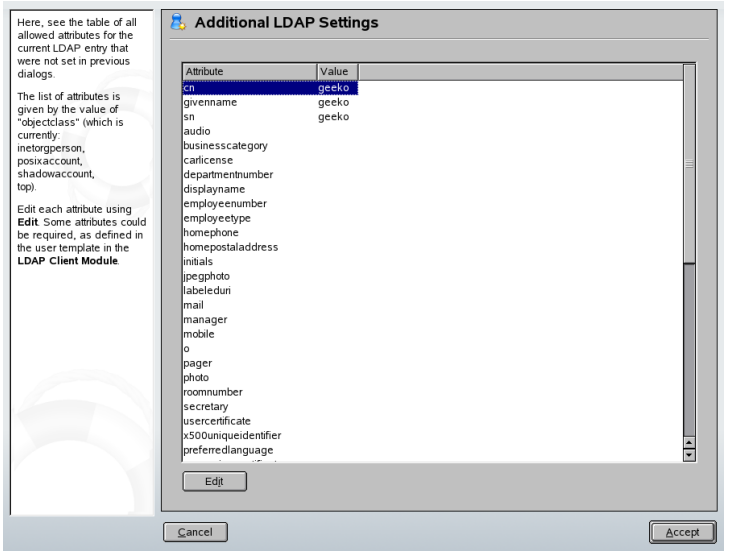
con la procedura descritta nella sezione chiamata «Configurazione dei moduli di amministrazione utenti e gruppi YaST» (p. 717).

c Modificare o accettare le *Impostazioni parola d'ordine* di default.

d Nella scheda *Plug-In*, selezionare il plug-in LDAP, quindi fare clic su *Launch (Avvia)* per configurare ulteriori attributi LDAP assegnati al nuovo utente (vedere la Figura 45.6, «YaST: Ulteriori impostazioni LDAP» (p. 721)).

4 Fare clic su *Accetta* per rendere effettive le impostazioni e uscire dalla configurazione utente.

Figura 45.6 *YaST: Ulteriori impostazioni LDAP*



Il modulo di input iniziale dell'amministrazione utenti offre *opzioni LDAP*. Ciò consente di applicare filtri di ricerca LDAP al set di utenti disponibili, oppure di passare al modulo per la configurazione degli utenti e gruppi LDAP selezionando *Configurazione utenti e gruppi LDAP*.

45.7 Per ulteriori informazioni

Argomenti più complessi, come la configurazione SASL o la creazione di un server LDAP di replica che distribuisca il carico di lavoro tra più slave, non sono stati intenzionalmente trattati in questo capitolo. Informazioni dettagliate sui due argomenti sono disponibili nella *OpenLDAP 2.2 Administrator's Guide* (seguono riferimenti).

Il sito Web del progetto OpenLDAP offre una documentazione esauriente per utenti LDAP inesperti e avanzati:

OpenLDAP Faq-O-Matic
: Raccolta di domande e risposte molto ampia in merito all'installazione, configurazione e all'utilizzo di OpenLDAP. Disponibile all'indirizzo `http://www.openldap.org/faq/data/cache/1.html`.

Quick Start Guide
: Istruzioni sintetiche passo per passo per l'installazione del primo server LDAP. Disponibile all'indirizzo `http://www.openldap.org/doc/admin22/quickstart.html` o su un sistema installato in `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`.

OpenLDAP 2.2 Administrator's Guide
: Introduzione dettagliata a tutti gli aspetti importanti della configurazione LDAP, tra cui controllo dell'accesso e cifratura. Vedere `http://www.openldap.org/doc/admin22/` o, su un sistema installato, `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

Understanding LDAP
: Introduzione generale dettagliata ai principi di base di LDAP: `http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf`.

Letteratura stampata su LDAP:

- *LDAP System Administration* di Gerald Carter (ISBN 1-56592-491-6)
- *Understanding and Deploying LDAP Directory Services* di Howes, Smith, and Good (ISBN 0-672-32316-8)

Il materiale di riferimento ottimale per LDAP è costituito dagli RFC (request for comments, richiesta di commenti) corrispondenti, da 2251 a 2256.

46 Il server Web Apache

Con una partecipazione superiore al 60%, Apache è il server Web più utilizzato al mondo secondo http://www.netcraft.com. Per le applicazioni Web, Apache è spesso utilizzato su Linux con il database MySQL e i linguaggi di programmazione PHP e Perl. Questa combinazione viene spesso chiamata LAMP.

Questo capitolo presenta il software del Web e del server dell'applicazione Apache nella versione 2.x. L'installazione e la configurazione di Apache sono spiegate in questo capitolo unitamente all'utilizzo di alcuni dei moduli disponibili.

46.1 Prefazione e terminologia

Questa sezione riporta le definizione dei termini frequentemente utilizzati relativi al Web e particolari di Apache.

IMPORTANTE: Terminologia

In questo documento, il termine *Apache* si riferisce alla versione Apache 2.x. Per la documentazione relativa ad Apache 1.x, vedere ilsito Web di Apache.

46.1.1 Server Web

Un server Web consegna le pagine Web richieste da un client. Il client può essere un browser Web, ad esempio Konqueror o qualsiasii altro dispositivo in grado di connettersi al World Wide Web (www). Queste pagine possono essere memorizzate per intero su

un disco (pagine statiche) o generate in risposta a una query (pagine dinamiche) di un'entità esterna, ad esempio un database o un servizio Web.

46.1.2 HTTP

La comunicazione tra il client e il server Web avviene tramite l'hypertext transfer protocol (HTTP). La versione corrente, HTTP 1.1, è documentata nell' RFC 2068 e nell'aggiornamento RFC 2616. Questi RFC sono disponibili su `http://www.w3.org`.

46.1.3 URL

URL corrisponde a universal resource locator. I client utilizzano gli URL come `http://www.example.com/index.html`, per richiedere le pagine dal server. Un URL comprende:

Protocollo
Protocolli frequentemente utilizzati:

http://
Il protocollo HTTP

https://

Versione cifrata, sicura di HTTP

ftp://

File transfer protocol per il download e il caricamento di file

Dominio

In questo esempio, il dominio è `www.example.com`. Il dominio è il nome che corrisponde a un indirizzo IP. Quindi, `www.example.com` effettua la mappatura unicamente a un indirizzo IP come 123.456.789.1. A sua volta, il numero identifica unicamente il computer che esegue un server Web. La mappatura di un nome di dominio a un indirizzo IP è comunemente definita *risoluzione del nome*. Il dominio può essere suddiviso in diverse parti, in questo caso: `www`, `example` e `com`. L'ultima parte del nome di dominio si riferisce al top level domain (TLD). In questo esempio,

`com` è il TLD. Il TLD rappresenta il livello massimo del processo di risoluzione del nome. I TLD possono essere generici (gTLD, come `com`, `org` e `di rete`) o specifici di un paese (ccTLD, come `de` per la Germania). Tutte le parti di un nome di dominio, riunite insieme, vengono definite come nomi di dominio completi (FQDN).

Risorsa
In questo esempio, la risorsa è `index.html`. Questa parte specifica il percorso completo alla risorsa. La risorsa può essere un file, come in questo esempio. In ogni caso, può trattarsi anche di uno script CGI, di una pagina JavaServer o di qualche altra risorsa.

Il meccanismo Internet responsabile, ad esempio il domain name system (DNS), inoltra la query al dominio `www.example.com` a uno o più computer che detengono la risorsa. Apache consegna poi la risorsa effettiva, in questo esempio la pagina `index.html`, al client. In questo caso, il file è situato nella directory di livello superiore. In ogni caso, le risorse possono anche essere posizionate in sottodirectory, come in `http://www.example.com/linux/novell/suse`.

46.1.4 Direttiva

Per configurare Apache, il termine *direttiva* viene spesso utilizzato come sinonimo di «opzione di configurazione.» Direttiva è il termine tecnico del software del server Web Apache.

46.2 Installazione

Su SUSE Linux, Apache viene eseguito "in modo eccellente" con una configurazione standard predefinita. Seguendo le istruzioni di questo capitolo, è possibile installare ed eseguire il server web Apache in pochissimo tempo. Per installare e configurare Apachhe `è necessario essere` utenti root.

46.2.1 Installazione di Apache con YaST

Il pacchetto SUSE Linux apache2 presenta lievi differenze per quanto riguarda il layout dell'applicazione e del file system rispetto al pacchetto software standard disponibile

nel sito Web di Apache (http://httpd.apache.org). Nella seguente sezione viene descritta in dettaglio l'installazione del pacchetto SUSE Linux apache2 e vengono evidenziate le differenze esistenti.

Per installare un server Web semplice, attenersi alla seguente procedura:

Procedura 46.1 *Installazione rapida*

1. Avviare YaST nella modalità GUI o riga di comando.
2. Selezionare *Servizi di rete* → *Server HTTP*.
3. Fare clic su *Continua* per confermare l'installazione dei pacchetti `apache2` e `apache2-prefork`.
4. Al termine dell'installazione, viene visualizzato l'*Apache Configuration Wizard (Procedura guidata configurazione Apache)* ed è possibile iniziare a configurare il server Web.

Se si procede come sopra descritto, tuttavia, non sarà disponibile il supporto per i database e PHP. Per installare un server con il supporto per i database e PHP, attenersi alla seguente procedura:

Procedura 46.2 *Installazione di un server Web semplice*

1. Avviare YaST nella modalità GUI o riga di comando.
2. Selezionare *Software* → *Installare/togliere i pacchetti*.
3. Selezionare *Selezione* in *Filtro*, quindi *Server Web semplice con Apache2*.
4. Fare clic su *OK*.
5. Confermare l'installazione dei pacchetti dipendenti per completare la procedura di installazione di SUSE Linux Apache2.

Per gli utenti avanzati, SUSE Linux consente di selezionare pacchetti personalizzati. Per eseguire un'installazione personalizzata di un server Web, attenersi alla seguente procedura:

Procedura 46.3 *Installazione del pacchetto RPM Apache di default con YaST*

1. Avviare YaST nella modalità GUI o riga di comando. Selezionare *Software* → *Installare/togliere i pacchetti*.

2. Selezionare *Cerca* in *Filtro*, quindi immettere `apache2` nel campo *Cerca*.

3. Selezionare `apache2` per l'installazione.

4. Nei passaggi 2 e 3 selezionare i moduli desiderati. Vedere Sezione 46.5, «Moduli Apache» (p. 753).

5. Al termine, fare clic su *Accetta*.

6. Viene quindi chiesto di scegliere una delle dipendenze per il pacchetto `apache2-MPM` necessario: `apache2-prefork` o `apache2-worker`. Per una descrizione delle differenze esistenti tra queste dipendenze, fare riferimento a Sezione 46.2.2, «Moduli per il multiprocessing» (p. 727). In caso di dubbio, selezionare il pacchetto `apache2-prefork`, che è l'impostazione di default per sistemi operativi Unix, quindi fare clic su *OK*.

7. Confermare l'installazione dei pacchetti dipendenti per completare la procedura di installazione di SUSE Linux Apache2.

NOTA: Avvio di un server Web

Quando si installa Apache, il server Web non viene avviato automaticamente. Per informazioni sul controllo dell'avvio e dell'arresto di Apache, fare riferimento a Sezione 46.3.3, «Attivazione, avvio e arresto di Apache» (p. 747).

46.2.2 Moduli per il multiprocessing

Come citato in Installazione del pacchetto RPM Apache di default con YaST (p. 727), SUSE Linux offre due diversi moduli per il multiprocessing (MPM) per l'utilizzo con Apache. Gli MPM si occupano dell'accettazione e della gestione delle richieste a un server Web, rappresentando la parte centrale del software apposito.

MPM prefork

L'MPM prefork implementa un server Web non basato su thread e con funzioni di prefork. Rende il server Web simile ad Apache versione 1.x, poiché isola ciascuna richiesta e la gestisce duplicando un processo secondario separato. In questo modo, le richieste problematiche non hanno conseguenze sulle altre, evitando un blocco del server Web.

Se da un lato garantisce stabilità con questo approccio basato sui processi, l'MPM prefork consuma molte più risorse di un altro programma equivalente, l'MPM worker. L'MPM prefork è considerato l'MPM predefinito per i sistemi operativi basati su Unix.

IMPORTANTE: Gli MPM nella presente documentazione

Questo documento presume l'utilizzo di Apache con l'MPM prefork.

MPM worker

L'MPM worker propone un server Web multithread. Un thread è una forma «più leggera» di processo. Il vantaggio di un thread rispetto a un processo è il consumo più basso di risorse. Invece di duplicare solamente processi secondari, l'MPM worker supporta richieste utilizzando thread con processi del server. I processi secondari di tipo preforked sono multithread.

Questo approccio migliora le prestazioni di Apache, consumando un numero inferiore di risorse di sistema rispetto all'MPM prefork. Uno dei principali svantaggio è la stabilità dell'MPM worker: se un thread viene danneggiato, tutti i thread di un processo possono subirne le conseguenze. La conseguenza peggiore è un arresto del server. Gli errori interni del server, dovuti a thread incapaci di comunicare con le risorse di sistema, possono verificarsi soprattutto per l'utilizzo di CGI (descritto nella sezione chiamata «CGI (Common Gateway Interface): `mod_cgi` » (p. 755)) con Apache sottoposto a un carico eccessivo.

Un altro punto a sfavore dell'utilizzo dell'MPM worker con Apache è che non tutti i moduli di Apache disponibili (vedere la Sezione 46.5, «Moduli Apache» (p. 753)) sono thread-safe, per questo motivo non possono essere utilizzati insieme con MPM worker.

AVVERTIMENTO: PHP come modulo Apache (`mod_php`)

Non tutti i moduli PHP disponibili sono thread-safe. L'utilizzo dell'MPM worker con `mod_php` è fortemente sconsigliato.

46.2.3 Layout predefinito di applicazioni e file system

In SUSE Linux i file del pacchetto Apache vengono archiviati in posizioni predefinite. Di seguito sono riportate le posizioni dei file più importanti.

Binari

A quasi tutti i file eseguibili in SUSE Linux Apache viene aggiunto il valore `2` per differenziarli in caso di un'installazione parallela di Apache 1.x e Apache 2.x.

`/usr/sbin/httpd2`
Collegamento simbolico che fa riferimento a un determinato modulo multiprocessore come descritto nella Sezione 46.2.2, «Moduli per il multiprocessing» (p. 727). Il valore predefinito è `httpd2-prefork`. Il collegamento simbolico viene gestito dallo script di avvio in base alle impostazioni della configurazione di sistema di MPM.

`/usr/sbin/httpd2-prefork`
L'eseguibile effettivo Apache2.

`/usr/sbin/apache2ctl`
Script di controllo per l'avvio e l'arresto del server Web, fornito dal progetto Apache HTTPD. Per ulteriori informazioni o per eseguire `/usr/sbin/apache2ctl help`, vedere la Sezione 46.3.3, «Attivazione, avvio e arresto di Apache» (p. 747).

`/etc/init.d/apache2`
Script di avvio e arresto perfettamente integrabile nell'installazione SUSE Linux e che avvia Apache durante il processo di avvio. Consente di verificare l'esistenza di una configurazione valida prima dell'avvio e dell'arresto del server e di ignorare la posizione della configurazione. Semplifica inoltre l'inserimento di ulteriori file di

configurazione, il caricamento dei moduli o l'avvio di un'istanza separata del server senza modificare lo script.

/usr/sbin/rcapache2
Utile collegamento simbolico per `/etc/init.d/apache2`, perché per impostazione predefinita `/etc/init.d/` non è incluso nel percorso. Per avviare Apache, è sufficiente utilizzare `rcapache2 start`.

/usr/sbin/htpasswd2
Utility per la generazione di password cifrate per l'autenticazione basata su `.htaccess`. Per ulteriori informazioni sull'utilizzo di questo strumento, vedere la pagina di manuale `htpasswd2(1)`.

File di configurazione

Quasi tutti i file di configurazione sono archiviati in `/etc/apache2`. Per ulteriori informazioni su come modificare le impostazioni di configurazione, vedere la Sezione 46.3, «Configurazione» (p. 733).

/etc/apache2/httpd.conf
File di configurazione di primo livello. Se possibile, non modificare questo file poiché contiene principalmente altri file di configurazione e dichiara le impostazioni globali.

/etc/apache2/*.conf
I file di configurazione di alcuni moduli Apache esterni vengono salvati nella directory `/etc/apache2/`. Questi file sono generalmente contrassegnati con il prefisso del nome del modulo stesso (`mod_*.conf`).

/etc/apache2/conf.d/*
Directory che contiene altri file di configurazione inclusi in determinati pacchetti. Per un esempio, vedere la sezione chiamata «PHP: `mod_php4`, `mod_php5` » (p. 762).

/etc/apache2/vhosts.d/*
Directory che contiene i file di configurazione opzionali per gli host virtuali. Per ulteriori informazioni, vedere la Sezione 46.4, «Host virtuali» (p. 749).

/etc/sysconfig/apache2
File di configurazione SUSE Linux relativo ad Apache2. Contiene tutti i parametri di configurazione che controllano il server Web Apache. `/etc/sysconfig/apache2` viene utilizzato da YaST per la configurazione di Apache come descritto nella Sezione 46.3.1, «Configurazione di Apache con YaST» (p. 733). Può essere modificato anche manualmente, come illustrato in Sezione 46.3.2, «Configurazione manuale di Apache» (p. 741).

File di log

Per impostazione predefinita, nei file di Apache riportati di seguito sono disponibili varie informazioni sul relativo stato in fase di esecuzione.

/var/log/apache2/error_log
In questo file vengono registrate le informazioni di avvio e arresto e tutti gli errori verificatisi in fase di esecuzione.

/var/log/apache2/access_log
In questo file vengono registrate tutte le richieste al server Web. Il formato predefinito di queste voci è combinato e include le informazioni sull'host e l'agente utente che inviano la richiesta oltre che l'URI di riferimento.

Home directory

La directory fisica `/srv/www/htdocs` rappresenta la posizione predefinita utilizzata da Apache per fornire le pagine Web. Funge da «directory root» per una richiesta client. Per pubblicare le pagine Web con Apache, archiviare i file in ordine gerarchico all'interno o sotto a questa directory.

Un URL quale http://www.example.com/index.html fa riferimento a `/srv/www/htdocs/index.html` nella configurazione Apache predefinita in SUSE Linux per un dominio di nome example.com.

46.2.4 Generazione manuale dei moduli

Apache è stato creato seguendo un approccio modulare, questo significa che i moduli forniscono le capacità del software del server Web. Di conseguenza, gli utenti avanzati

possono estendere Apache scrivendo moduli personalizzati. Per informazioni più dettagliate consultare le pagine man riportate qui di seguito.

apache2-devel

Per essere in grado di sviluppare moduli per Apache, o di compilare moduli di terzi, è necessario disporre del pacchetto `apache2-devel` unitamente agli strumenti di sviluppo corrispondenti. `apache2-devel` contiene inoltre gli strumenti `apxs2`, necessari alla compilazione di moduli aggiuntivi per Apache.

apxs2

I binari `apxs2` si trovano nella posizione`/usr/sbin`:

- `/usr/sbin/apxs2`— è adatto per generare un modulo di estensione che funziona con qualsiasi MPM. La posizione di installazione è `/usr/lib/apache2`.
- `/usr/sbin/apxs2-prefork`— è adatto per il @@@prefork dei moduli MPM. La posizione di installazione è `/usr/lib/apache2-prefork`.
- `/usr/sbin/apxs2-prefork`—adatto per i moduli di lavoro MPM.

`apxs2` installa i moduli in modo tale che possano essere utilizzati per tutti gli MPM. Gli altri due programmi installano i moduli in modo tale che possano essere utilizzati solo per i rispettivi MPM. `apxs2` installa i moduli in `/usr/lib/apache2` e `apxs2-prefork` in `/usr/lib/apache2-prefork`.

`apxs2` abilita la compilazione e l'installazione di moduli da sorgente (comprese le modifiche necessarie per i file di configurazione) che crea @@@@*dynamic shared objects* (DSO) caricabili in Apache al runtime. Installare un modulo dal sorgente con i comandi `cd /path/to/module/source; apxs2 -c -i mod_foo.c`. Le altre opzioni di`apxs2` sono descritte alla `pagina man` apxs2(1). I moduli dovrebbero quindi essere attivati in `/etc/sysconfig/apache2` con `APACHE_MODULES` come descritto inSezione 46.3.2, «Configurazione manuale di Apache» (p. 741).

46.3 Configurazione

In SUSE Linux Apache può essere configurato in due modi differenti: con YaST o manualmente. La configurazione manuale offre un livello elevato di dettaglio ma non presenta le comodità della GUI di YaST.

IMPORTANTE: Modifiche alla configurazione

Le modifiche ad alcuni valori di configurazione per Apache hanno effetto solo dopo il riavvio di Apache. Questo avviene automaticamente quando si termina la configurazione utilizzando YaST con la casella di controllo *Abilitato* spuntata per *HTTP Service*. Il riavvio manuale è descritto nella Sezione 46.3.3, «Attivazione, avvio e arresto di Apache» (p. 747). La maggior parte delle modifiche alla configurazione richiede solo il ricaricamento con `rcapache2 reload`.

46.3.1 Configurazione di Apache con YaST

YaST consente di configurare un host in rete come server Web. Per configurare un server di questo tipo, avviare YaST e selezionare *Servizi di rete → Server HTTP*. La prima volta che si apre il modulo, viene avviato l'Assistente di sistema: Server HTTP e viene chiesto di effettuare alcune scelte di base riguardanti l'amministrazione del server.

Assistente di sistema: Server HTTP

L'Assistente di sistema: Server HTTP include cinque passaggi o finestre di dialogo. Nell'ultimo passaggio è possibile scegliere di attivare la modalità di configurazione avanzata per configurare impostazioni ancora più specifiche.

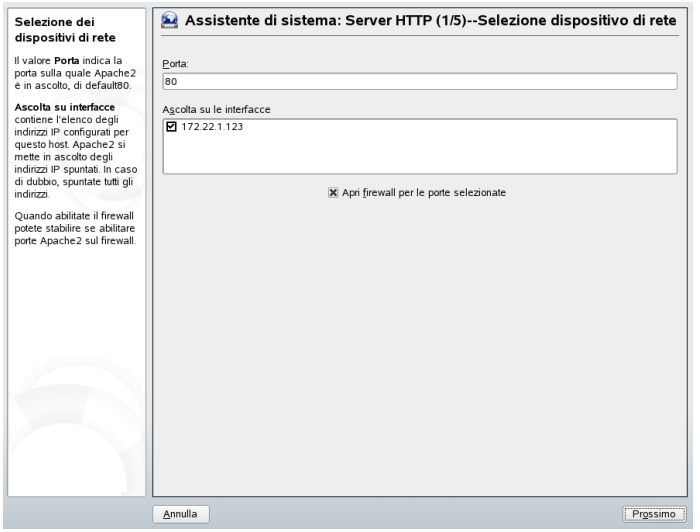
Selezione dispositivo di rete

Specificare le interfacce di rete e le porte utilizzate da Apache per l'ascolto delle richieste in entrata. È possibile selezionare una qualsiasi combinazione di interfacce di rete esistenti e i relativi indirizzi IP. È possibile utilizzare le porte di tutti i tre intervalli, ovvero le porte note, le porte registrate e le porte dinamiche o private, non riservate da altri servizi.

Per default, vengono ascoltate le richieste in entrata su tutte le interfacce di rete (indirizzi IP) sulla porta 80. Quando il firewall è abilitato, è possibile scegliere se abilitare le porte Apache sul firewall.

Selezionare *Apri firewall sulle porte selezionate* per aprire le porte nel firewall su cui il server Web è in ascolto. Questa operazione è necessaria per rendere disponibile il server Web sulla rete, che può essere una rete LAN, WAN oppure Internet pubblica. La chiusura della porta `Listen (Ascolto)` risulta utile negli scenari di verifica in cui non è necessario un accesso esterno al server Web. Se si è soddisfatti delle impostazioni di default oppure dopo avere apportato le modifiche desiderate, fare clic su *Avanti* per continuare la configurazione.

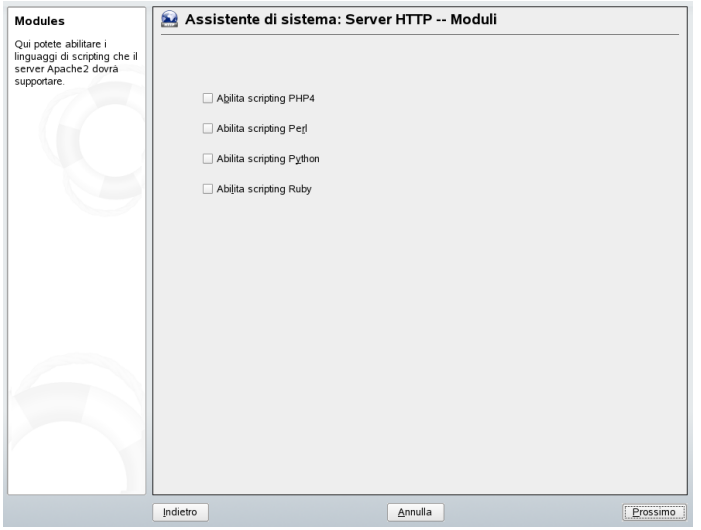
Figura 46.1 *Assistente di sistema: Server HTTP -- Selezione dispositivo di rete*



Moduli

Il pacchetto SUSE Linux Apache include una vasta gamma di moduli Apache. I moduli, disponibili per svariati task, consentono di estendere le funzionalità di Apache. L'opzione di configurazione *Moduli* permette di caricare e scaricare vari moduli Apache durante la fase di avvio del server. Per ulteriori informazioni sui moduli, fare riferimento alla Sezione 46.5, «Moduli Apache» (p. 753). Fare clic su *Avanti* per continuare.

Figura 46.2 *Assistente di sistema: Server HTTP -- Moduli*

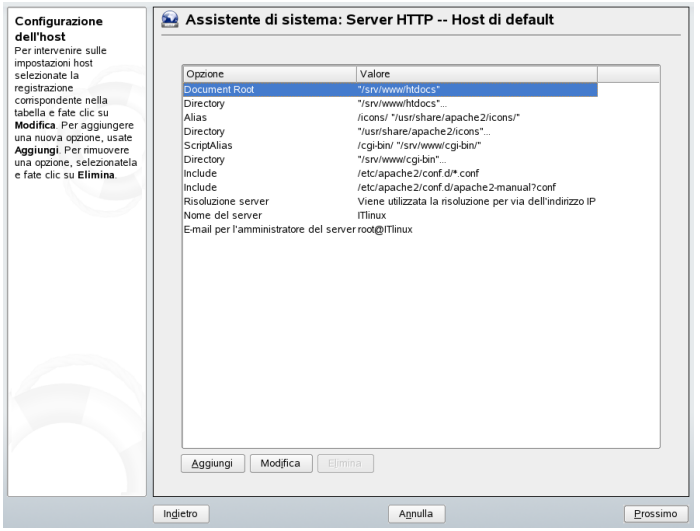


Host predefinito

Questa opzione si riferisce al server Web di default. Come descritto nella Sezione 46.4, «Host virtuali» (p. 749), Apache può gestire più domini da un singolo computer fisico. Il primo dominio dichiarato, o `Host virtuali`, nel file di configurazione è comunemente noto come *host di default*. Per modificare le impostazioni dell'host, scegliere la voce appropriata nella tabella e quindi fare clic su *Modifica*. Per aggiungere un nuovo host, fare clic su *Aggiungi*. Per cancellare un host, selezionarlo e quindi fare clic su *Cancella*.

In questo passaggio è possibile decidere di aggiungere un'opzione SSL (Secure Sockets Layer) e il relativo valore alle impostazioni dell'host. Per ulteriori informazioni, vedere la sezione chiamata «Aggiunta del supporto SSL» (p. 740).

Figura 46.3 *Assistente di sistema: Server HTTP -- Host predefinito*



Di seguito vengono elencate le impostazioni di default del server:

Document Root
Come descritto nella sezione chiamata «Home directory» (p. 731), `/srv/www/htdocs` è il percorso di default da cui Apache gestisce le pagine Web.

Directory
`/srv/www/htdocs` è il percorso delle pagine Web.

Alias
Le direttive `Alias` consentono di mappare gli URL a percorsi di file system fisici. Questo significa che è possibile accedere a un percorso anche se *non è incluso* nella `radice documenti` del file system tramite un URL mappato a tale percorso.

Il file di default di SUSE Linux `Alias /icons` punta a `/usr/share/apache2/icons` per le icone Apache visualizzate nella vista degli indici delle directory.

Directory
`/usr/shareapache2/icons` è il percorso della directory `Alias`.

ScriptAlias
La direttiva `ScriptAlias`, simile alla direttiva `Alias`, consente di mappare un URL al percorso di un file system. La differenza è data dal fatto che `ScriptAlias` imposta la directory di destinazione come percorso CGI, il che significa che gli script CGI devono essere eseguiti in tale percorso.

Directory
`/srv/www/cgi-bin` è il percorso della directory `ScriptAlias`.

Include (Includi)
`/etc/apache2/conf.d/*.conf` è la directory contenente i file di configurazione forniti con alcuni pacchetti. `/etc/apache2/conf.d/apache2-manual?conf` è la directory contenente tutti i file di configurazione `apache2-manual`.

Risoluzione server
Questa opzione si riferisce alla Sezione 46.4, «Host virtuali» (p. 749).

Determina server richiedente tramite intestazioni HTTP consente a un `Host Virtuale` di rispondere a una richiesta inviata al nome del server (vedere la Sezione 46.4.1, «Host virtuali basati sul nome» (p. 749)).

Determina server richiedente tramite indirizzo IP del server consente ad Apache di selezionare l'host richiesto in base alle informazioni dell'intestazione HTTP inviate dal client. Per ulteriori informazioni sugli host virtuali basati su IP, vedere la Sezione 46.4.2, «Host virtuali basati su IP» (p. 752).

Nome del server
Specifica l'URL di default utilizzato dai client per contattare il server Web. Utilizzare un FQDN (vedere Dominio (p. 724)) per contattare il server Web all'indirizzo `http://`*`FQDN`* oppure specificare il relativo indirizzo IP.

E-mail per l'amministratore del server
Specificare l'indirizzo e-mail dell'amministratore del server Web in *E-mail per l'amministratore del server*.

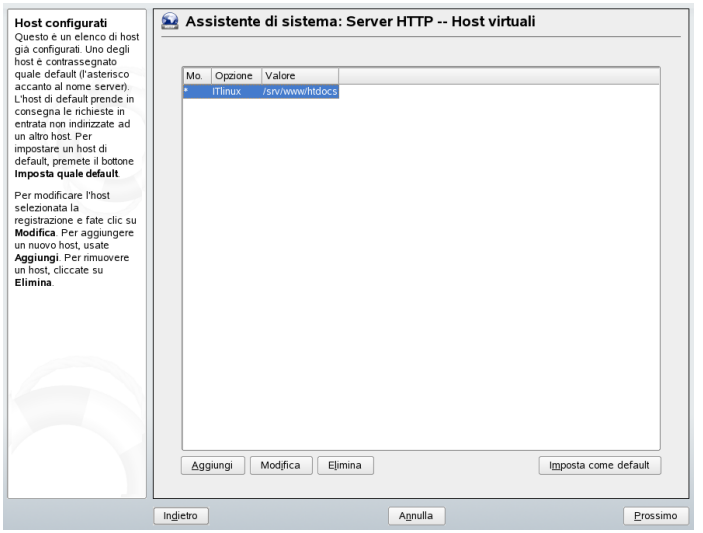
Dopo avere completato il passaggio *Host predefinito*, fare clic su *Avanti* per passare alla finestra di configurazione successiva.

Host virtuali

In questo passaggio viene visualizzato un elenco degli host virtuali già configurati (vedere la Sezione 46.4, «Host virtuali» (p. 749)). Accanto al nome di server di uno di questi host è presente un asterisco per indicare che è l'host di default. Per impostare un host di default, selezionare il server e fare clic su *Imposta come default*.

Per aggiungere un host, fare clic su *Aggiungi*. Viene visualizzata una finestra di dialogo nella quale è possibile immettere le informazioni di base dell'host. *Identificazione server* include il nome del server, la radice del contenuto del server e l'e-mail dell'amministratore. Il testo della Guida nella parte sinistra della finestra contiene una descrizione dettagliata di tutti questi elementi. *Risoluzione server* consente di impostare la modalità di identificazione di un host. È possibile scegliere se si desidera identificare il server di una richiesta in base alle intestazioni HTTP oppure in base all'indirizzo IP del server selezionando l'apposita opzione. La seconda opzione consente di identificare l'host virtuale in base all'indirizzo IP utilizzato dal client durante la connessione al server. È inoltre possibile scegliere di abilitare il supporto SSL selezionando l'apposita opzione nonché specificare il percorso del certificato. Quando si fa clic su *Sfoglia*, viene visualizzata la directory di default `/etc/apache2/ssl.crt`. Dopo avere immesso tutte le informazioni desiderate, fare clic su *Avanti* per proseguire con il passaggio finale della configurazione.

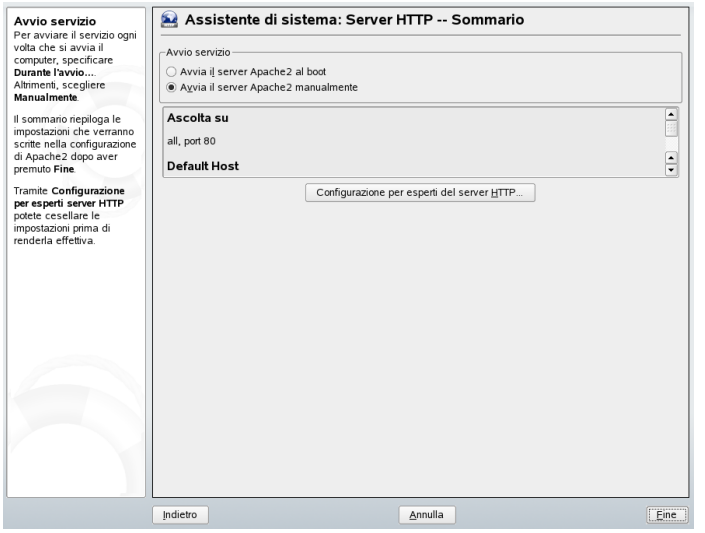
Figura 46.4 *Assistente di sistema: Server HTTP -- Host virtuali*



Sommario

Questo è il passaggio finale dell'assistente, nel quale è possibile specificare come e quando il server Apache dovrà essere avviato, ovvero automaticamente durante la procedura di avvio del sistema oppure manualmente. Vengono inoltre visualizzati sia la porta selezionata in precedenza che gli host di default e virtuali. Se si è soddisfatti delle impostazioni, fare clic su *Finito* per completare la configurazione.

Figura 46.5 *Assistente di sistema: Server HTTP -- Sommario*



Configurazione per esperti del server HTTP

Il modulo del server HTTP consente di apportare ulteriori modifiche alla configurazione. Fare clic su *Configurazione per esperti del server HTTP* per visualizzare ulteriori opzioni di configurazione. È quindi possibile apportare le seguenti modifiche:

Ascolta su

Quando si seleziona l'impostazione *Ascolta su* e si fa clic su *Modifica*, viene visualizzata una nuova finestra nella quale è possibile aggiungere, cancellare o modificare voci.

Moduli
Quando si seleziona l'impostazione *Moduli* e si fa clic su *Modifica*, è possibile modificare lo stato dei moduli Apache2 tramite il controllo *Cambia lo stato*. Fare clic su *Aggiungi modulo* per aggiungere un nuovo modulo.

Host predefinito
Quando si seleziona *Host predefinito* e si fa clic su *Modifica*, è possibile modificare le impostazioni dell'host. È inoltre possibile aggiungere, modificare o cancellare opzioni.

Hosts
Quando si seleziona *Hosts* e si fa clic su *Modifica*, è possibile aggiungere, cancellare, modificare o impostare come default un host.

In tutte le finestre di dialogo precedenti è possibile fare clic su *File di log* per visualizzare il log degli errori e il log degli accessi. Fare clic su *OK* per completare la configurazione e tornare al centro controllo YaST.

Aggiunta del supporto SSL

Per aggiungere un'opzione SSL all'host, fare clic su *Aggiungi* nel terzo passaggio dell'Assistente di sistema: Server Wizard in cui viene configurato l'host di default. Se il server è già stato configurato e non è più possibile accedere all'assistente, è possibile configurare un'opzione SSL selezionando *Host di default* nella finestra di dialogo Configurazione del server HTTP oppure facendo clic su *Modifica* e quindi su *Aggiungi*. In entrambi i casi, viene visualizzata una finestra popup nella quale è possibile selezionare un'opzione *SSL* e fare clic su *OK* per confermare la scelta effettuata. Viene quindi chiesto di immettere un valore per l'opzione selezionata. In alcuni casi potrebbe essere sufficiente impostare il valore su *on* o *off*, mentre in altri potrebbe essere necessario immettere un valore appropriato. In caso di dubbio sui parametri da utilizzare durante la configurazione di SSL, fare riferimento alla documentazione. Quando si fa clic su *OK*, l'opzione e il relativo valore vengono visualizzati nell'elenco delle configurazioni dell'host. Quando si fa clic su *Avanti*, viene visualizzato il passaggio successivo della configurazione.

Se nell'elenco delle configurazioni dell'host è indicata la voce *SSL*, fare clic su *Modifica* per visualizzare la finestra di dialogo per la configurazione di SSL. Se questa voce non è indicata, fare clic su *Aggiungi*, selezionare *SSL* e fare clic su *OK* per visualizzare automaticamente la finestra di dialogo nella quale è possibile aggiungere, cancellare o

modificare le opzioni SSL. Fare clic su *OK* per tornare all'Assistente di sistema: Server HTTP.

46.3.2 Configurazione manuale di Apache

Per configurare Apache manualmente, è necessario modificare i file di configurazione nel formato testo semplice come utente `root`.

IMPORTANTE: Modulo SuSEconfig per Apache2 rimosso

Il modulo SuSEconfig per Apache2 è stato rimosso da SUSE Linux. Quindi, non è più necessario eseguire `SuSEconfig` dopo aver modificato `/etc/sysconfig/apache2`.

/etc/sysconfig/apache2

`/etc/sysconfig/apache2` controlla alcune impostazioni globali di Apache, ad esempio i moduli da caricare, gli ulteriori file di configurazione da includere, i flag per l'avvio del server e quelli da aggiungere alla riga di comando. Per ciascuna opzione di configurazione inclusa in questo file è una disponibile una dettagliata descrizione, per questo motivo tali opzioni non vengono ulteriormente illustrate in questa sezione. `/etc/sysconfig/apache2` è generalmente sufficiente per qualsiasi tipo di configurazione su un server Web generico. Per specificare un particolare tipo di configurazione, vedere la sezione chiamata «Direttive di apache in /etc/apache2/httpd.conf: Ambiente globale » (p. 742).

IMPORTANTE: File creati automaticamente all'avvio del server

`/etc/sysconfig/apache2` crea o modifica automaticamente i seguenti file all'avvio o al riavvio del server Web.

- `/etc/apache2/sysconfig.d/loadmodule.conf`: include i moduli che vengono caricati in fase di esecuzione
- `/etc/apache2/sysconfig.d/global.conf`: include le impostazioni generali del server

- `/etc/apache2/sysconfig.d/include.conf`: include l'elenco dei file di configurazione disponibili

Non modificare questi file manualmente, ma solo le impostazioni corrispondenti in `/etc/sysconfig/apache2`.

Per modifiche di vario tipo a livello di configurazione, vedere i file nella directory `/etc/apache2/*`, in particolare per le modifiche alla configurazione manuale di host virtuali, dell'ambiente globale o del server principale.

Direttive di apache in /etc/apache2/httpd.conf: Ambiente globale

SUSE Linux utilizza `/etc/apache2/httpd.conf` come punto di riferimento per gli altri file di configurazione. Modificare questo file solo per abilitare le funzioni non disponibili in `/etc/sysconfig/apache2`. Le direttive incluse nella sezione *Ambiente globale* di `httpd.conf` influiscono sul funzionamento complessivo di Apache.

Nelle sezioni seguenti verranno illustrate alcune direttive non disponibili in YaST. Direttive di base quali l'`home directory` (Document Root (p. 736)) sono fondamentali e obbligatorie sia nell'`Ambiente globale` che per l'`host virtuale`.

I parametri e le direttive seguenti, ordinati in base alla connessione logica e all'ambito di configurazione, devono essere impostati in `/etc/apache2/httpd.conf`.

LoadModule *module_identifier /path/to/module*

La direttiva `LoadModule` specifica il modulo Apache da caricare in fase di esecuzione. *`module_identifier`* rappresenta il nome del modulo in base alla relativa documentazione. */path/to/module* può essere un percorso relativo o assoluto cha fa riferimento al file.

Esempio 46.1 *Direttiva LoadModule*

```
LoadModule rewrite_module /usr/lib/apache2-prefork/mod_rewrite.so
```

In SUSE Linux non è necessario utilizzare direttamente le istruzioni `LoadModule` poichè in `/etc/sysconfig/apache2` viene utilizzato `APACHE_MODULE`.

MaxClients *numero*

Il numero massimo di client che Apache può gestire contemporaneamente. Il valore di MaxClients deve essere sufficientemente grande da consentire la gestione delle richieste simultanee che il sito Web prevede di ricevere, ma sufficientemente piccolo da garantire l'elaborazione di tutti questi processi nella memoria RAM fisica.

Timeout *secondi*

Specifica il periodo di attesa prima che in Apache venga indicato un tempo massimo per una richiesta.

Direttive di Apache in /etc/apache2/httpd.conf: Server principale

Le direttive nella sezione `Server principale` si applicano quando le richieste di un client non possono essere gestite da alcun `Host virtuale` e devono quindi essere elaborate da un server predefinito o principale. Inoltre, i parametri specificati in questo contesto sono predefiniti per tutti gli host virtuali configurati. Di conseguenza, tutte le direttive incluse nella sezione `Server principale` possono essere specificate anche nel contesto `Host Virtuale` sovrascivendo i valori predefiniti.

DirectoryIndex *nomi file*

Consente di specificare i file che è necessario cercare in Apache per completare un URL che non include le informazioni sui file. L'impostazione predefinita è `index.html`. Se ad esempio il client richiede l'URL `http://www.example.com/foo/` e la directory `foo` contiene un file di nome `index.html`, al client verrà inviata questa pagina. Per dichiarare più file, separarli mediante spazi.

Esempio 46.2 *Direttiva DirectoryIndex*

```
DirectoryIndex index.html index.shtml start.php begin.pl
```

AllowOverride All | None | *opzione*

Questa direttiva può essere utilizzata *solo* in una dichiarazione `<Directory></Directory>`. Vedere Directory (p. 736).

`AllowOverride` specifica le opzioni di accesso e visualizzazione che possono essere ignorate da un file `.htaccess`, oppure dai file specificati in `AccessFileName` come descritto nella sezione chiamata «`AccessFileName` *nomi file* » (p. 745).

I valori possibili sono:

`All`
Il file `.htaccess` può ignorare tutte le opzioni.

`None`
Il file `.htaccess` non può ignorare alcuna opzione.

`AuthConfig`
Le directory possono essere protette da password mediante un file `.htaccess`.

`FileInfo`
Consente di utilizzare le direttive che controllano i tipi di documenti inclusi in un file `.htaccess`. Un esempio tipico è la configurazione di pagine di errore personalizzate con `ErrorDocument` (vedere `http://httpd.apache.org/docs-2.0/mod/core.html#errordocument`).

`Indexes`
Se non è disponibile alcun documento `DirectoryIndex`, è possibile utilizzare questo parametro che consente di controllare la visualizzazione del contenuto di una directory in Apache.

`Limit`
Controlla l'accesso a una directory o ad alcuni file relativi a un client. A questo scopo, vengono utilizzate le direttive `Allow`, `Deny` e `Order` in un file `.htaccess`. Per informazioni sull'utilizzo di queste direttive, vedere la documentazione sui modulo di accesso (`http://httpd.apache.org/docs-2.0/mod/mod_access.html`).

`Options`
Consente di utilizzare le direttive `Options` e `XBitHack` in un file `.htaccess`. La direttiva `Options` (`http://httpd.apache.org/docs-2.0/mod/core.html#options`) controlla quali funzioni di server sono disponibili in una determinata directory. La direttiva `XBitHack` (`http://httpd.apache.org/docs-2.0/mod/mod_include.html#xbithack`) consente ai file con bit

di esecuzione di essere analizzati come SSI (vedere la sezione chiamata «Server-Side Includes con `mod_include` » (p. 754)).

IMPORTANTE

Queste impostazioni vengono applicate in maniera ricorrente alla directory e alle relative sottodirectory. È possibile combinare queste opzioni, eccetto `All` e `None` separandole con degli spazi.

Esempio 46.3 *Direttiva AllowOverride*

```
<Directory /srv/www/htdocs>
    AllowOverride None
</Directory>
<Directory /srv/www/htdocs/project>
    AllowOverride All
</Directory>
<Directory /srv/www/htdocs/project/webapp>
    AllowOverride Indexes Limit AuthConfig
</Directory>
```

AccessFileName *nomi file*

`AccessFileName` consente di impostare i file che possono ignorare le autorizzazioni di accesso globale e le altre impostazioni per le directory (vedere Directory (p. 736)).

L'impostazione predefinita è `.htaccess`. Per dichiarare più file, separarli con degli spazi.

Esempio 46.4 *Direttiva AccessFileName*

```
AccessFileName .htaccess .acl permission.txt
```

ErrorLog *file | "|command"*

Specifica il nome del file in cui vengono protocollati i messaggi di errore in Apache. In alternativa, questi messaggi possono essere salvati in un comando o uno script. L'impostazione predefinita è `/var/log/apache2/error_log`.

Esempio 46.5 *Direttiva ErrorLog*

```
ErrorLog /var/log/apache2/error_log
ErrorLog "|/path/to/script"
```

`LogLevel` *`livello`*

Imposta il livello di dettagli da specificare nei messaggi di log. In un livello di dettagli in ordine crescente (e gravità decrescente dei messaggi), il *`livello`* può essere

- `emerg`
- `alert`
- `crit`
- `error`
- `warn`
- `notice`
- `info`
- `debug`

L'impostazione predefinita è `warn`, consigliata per le attività quotidiane. Per le operazioni di debug si consiglia di utilizzare `info` e `debug` perchè forniscono maggiori dettagli.

Esempio 46.6 *Direttiva LogLevel*

```
LogLevel debug
```

Direttive di apache in /etc/apache2/httpd.conf: Sezione Host virtuali

Per gestire più domini o nomi host su un computer fisico, è necessario utilizzare i container `VirtualHost` dichiarati nelle sezioni `Host virtuali` della configurazione. Per ulteriori dettagli sulla sintassi e le funzionalità degli host virtuali, vedere la Sezione 46.4, «Host virtuali» (p. 749).

46.3.3 Attivazione, avvio e arresto di Apache

Per attivare il server Web Apache all'avvio, utilizzare il runlevel editor di YaST. Per avviarlo, selezionare *Sistema → Servizi sistema (Runlevel)* in YaST. Andare alla voce*apache2*. Selezionare *Abilita* per avviare automaticamente Apache all'avvio della macchina. Gli utenti esperti possono utilizzare lo strumento `chkconfig` per avviare Apache all'avvio della macchina sulla riga di comando: `/sbin/chkconfig -a apache2`.

Per avviare o fermare Apache, utilizzare lo script `/usr/sbin/rcapache2` come `utente` root. `/usr/sbin/rcapache2` prende i seguenti parametri per avviare e fermare il server Web Apache:

`avvia`
Avvia il server Web Apache

`startssl`
Avvia il server Web Apache con il supporto SSL. Per informazioni relative alla configurazione di Apache con SSL, consultare sezione chiamata «Aggiunta del supporto SSL» (p. 740) e sezione chiamata «Secure Sockets Layer e Apache: `mod_ssl`» (p. 759).

`ferma`
Ferma il server Web Apache

`configtest`
Prova la configurazione di Apache senza fermare, avviare o riavviare il server Web. Poichè questa prova viene forzata ogni volta che viene avviato, ricaricato o riavviato il server, generalmente non è necessario eseguirla esplicitamente.

`riavvia`
Prima ferma e poi avvia di nuovo il server Web.

`try-restart`
Riavvia il servere Web se è in esecuzione.

restart-hup
Riavvia il server Web Apache inviandogli un segnale `SIGHUP`. Questa funzione non viene normalmente utilizzata.

graceful e ricarica
Ferma il server Web avvertendo tutti i processi Apache forked di terminare la loro richiesta prima di chiudere. Poichè ogni processo si blocca, viene sostituito da uno appena avviato, che risulta dal completo "riavvio" di Apache.

SUGGERIMENTO

`rcapache2 reload` è il metodo preferito per riavviare Apache in ambienti di produzione poichè consente a tutti i client di essere serviti senza provocare interruzioni alla connessione.

---

stato
Controlla lo stato di runtime del server Web Apache.

Esempio 46.7 *Output di esempio all'avvio e all'arresto di Apache*

```
tux@sun # rcapache2 status
Checking for httpd2:                                    non utilizzato

tux@sun # rcapache2 configtest
Syntax OK

tux@sun # rcapache2 start
Starting httpd2 (prefork)                               fatto

tux@sun # rcapache2 status
Checking for httpd2:                                    in esecuzione

tux@sun # rcapache2 start
Starting httpd2(graceful restart)                               fatto

tux@sun # rcapache2 status
Checking for httpd2:                                    in esecuzione
```

Un avvio non corretto o un mancato avvio in Apache potrebbero dare come risultato un file di configurazione malformato. Per il mancato avvio, potrebbero anche non essere visualizzati messaggi. Controllare sempre il log degli errori principale a ogni avvio e riavvio.

46.4 Host virtuali

Il termine *host virtuale* si riferisce alla capacità di Apache di servire diversi URI (universal resource identifiers) dalla stessa macchina fisica. Questo significa che, diversi domini, come www.example.com e www.example.net, vengono eseguiti da un solo server Web su una macchina fisica.

Generalmente si utilizzano host virtuali per risparmiare sui costi amministrativi (la manutenzione è limitata a un solo server Web) e di hardware (ogni dominio non richiede un server dedicato). Gli host virtuali possono essere basati sul nome, sull'IP o sulla porta.

Gli host virtuali possono essere configurati con YaST (vedi Host predefinito (p. 735)) o modificando manualmente la sezione `Host Virtuale` di `httpd.conf` (vedere la Sezione 46.3.2, «Configurazione manuale di Apache» (p. 741)).

Come predefinito, Apache in SUSE Linux viene preparato per un file di configurazione per host virtuale in `/etc/apache2/vhosts.d/`. Un modello di base per un host virtuale è fornito nella directory (`vhost.template`). La configurazione dell'host virtuale può anche essere aggiunta altrove, ad esempio in un file che è inserito nella configurazione.

IMPORTANTE

È molto utile controllare l'impostazione dell'host virtuale con il comando `httpd2 -S`. Questo comando emette le impostazioni dell'host virtuale come vengono comprese da Apache ed è in grado di assistere l'utente nell'ottenere i risultati desiderati. Se si utilizza Apache con flag come -DSSL, si devono utilizzare gli stessi flag durante il test, ad esempio `httpd2 -S -DSSL`.

46.4.1 Host virtuali basati sul nome

Con gli host virtuali basati sul nome, viene servito più di un sito web per indirizzo IP. Apache utilizza il campo host nell'intestazione HTTP inviato dal client per connettere la richiesta a una voce `ServerName` corrispondente di una delle dichiarazioni dell'host virtuale. Se non si trova nessun`ServerName`corrispondente, il primo`VirtualHost` specificato viene utilizzato come predefinito.

`NameVirtualHost` avvia la sezione`Host virtuale` in una configurazione Apache.

NameVirtualHost

`NameVirtualHost` dice al server Web Apache su quale indirizzo IP e, a scelta, quale porta ascoltare per le richieste da parte di client contenenti il nome di dominio nell'intestazione HTTP.

Il primo argomento può essere un nome di dominio completo, ma si consiglia di utilizzare l'indirizzo IP. Il secondo argomento è la porta ed è facoltativo. Come impostazione predefinita, viene utilizzata la porta 80 che è configurata tramite la direttiva`Ascolto` (Selezione dispositivo di rete (p. 733)).

Il carattere jolly `*` può essere utilizzato sia per l'indirizzo IP, sia per il numero della porta per ricevere le richieste su tutte le interfacce. Gli indirizzi IPv6 devono essere racchiusi tra parentesi quadre.

Esempio 46.8 *Variazioni delle voci VirtualHost basate sul nome*

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.1.100:80
NameVirtualHost 192.168.1.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:164::]:80
```

<VirtualHost></VirtualHost> in contesto basato sul nome

Il blocco `<VirtualHost></VirtualHost>` contiene le informazioni da applicare a un particolare dominio. Quando Apache riceve una richiesta da un client per un `VirtualHost` definito, utilizza le direttive allegate a questa sezione. È possibile utilizzare qualsiasi direttiva Apache consentita nel contesto `VirtualHost`. Il tag di apertura `VirtualHost`, nella configurazione di un host virtuale basato sul nome, prende i seguenti argomenti:

- Indirizzo IP (o nome di dominio completo) precedentemente dichiarato con la direttiva `NameVirtualHost`.

- Il numero di porta facoltativo precedentemente dichiarato con la direttiva `NameVirtualHost`.

Il carattere jolly * è ammesso anche come sostituto dell'indirizzo IP. Questa sintassi è valida solo in combinazione con l'utilizzo del carattere jolly in `NameVirtualHost *`. Quando si utilizzano gli indirizzi IPv6, l'indirizzo deve essere racchiuso tra parentesi quadre.

Esempio 46.9 *DirettiveVirtualHost basate sul nome*

```
<VirtualHost 192.168.0.20>
    ServerName www.example.com
    DocumentRoot /srv/www/htdocs/example.com
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com-error_log
    CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>

<VirtualHost 192.168.1.100:80>
    ServerName www.example.net
    DocumentRoot /srv/www/htdocs/example.net
    ServerAdmin webmaster@example.net
    ErrorLog /var/log/apache2/www.example.net-error_log
    CustomLog /var/log/apache2/www.example.net-access_log common
</VirtualHost>

<VirtualHost [2002:c0a8:164::]>
 # 2002:c0a8:164:: è l''indirizzo IPv6 equivalente a 192.168.1.100
    ServerName www.example.org
    DocumentRoot /srv/www/htdocs/example.org
    ServerAdmin webmaster@example.org
    ErrorLog /var/log/apache2/www.example.org-error_log
    CustomLog /var/log/apache2/www.example.org-access_log common
</VirtualHost>
```

In questo esempio, i domini www.example.com e www.example.net sono ospitati sulla macchina con l'indirizzo IP `192.168.1.100`. Il primo`VirtualHost` è predefinito per tutte le richieste in entrata al server Web.

Le direttive `ErrorLog` (descritta insezione chiamata «`ErrorLog` *`file | "|command"`* » (p. 745)) e `CustomLog` (vedere `http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog`) non devono contenere il nome di dominio. Qui utilizzare un nome a scelta.

46.4.2 Host virtuali basati su IP

Questa configurazione alternativa di host virtuali richiede la configurazione di più IP su una macchina. Un'istanza di Apache supporta l'hosting di diversi domini, a ognuno dei quali viene assegnato un IP diverso.

IMPORTANTE: Indirizzi IP e host virtuali basati su IP

Il server fisico deve avere un unico indirizzo IP per ciascuno degli host virtuali basati su IP. Se la macchina non dispone di più schede di rete, possono essere utilizzate interfacce di rete virutali (IP aliasing).

Configurazione dell'IP aliasing

Affinché Apache possa supportare l'hosting di più IP, la macchina fisica deve accettare richieste da più IP. Questo stato di fatto si chiama hosting multi-IP. Inoltre, l'IP aliasing deve essere attivato nel kernel. Questa è un'impostazione predefinita in SUSE Linux.

Una volta configurato il kernel per l'IP aliasing, pssono essere utilizzati i comandi `ifconfig` e `route` per configurare altri IP sull'host. Questi comandi devono essere eseguiti come utente `root`.

Nell'esempio seguente si presume che l'host abbia già l'IP `192.168.0.10` assegnato per il dispositivo di rete `eth0`. Digitare il comando `ifconfig` per visualizzare l'IP dell'host. Con i seguenti comandi possono essere aggiunti ulteriori indirizzi IP:

```
ip addr add 192.168.0.20/24 dev eth0
ip addr add 192.168.0.30/24 dev eth0
```

Tutti questi indirizzi IP sono assegnati allo stesso dispositivo di rete fisico (`eth0`).

`<VirtualHost></VirtualHost>` nel contesto basato su IP.

Una volta configurato l'IP aliasing sul sistema (oppure l'host è stato dotato di più schede di rete), Apache può essere configurato. Per ogni server virtuale è necessario un blocco `VirtualHost` separato.

L'esempio seguente mostra Apache in esecuzione su una macchina con l'IP `192.168.1.10`, che ospita due domini sugli IP aggiuntivi `192.168.0.20` e `192.168.0.30`. Quest esempio specifico funziona solo su una rete privata, poiché gli IP che vanno da `192.168.0.0` a `192.168.0.255` non vengono instradati sulla rete Internet pubblica.

Esempio 46.10 *Direttive VirtualHost basati su IP*

```
<VirtualHost 192.168.0.20>
    ServerName www.example.com
    DocumentRoot /srv/www/htdocs/example.com
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com-error_log
    CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>

<VirtualHost 192.168.0.30>
    ServerName www.example.net
    DocumentRoot /srv/www/htdocs/example.net
    ServerAdmin tux@example.net
    ErrorLog /var/log/apache2/www.example.net-error_log
    CustomLog /var/log/apache2/www.example.net-access_log common
</VirtualHost>
```

In questo esempio, le direttive `VirtualHost` sono specificate solo per le interfacce, anziché con `192.168.0.10`. Quando una direttiva `Listen` (descritta in Selezione dispositivo di rete (p. 733)) viene configurata anche per l'indirizzo `192.168.0.10`, deve essere creato un host vituale basato su IP per rispondere alle richieste HTTP effettuate a quella interfaccia oppure vengono applicate le direttive trovate nella sezione `Main Server` del file `/etc/apache2/httpd.conf` (vedere la sezione chiamata «Direttive di Apache in /etc/apache2/httpd.conf: Server principale » (p. 743)).

46.5 Moduli Apache

Il software Apache è basato su moduli: tutte le funzionalità eccetto alcuni task core sono gestite da moduli. Il software si è evoluto a tal punto che, anche l'HTTP viene elaborato da un modulo (http_core).

I moduli Apache possono essere compilati nel binario Apache al momento del build oppure caricati in modo dinamico al runtime. Per il caricamento al momento dell'esecuzione, consultare sezione chiamata «`LoadModule` *`module_identifier`*

/path/to/module » (p. 742) per il caricamento manuale dei moduli e Moduli (p. 734) per utilizzare YaST.

Apache in SUSE Linux viene fornito con i seguenti moduli disponibili in `apache2` RPM (prefix "mod_" omesso in questa sede): access, actions, alias, asis, auth, auth_anon, auth_dbm, auth_digest, auth_ldap, autoindex, cache, case_filter, case_filter_in, cern_meta, cgi, charset_lite, dav, dav_fs, deflate, dir, disk_cache, dumpio, echo, env, expires, ext_filter, file_cache, headers, imap, include, info, ldap, log_config, log_forensic, logio, mem_cache, mime, mime_magic, negotiation, proxy, proxy_connect, proxy_ftp, proxy_http, rewrite, setenvif, speling, ssl, status, suexec, unique_id, userdir, usertrack, and vhost_alias. Inoltre, SUSE Linux fornisce i seguenti moduli Apache come pacchetti RPM che devono essere installati separatamente: `apache2-mod_auth_mysql`, `apache2-mod_fastcgi`, `apache2-mod_macro`, `apache2-mod_murka`, `apache2-mod_perl`, `apache2-mod_php4`, `apache2-mod_php5`, `apache2-mod_python`, and `apache2-mod_ruby`.

Alcuni di questi moduli sono documentati in modo più dettagliato in questa sezione. Per una descrizione degli altri moduli presenti nella distribuzione di base, visitare il sito web Apache Modules Web all'indirizzo `http://httpd.apache.org/docs-2.0/mod/`. Per i moduli di terzi, consultare `http://modules.apache.org/`.

I moduli Apache possono essere suddivisi in tre diverse categorie: moduli base, moduli di estensione e moduli esterni.

46.5.1 Moduli di base

I moduli di base vengono compilati in Apache per impostazione predefinita. Questi sono disponibili a meno che non altrimenti specificato in modo esplicito in fase di generazione. In SUSE Linux Apache dispone solo dei moduli di base minimi compilati. Tuttavia, sono tutti disponibili come *oggetti condivisi*: anzichè essere inclusi nel binario stesso `/usr/sbin/httpd2`, è possibile includerli in fase di esecuzione configurando `APACHE_MODULES` in `/etc/sysconfig/apache2`.

Server-Side Includes con `mod_include`

`mod_include` fornisce uno strumento per l'elaborazione dei file prima che i dati vengano inviati al client. Generalmente, `mod_include` viene utilizzato per includere

in un documento i file che vengono analizzati nel formato HTML prima di raggiungere il client. Questo è il motivo per cui allo strumento è stato assegnato il nome Server-Side Includes (SSI).

Con gli SSI vengono eseguiti speciali comandi sul server, attivati da commenti SGML formattati. Questi comandi SGML sono caratterizzati dalla sintassi seguente:

```
<!--#element attribute=value -->
```

Per un elenco dei valori di un *elemento* e un *attributo*, vedere la documentazione di mod_include in http://httpd.apache.org/docs-2.0/mod/mod_include.html.

Per utilizzare `mod_include` in SUSE Linux, aggiungere `include` a `APACHE_MODULES` in `/etc/sysconfig/apache2` oppure utilizzare YaST come descritto in Moduli (p. 734).

SUGGERIMENTO

Utilizzare la direttiva `XBitHack` (http://httpd.apache.org/docs-2.0/mod/mod_include.html#xbithack) per indicare ad Apache di analizzare i file con il set di bit `execute` per le direttive SSI.

Ciò significa che anzichè dover cambiare l'estensione di un file per contrassegnarlo come elemento SSI (`.shtml` nell'esempio sopra menzionato), è possibile utilizzare un file `.html` normale ed eseguire `chmod +x myfile.html`.

CGI (Common Gateway Interface): `mod_cgi`

`mod_cgi` consente ad Apache di inviare il contenuto creato da programmi o script CGI ("Common Gateway Interface") esterni. Agisce ad esempio tra un linguaggio di programmazione disponibile sul computer fisico e il server Web Apache. Gli script CGI sono supportati in teoria da tutti i linguaggi di programmazione. Tuttavia, vengono generalmente utilizzati linguaggi quali `Perl` o `C`. `mod_cgi` è il metodo più utilizzato per includere contenuto dinamico in un sito Web.

Nella programmazione CGI, a differenza di quella "normale", i programmi e gli script CGI devono essere in grado di generare un tipo MIME `Content-type: text/html` per produrre l'output in HTML.

Esempio 46.11 *Semplice script CGI in Perl*

```
#!/path/to/perl
print "Content-type: text/html\n\n";
print "Hello, World.";
```

La differenza tra i moduli associati specificamente a un linguaggio di programmazione, ad esempio `mod_php5`) e `mod_cgi` consiste nella possibilità di combinare `mod_cgi` con `mod_suexec` (vedere la sezione chiamata «Esecuzione di CGI come altro utente con `mod_suexec` » (p. 757)). Questa combinazione consente di eseguire gli script CGI con uno specifico ID utente. Generalmente, gli script che utilizzano `mod_cgi` da solo oppure `mod_php5` vengono eseguiti con l'ID utente di Apache (di default in SUSE Linux: `wwwrun`). I moduli progettati per un determinato linguaggio di programmazione (ad esempio `mod_php5` o `mod_ruby`) integrano un interprete persistente in Apache per l'esecuzione degli script con l'utente ID di Apache.

Di conseguenza, l'utilizzo dei CGI con `mod_suexec` semplifica le operazioni di amministrazione dal momento che i processi CGI possono essere assegnati a singoli utenti anzichè al server Web stesso. Questa combinazione garantisce inoltre una maggiore sicurezza del file system: lo script eredita solo i diritti del file system dell'utente. Nel caso dei moduli, invece, allo script vengono assegnati i permessi per i file relativi all'utente del server Web, con il rischio che vengano accidentalmente visualizzati i dati nel file system.

I processi CGI vengono conclusi al termine della richiesta di un client sul server Web. Pertanto, i CGI non sono persistenti e, una volta conclusi, rilasciano tutte le risorse occupate. Ciò rappresenta un vantaggio soprattutto in caso di errori di programmazione. Nei moduli l'interprete è persistente, quindi gli effetti degli errori possono accumularsi con il rischio che non sia più possibile rilasciare risorse quali le connessioni a un database. Potrebbe anche essere necessario riavviare Apache.

Per utilizzare `mod_cgi` in SUSE Linux, aggiungere `cgi` ad `APACHE_MODULES` in `/etc/sysconfig/apache2` oppure utilizzare YaST come descritto in Moduli (p. 734). In SUSE Linux la directory predefinita per gli elementi CGI è `/srv/www/cgi-bin/`.

Se si desidera modificare manualmente un file di configurazione Apache, utilizzare l'esempio seguente come linea guida per la configurazione di `mod_cgi`.

Esempio 46.12 *Attivazione manuale di mod_cgi*

```
# Global Environment
LoadModule cgi_module /path/to/mod_cgi.so

# Main Server and/or Virtual Host and/or
# Directory and/or .htaccess context
AddHandler cgi-script .cgi .pl

# Main Server and/or Virtual Host context
ScriptAlias /cgi-bin/ /srv/www/cgi-bin/

# Alternatively, explicitly allow CGI scripts in a directory
# Main Server and/or Virtual Host context
<Directory /srv/www/some/dir>
    Options +ExecCGI
<Directory>
```

46.5.2 Moduli di estensione

I moduli etichettati come estensioni sono inclusi nel pacchetto di programmi Apache ma non vengono generalmente compilati staticamente sul server. In SUSE Linux queste estensioni sono disponibili come oggetti condivisi caricabili in Apache in fase di esecuzione.

Esecuzione di CGI come altro utente con `mod_suexec`

`mod_suexec` consente, insieme a `mod_cgi` (sezione chiamata «CGI (Common Gateway Interface): `mod_cgi` » (p. 755)), di eseguire gli script CGI come un utente e un gruppo specificati. A questo scopo, viene utilizzato il programma suEXEC in `/usr/sbin/suexec2`. Si tratta di un wrapper chiamato da Apache a ogni esecuzione di un programma o di uno script CGI. Sia il wrapper che il programma ricevono l'ID assegnato all'utente e al gruppo configurati. Tale ID vene quindi eseguito come utente o gruppo configurato.

Benché questo metodo riduca significativamente i rischi di sicurezza tipici degli script CGI generati dagli utenti, occorre tenere in considerazione alcuni importanti fattori illustrati di seguito.

Considerazioni sull'utilizzo di suEXEC

- `suEXEC docroot`: tutti gli script vengono eseguiti solo in questa directory di base. Pertanto, l'esecuzione degli script con suexec all'esterno della directory `docroot` non è consentita e genera un errore. `docroot` viene impostato durante la compilazione di `suEXEC` e non può essere modificato nella fase di esecuzione. In SUSE Linux la directory predefinita è `/srv/www`.

- `uidmin` rappresenta l'ID minimo che deve essere assegnato a un utente affinché quest'ultimo possa essere utilizzato per eseguire gli script con `suEXEC`. Ciò impedisce che gli script possano essere eseguiti come utenti di sistema, ad esempio come utente `root`. Non creare utenti con ID inferiori ai valori di `uidmin` se tali utenti dovranno essere utilizzati con `mod_suexec`. In SUSE Linux il valore `uidmin` predefinito è pari a 96.

- `gidmin`: equivale a `uidmin` ma per l'ID di gruppo. In SUSE Linux il valore `gidmin` predefinito corrisponde a 96.

- Permessi per file e directory. Lo script in questione deve appartenere allo stesso utente e allo stesso gruppo così come specificato per l'utente e il gruppo `suEXEC`. Inoltre, sia il file che la directory di residenza devono poter essere scritti solo dal proprietario.

- `suEXEC safepath`. Tutti i programmi utilizzati in uno script, quale Perl, devono risiedere nei percorsi contrassegnati come sicuri per suexec. `safepath` viene impostato a livello di compilazione `suEXEC` e non può essere modificato in fase di esecuzione. In SUSE Linux il percorso `safepath` predefinito è `/usr/local/bin:/usr/bin:/bin`.

In caso di errori provocati da `mod_suexec`, consultare il file di log suexec in `/var/log/apache2/suexec.log`.

Per utilizzare `mod_suexec` in SUSE Linux, aggiungere `suexec` a `APACHE_MODULES` in `/etc/sysconfig/apache2` oppure utilizzare YaST come descritto in Moduli (p. 734). Non dimenticare che per eseguire suexec, è necessario `mod_cgi`.

mod_suexec è più utile in un ambiente host virtuale come descritto nella Sezione 46.4, «Host virtuali» (p. 749). Per specificare un gruppo e un utente specifici per l'esecuzione degli script CGI, immettere la sintassi seguente nel file che contiene le dichiarazione dell'host virtuale (in SUSE Linux il file predefinito è /etc/apache2/vhosts.d/*):

Esempio 46.13 *mod_suexec Configurazione*

```
<VirtualHost 192.168.0>
# ...
ScriptAlias /cgi-bin/ /srv/www/vhosts/www.example.com/cgi-bin/
SuexecUserGroup tux users
# ...
</VirtualHost>
```

La sintassi SuexecUserGroup *username group* dell'esempio assegna a tutti gli script che risiedono in /srv/www/vhosts/www.example.com/cgi-bin/ l'ID utente del pinguino Tux e all'ID del gruppo di utenti.

Secure Sockets Layer e Apache: mod_ssl

mod_ssl fornisce una cifratura avanzata mediante l'utilizzo dei protocolli Secure Sockets Layer (SSL) e Transport Layer Security (TLS) per le comunicazioni HTTP tra un client e il server Web. A questo scopo, prima di rispondere a una richiesta di un URL, il server invia un certificato SSL con le informazioni che dimostrano la validità dell'identità del server. Ciò garantisce anche che il server rappresenti esclusivamente il punto finale corretto per la comunicazione. Inoltre, il certificato genera una connessione cifrata tra il client e il server che può trasportare le informazioni senza il rischio di esporre il contenuto in testo normale riservato. L'effetto più visibile derivante dall'utilizzo di mod_ssl con Apache è che gli URL presentano il prefisso https:// anzichè http://.

La porta predefinita per le richieste SSL e TLS sul server Web è la 443. I dati possono essere ricevuti sia sulla porta «normale» 80, che sulla porta SSL/TLS 443, senza il rischio di conflitti. Infatti è possibile eseguire connessioni HTTP e HTTPS nella stessa istanza di Apache. Per inviare le richieste alle porte 80 e 443 su server virtuali separati, viene generalmente utilizzato un host virtuale (vedere la Sezione 46.4, «Host virtuali» (p. 749).

IMPORTANTE: SSL e host virtuali basati sui nomi

Non è possibile eseguire più host virtuali SSL su un server con un solo indirizzo IP. Gli utenti che tentano di collegarsi al server riceveranno un messaggio di avviso che indica che il certificato non corrisponde al nome del server ogni volta che visitano l'URL. Per il buon esito di una comunicazione basata su un certificato SSL valido, è necessaria una porta o un indirizzo IP distinto per ciascun dominio SSL.

In questo questo caso, anzichè un messaggio di avviso si otterrà lo stesso livello di cifratura di un sito SSL valido. Ciò significa che finché il messaggio di avviso è soddisfacente, la comunicazione tra il server Web e il client è ancora sicura. Non è quindi più necessario conoscere in maniera esclusiva l'identità del server, la quale è garantita da un certificato SSL valido.

Per attivare `mod_ssl` in SUSE Linux, aggiungere `ssl` a `APACHE_MODULES` in `/etc/sysconfig/apache2` oppure utilizzare YaST come descritto in Moduli (p. 734). Inoltre, è necessario configurare il server Web in modo che riceva i dati sulla porta HTTPS standard 443. È possibile eseguire questa operazione manualmente in `/etc/apache2/listen.conf` oppure in YaST mediante la voce di menu *Listen (Ascolta)* (vedere Selezione dispositivo di rete (p. 733)).

È possibile creare un certificato SSL di verifica immettendo `cd /usr/share/doc/packages/apache2; ./certificate.sh` come utente `root`. Per creare il certificato SSL, seguire le istruzioni visualizzate sullo schermo. I file di certificato risultanti vengono archiviati nelle directory `/etc/apache2/ssl*`.

Per ottenere un certificato «effettivo» con validità globale, contattare gli appositi fornitori, tra cui Thawte (`http://www.thawte.com/` o Verisign (`www.verisign.com`).

Se si desidera modificare manualmente un file di configurazione Apache, utilizzare l'esempio seguente come linea guida per la configurazione di `mod_ssl`.

Esempio 46.14 *Configurazione manuale di mod_ssl*

```
# Global Environment
# listen on the standard SSL port
Listen 443
# load module only if rcapache2 start-ssl was issued
<IfDefine SSL>
LoadModule ssl_module /path/to/mod_ssl.so
</IfDefine>

# Main Server context
# include global (server-wide) SSL configuration
# that is not specific to any virtual host
# only if ssl_module was loaded
<IfModule mod_ssl.c>
Include /etc/apache2/ssl-global.conf
</IfModule>
```

SUGGERIMENTO

Non dimenticare di aprire il firewall per la connessione Apache SSL sulla porta 443. Questa operazione può essere esegua mediante YaST selezionando *Security and Users (Sicurezza e utenti)* → *Firewall (Firewall)* → *Allowed Services (Servizi consentiti)*. Quindi aggiungere *HTTPS Server (Server HTTPS)* all'elenco dei *Allowed Services (Servizi consentiti)*.

46.5.3 Moduli esterni

Ufficialmente, i moduli marcati come esterni non sono compresi nella distribuzione Apache. In ogni caso, SUSE Linux ne fornisce diversi disponibili per l'uso. Questo capitolo riporta una breve spiegazione dei moduli esterni e delle loro funzionalità.

Uso di Perl per gestire Apache: `mod_perl`

`mod_perl` ha un interprete Perl permanente incorporato in Apache. Questo evita l'overhead provocato da`mod_cgi` che chiama un eseguibile esterno su ogni richiesta a un CGI. `mod_perl` consente inoltre di controllare molti aspetti della funzionalità Apache con l'ausilio del linguaggio di programmazione Perl.

Per utilizzare `mod_perl` in SUSE Linux, installare l'RPM `apache2-mod_perl` e attivare il modulo tramite YaST (Moduli (p. 734)) o manualmente in`/etc/sysconfig/apache2`. Dopo l'installazione e l'attivazione, un file di configurazione

separato, mod_perl.conf, viene messo in/etc/apache2/conf.d/. Inoltre, lo script di avvio mod_perl viene installato come mod_perl-startup.pl. Per ulteriori informazioni sull'utilizzo del modulo, consultare la documentazione disponibile sul sito Web di mod_perl (http://perl.apache.org/).

PHP: mod_php4, mod_php5

PHP è un linguaggio di programmazione noto originariamente predisposto per l'utilizzo sul Web. Esiste nelle versioni PHP4 e PHP5. Mentre PHP4 rappresenta il classico concetto di PHP e l'approccio a quest'ultimo, PHP5 ha introdotto nuove possibilità di programmazione orientate agli oggetti e molte altre caratteristiche avanzate. mod_php4 e mod_php5 sono entrambi disponibili in SUSE Linux. Hanno un interprete PHP incorporato in Apache come modulo permanente.

Per utilizzaremod_php4 o mod_php5 in SUSE Linux, installare il rispettivo RPM (apache2-mod_php4, apache2-mod_php5) e attivare il modulo tramite YaST (Moduli (p. 734)) o manualmente in /etc/sysconfig/apache2.

Dopo l'installazione e l'attivazione, un file di configurazione separato per il rispettivo modulo (php4.conf o php5.conf) viene collocato in /etc/apache2/conf.d/. Il sito Web di PHP (http://www.php.net) è una risorsa eccellente per l'utilizzo di Apache con PHP.

Python e Apache: mod_python

mod_python ha un interprete Python permanente incorporato in Apache. Python è un linguaggio di programmazione orientato agli oggetti con una sintassi molto chiara e leggibile. Una caratteristica insolita ma conveniente è data dal fatto che la struttura del programma dipende dal rientro del codice sorgente anziché dagli elementi di demarcazione regolari come begin ed end.

Per utilizzare mod_python in SUSE Linux, installare l'RPM apache2-mod_python e attivare il modulo tramite YaST (Moduli (p. 734)) o manualmente in /etc/sysconfig/apache2. Per ulteriori informazioni sull'utilizzo del modulo, consultare la documentazione disponibile sul sito Web di mod_python (http://www.modpython.org/).

L'interprete Ruby in Apache: mod_ruby

mod_ruby ha l'interprete Ruby incorporato nel server Web Apache e consente l'esecuzione degli script CGI Ruby in modo nativo. Ruby è un linguaggio di programmazione orientato agli oggetti relativamente nuovo e di livello elevato che, per certi aspetti, assomiglia a Perl e a Python. Come Python, ha una sintassi pulita e trasparente. Ruby ha però adottato abbreviazioni (ad esempio `$.r` come numero dell'ultima riga letta nel file di input) apprezzate da alcuni programmatori e malviste da altri. Il concetto di base di Ruby assomiglia molto a quello di Smalltalk.

Per utilizzare mod_ruby in SUSE Linux, installare l'RPMapache2-mod_ruby e attivare il modulo tramite YaST (Moduli (p. 734)) o manualmente in/etc/sysconfig/apache2. Per ulteriori informazioni sull'utilizzo del modulo, consultare la documentazione disponibile sul sito Web di mod_ruby(http://www.modruby.net/en/index.rbx).

Accesso a file system nativi: mod_dav

mod_dav fornisce la funzioanlità WebDAV (Web-Based Distributed Authoring and Versioning) per Apache. WebDAV è un'estensione del protocollo HTTP che consente agli utenti di modificare e gestire in modo collaborativo file su server remoti. Le capacità di WebDAV sono analoghe a quelle di FTP con la differenza principale che HTTP viene utilizzato come protocollo sottostante per l'accesso al server. In effetti, mod_dav rende un server Web Apache un file system remoto avanzato.

È buona norma, se non richiesto, limitare l'accesso alle directory disponibili tramite WebDAV. Le precauzioni minime da prendere consistono nell'impostazione dell'autenticazione di base HTTP per la risorsa WebDAV, insieme alle clausole Limite all'interno della direttivaLocation.

Per accedere a una risorsa WebDAV, deve essere presente un software WebDAV sul lato client. SUSE Linux è già dotato delle capacità WebDAV: Per il collegamento a un file system WebDAV Apache, è possibile utilizzareKonqueror con il prefissowebdav:// owebdavs:// (per WebDAV tramite connessioni SSL).

Per mod_dav è necessario disporre del modulo mod_dav_fs, che fornisce l'accesso per WebDAV al file system effettivo. Per utilizzaremod_dav in SUSE Linux, attivare il modulo tramite YaST (Moduli (p. 734)) o manualmente in/etc/sysconfig/apache2. Eseguire la stessa operazione per mod_dav_fs. Per ulteriori informazioni

sull'utilizzo del modulo, consultare la documentazione disponibile sul sito Web di mod_dav(http://httpd.apache.org/docs-2.0/mod/mod_dav.html).

Offerta di pagine home utente: mod_userdir

mod_userdir in SUSE Linux non prevede l'offerta dei contenuti della cartella ~/public_html di ciascun utente come pagine Web pubbliche. L'URL per accedere a queste pagine si trova quindi in http://www.example.com/~*nome utente*/.

SUGGERIMENTO

Per motivi di sicurezza mod_userdir in SUSE Linux proibisce l'accesso a qualsiasi directory della directory home dell'utente root. È possibile inoltre consentire a certi utenti in particolare di avere home page pubbliche con:

```
# Main server context
UserDir disabled
UserDir enabled tux
    wilber
```

Per utilizzare mod_userdir in SUSE Linux, attivare il modulo tramite YaST (Moduli (p. 734)) o manualmente in/etc/sysconfig/apache2. Per ulteriori informazioni sull'utilizzo del modulo, consultare la documentazione disponibile sul sito Web di mod_userdir(http://httpd.apache.org/docs-2.0/mod/mod_userdir.html).

Modifica del layout dell'URL: mod_rewrite

mod_rewrite viene spesso definito «il coltellino svizzero della manipolazione dell' URL.» mod_rewrite riscrive immediatamente gli URL richiesti in base a una specifica regola impostata. Generalmente il risultato è analogo ahttp://www.example.com/2/1/de per http://www.example.com/display.php?cat=2&article=1&lang=de.

L'URL Rewriting Guide spiega i vantaggi e gli svantaggi di questo modulo potente, ma complesso:

«Con mod_rewrite o ci si tira la zappa sui piedi la prima volta che lo si usa e poi mai più, o lo si ama per sempre data la sua potenza. »

I set di`RewriteRule`possono essere impostati in tutti i contesti di configurazione: per il server principale, per gli host virtuali, per le directory e per i file `.htaccess`. Un buon punto di partenza per la riscrittura degli URL con`mod_rewrite` è la URL Rewriting Guide sul sito http://httpd.apache.org/docs-2.0/misc/rewriteguide.html.

Per utilizzare `mod_rewrite` in SUSE Linux, attivare il modulo tramite YaST (Moduli (p. 734)) o manualmente in`/etc/sysconfig/apache2`.

46.6 Sicurezza

Un server Web accessibile pubblicamente via Internet richiede uno lavoro di amministrazione continuativo. È inevitabile che si verifichino problemi di sicurezza, sia relativi al software, sia a un'accidentale errata configurazione. Di seguito sono riportati alcuni suggerimenti per la gestione di questi problemi.

Tenersi aggiornati

In caso vengano trovati punti di vulnerabilità nel software Apache, SUSE pubblicherà un avviso di sicurezza. Questo avviso contiene istruzioni per la correzione dei punti di vulnerabilità, che dovranno essere messe in opera appena possibile. All'indirizzo http://www.suse.com/us/private/support/online_help/mailinglists/, è disponibile una mailing list di annunci di sicurezza SUSE. Le informazioni più recenti sui problemi di sicurezza per i pacchetti SUSE Linux sono disponibili anche online all'indirizzo http://www.novell.com/linux/security/securitysupport.html.

Inoltre, è consigliabile iscriversi alla mailing list di annunci Apache (http://httpd.apache.org/lists.html#http-announce) dove vengono pubblicate nuove versioni e correzioni di bug.

Autorizzazioni DocumentRoot

In SUSE Linux, la directory `DocumentRoot` che si trova in `/srv/www/htdocs` e la directory CGI `/srv/www/cgi-bin` appartengono di default all'utente `root`. Non è consigliabile modificare queste autorizzazioni. Se le directory fossere scrivibili per tutti, qualsiasi utente potrebbe aggiungervi dei file. Questi file potrebbero essere eseguiti da Apache con le autorizzazioni di `wwwrun` che darebbero all'utente l'accesso non desiderato alle risorse dei file system. Utilizzare le sottodirectory di `/srv/www/htdocs` e `/srv/www/cgi-bin` per organizzare i dati dell'utente

o quelli specifici del dominio in combinazione con la direttiva `Directory` (vedere Directory (p. 736)).

Directory CGI e SSI
Gli script interattivi in Perl, PHP, SSI o qualsiasi altro linguaggio di programmazione possono eseguire essenzialmente comandi arbitrari. Per ridurre il rischio è opportuno limitare l'esecuzione di CGI e SSI (vedere la sezione chiamata «CGI (Common Gateway Interface): `mod_cgi` » (p. 755), ScriptAlias (p. 737) e sezione chiamata «Server-Side Includes con `mod_include` » (p. 754)) a directory specifiche, anziché consentirne l'esecuzione dappertutto.

Un'altra possibilità è lavorare con il modulo `mod_suexec` (vedere la sezione chiamata «Esecuzione di CGI come altro utente con `mod_suexec` » (p. 757)) per le CGI in generale. Per i moduli Apache, una configurazione che tiene in grande considerazione la sicurezza per gli interpreti, come in sezione chiamata «PHP: `mod_php4`, `mod_php5` » (p. 762), aiuta a mantenere sicuro l'ambiente Web.

Autorizzazioni di accesso
Molto spesso, specialmente in ambienti di prova, le autorizzazioni di accesso a un server Web sono gestite in maniera casuale, proprio per la natura stessa della prova di una configurazione. Questo può provocare la rivelazione accidentale di informazioni sensibili o addirittura l'esposizione di un intero server al pubblico sbagliato. Per consentire l'accesso a determinati siti Web solo a utenti o client specifici, utilizzare la direttiva `Order` (`http://httpd.apache.org/docs-2.0/mod/mod_access.html#order`) insieme con i file `.htaccess` (vedere la sezione chiamata «`AccessFileName` *`nomi file`* » (p. 745)).

Inoltre, è possibile utilizzare l'approccio «security by obfuscation (sicurezza tramite offuscamento)»: un esempio tipico di questo approccio è l'esecuzione di Apache su un porta non standard (vedere Selezione dispositivo di rete (p. 733)). Si avrà di conseguenza un'URL con la porta aggiunta alla fine, ad esempio `http://www.example.com:8765`, che è un compromesso accettabile in ambienti di prova.

46.7 Soluzione dei problemi

Se Apache non si avvia, la pagina Web non è accessibile, o gli utenti non riescono a collegarsi al server Web, è importante trovare la causa del problema. Qui di seguito

sono riportati alcune posizioni tipiche nelle quali cercare spiegazioni di errori e verifiche importanti da effettuare.

In primo luogo, `rcapache2` (descritto nell Sezione 46.3.3, «Attivazione, avvio e arresto di Apache» (p. 747)) è prolisso per quanto riguarda gli errori, può essere quindi utile se viene effettivamente utilizzato per far funzionare Apache. A volte si è tentati di utilizzare il binario `/usr/sbin/httpd2` per avviare o fermare il server Web. Evitarlo e utilizzare invece `lo script`rcapache2. `rcapache2` fornisce anche consigli e suggerimenti per risolvere gli errori di configurazione.

In secondo luogo, l'importanza dei file di log (vedere la sezione chiamata «File di log» (p. 731)) non può essere esagerata. In caso di errori irreversibili o meno, i file di log di Apache rappresentano il posto giusto dove ricercare le cause. Inoltre, è possibile verificare la prolissità dei messaggi registrati con la direttiva `LogLevel` (vedi sezione chiamata «`LogLevel` *`livello`* » (p. 746)) se nei file di log sono necessari maggiori dettagli.

SUGGERIMENTO

Consultare i messaggi di log di Apache con il comando `tail -F /var/log/apache2/*_log &`. Quindi eseguire `rcapache2 restart`. A questo punto, cercare di collegarsi a un browser e verificare l'output.

Un errore comune è quello di non aprire le porte per Apache nella configurazione del firewall del server. Se si configura Apache con YaST, esiste un'opzione separata disponibile per questo problema specifico.

Se non si riesce a rintracciare l'errore con l'ausilio di quanto sopraccitato, consultare l'Apache bug database online al seguente indirizzo`http://httpd.apache.org/bug_report.html`. È possibile inoltre contattare la comunità degli utenti Apache tramite una mailing list disponibile all'indirizzo `http://httpd.apache.org/userslist.html`. Un newsgroup consigliato è `comp.infosystems.www.servers.unix`.

46.8 Per ulteriori informazioni

Apache è un server Web ampiamente utilizzato. Di conseguenza, esistono molti siti Web che offrono supporto e assistenza su Apache con livelli qualitativi differenti. In

ogni caso, il punto di partenza per qualsiasi ricerca relativa ad Apache e alle sue possibilità dovrebbe essere `http://httpd.apache.org/docs-2.0/`.

Il pacchetto RPM `apache2-doc` contiene inoltre il manuale di Apache per l'installazione locale e come riferimento. Per alcuni suggerimenti di configurazione specifici per SUSE, il file `/usr/share/doc/packages/apache2` contiene un riferimento rapido.

Il pacchetto RPM `apache2-example-pages` contiene alcune pagine di esempio per Apache che riportano informazioni relative al server Web.

46.8.1 Moduli Apache

Ulteriori informazioni sui moduli esterni di Apache da Sezione 46.5.3, «Moduli esterni» (p. 761) sono disponibili nelle seguenti posizioni:

- `httpd.apache.org/docs-2.0/mod/`
- `http://www.php.net/manual/en/install.unix.apache2.php`
- `http://www.modpython.org/`
- `http://www.modruby.net/`
- `http://perl.apache.org/`

46.8.2 CGI

Per ulteriori informazion circa l'utilizzo di `mod_cgi` (vedere la sezione chiamata «CGI (Common Gateway Interface): `mod_cgi` » (p. 755)) e la programmazione di CGI è disponibile nelle seguenti posizioni:

- `http://www.modperl.com/`
- `http://www.modperlcookbook.org/`
- `http://www.fastcgi.com/`
- `http://www.boutell.com/cgic/`

46.8.3 Sorgenti vari

Qualora si incontrassero difficoltà particolari di Apache in SUSE Linux, consultare il SUSE Support Database su http://portal.suse.com/sdb/en/index.html.

La storia di Apache è reperibile su http://httpd.apache.org/ABOUT_APACHE.html. Questa pagina spiega inoltre perchè il server si chiama Apache.

Informazioni relative all'aggiornamento dalla versione 1.3 alla 2.0 sono disponibili su http://httpd.apache.org/docs-2.0/en/upgrading.html.

47 Sincronizzazione dei file

Oggi sono in tanti a utilizzare ed a lavorare con più di un computer. Spesso se ne ha uno a casa, uno o più di uno al lavoro ed eventualmente anche un portatile o PDA che si utilizza durante gli spostamenti. Molti file dovranno essere disponibili su tutti quanti i computer con i quali si lavora per poterli elaborare, e chiaramente tutti i dati dovranno essere disponibili nella versione aggiornata su ogni sistema.

47.1 Software per la sincronizzazione dei dati

Nel caso di computer che compongono i singoli nodi di una rete veloce, la sincronizzazione dei dati non rappresenta un problema. Basta selezionare un file system di rete, per esempio NFS e salvare i file su un server. I vari computer accederanno in seguito tramite la rete agli stessi e identici dati depositati sul server. Questo approccio diventa improponibile nel caso di una rete molto lenta o nel caso di connessione saltuaria. Chi usa un laptop durante i suoi spostamenti necessità delle copie dei file da elaborare sul proprio disco rigido locale. Non appena però si inizia a modificare i file si presenta il problema della sincronizzazione. Se si modifica un file su un computer si deve badare assolutamente ad aggiornare la copia del file su tutti gli altri computer. Se si tratta di un fatto sporadico questo si lascia realizzare comodamente a mano con i comandi scp o rsync. Nel caso di numerosi file il tutto diventa già un po' più laborioso e richiede molta attenzione per evitare che si sovrascriva ad esempio un file nuovo con la vecchia versione.

AVVERTIMENTO: Occhio alla perdita di dati

In ogni caso bisogna sapere usare bene il programma impiegato e testare le sue funzionalità prima di amministrare i propri dati tramite un sistema di sincronizzazione. La copia di sicurezza è ed resta irrinunciabile per file importanti.

Per risparmiarsi queste procedure laboriose che richiedono tanto tempo prezioso e sono esposte ad errori vi è del software che seguendo approcci diversi automatizza questo processo. La seguente breve introduzione intende solamente dare all'utente un'idea del modo di funzionare di questi programmi e di come adoperarli. Prima di utilizzarli effettivamente consigliamo di leggere attentamente la documentazione relativa.

47.1.1 Unison

Unison non è un file system di rete. I file vengono editati e salvati in locale. Si può richiamare il programma manualmente per sincronizzare i file. La prima volta che si esegue il processo di sincronizzazione viene creata una banca dati su entrambi i sistemi coinvolti nella quale vengono memorizzate le somme di controllo, la data ed i permessi dei file selezionati. Alla prossima chiamata, unison è in grado di riconoscere i file che hanno subito delle modifiche e ne propone la trasmissione da un sistema all'altro. Solitamente potrete accettare tranquillamente le proposte di unison.

47.1.2 CVS

Impiegato soprattutto per l'amministrazione di varie versioni di sorgenti di programmi, CVS consente di avere delle copie dei file su diversi computer. In questo senso è adatto anche al nostro scopo. Il CVS ha un database centrale chiamato repository, che risiede sul server, ed il quale memorizza non solo i file ma anche le singole modifiche apportate ai file. Quando le modifiche eseguite in locale vengono immesse nel database, si parla di commit, le quali potranno essere scaricate dagli altri computer (update). Entrambi i processi vengono eseguiti dall'utente.

Inoltre CVS è tollerante nei confronti di errori riguardanti le modifiche effettuate da diversi computer: le modifiche vengono raccolte e solo se vi sono delle modifiche che interessano la stessa riga di un documento o file sorge un conflitto. Il database, in caso

di un conflitto, resta comunque in uno stato consistente; il conflitto è visibile solo sul client e solamente da lì risolvibile.

47.1.3 subversion

Al contrario di CVS che è «cresciuto» con il tempo, nel caso di subversion ci troviamo di fronte ad un progetto portato avanti sin dal principio in modo consistente. subversion è stato concepito per sostituirsi a CVS.

subversion presenta una serie di migliorie rispetto al suo predecessore. CVS è in grado di amministrare solo file e «ignora» le directory. subversion invece offre uno storico anche per le directory che potranno essere copiate e rinominate alla stregua di file. Inoltre, è possibile aggiungere per ogni file e directory dei metadati relativi ad una determinata versione del file o directory. A differenza di CVS, subversion consente un accesso di rete transparente grazie a dei propri protocolli come ad esempio WebDAV (Web-based Distributed Authoring and Versioning) che estende le funzionalità del protocollo HTTP fino a permettere accessi simultanei in scrittura su file residenti su server Web remoti.

subversion è stato realizzato in prima linea ricorrendo a pacchetti di applicazioni già esistenti. Infatti subversion utilizza il server Web Apache e l'estensione WebDAV.

47.1.4 mailsync

A differenza dei tool di sincronizzazione finora menzionati, Mailsync sincronizza solo e-mail di caselle diverse. Si può trattare sia di e-mail nella mail box locale che di mail box che risiedono su un server IMAP.

Per ogni messaggio viene deciso sulla base del message id, contenuto nell'intestazione della e-mail, se cancellarlo o sincronizzarlo. E' possibile sincronizzare sia singole mail box che gerarchie di mail box.

47.1.5 rsync

Se non vi occorre un'applicazione che vi permetta di controllare le singole versioni ed intendete sincronizzare vasti alberi di file tramite connessioni di rete lente, allora potete ricorrere al tool rsync. rsync dispone di meccanismi particolari che consentono di

trasmettere solo le modifiche apportate ai file, siano essi file di testo oppure dei binari. Per rilevare le differenze tra i file, rsync suddivide i file in blocchi e ne calcola la somma di controllo.

Però il rilevamento delle modifiche ha il suo prezzo. rsync richiede tra l'altro tanta RAM.

47.2 Criteri per scegliere il programma giusto

47.2.1 Client-server vs. peer-to-peer

Per la sincronizzazione dei dati si sono diffusi due modelli. Nel primo caso vi è un server centrale in base al quale i client sincronizzano i loro file. I client dovranno potersi collegare via rete almeno temporaneamente al server. Questo modello è quello utilizzato da subversion, CVS e WebDAV

L'alternativa è rappresentata da computer "equiparati" che sincronizzano i loro dati a vicenda. Questo è l'approccio che segue unison. rsync segue l'approccio client-server, comunque ogni client può fungere a sua volta da server.

47.2.2 Portabilità

Subversion, CVS, e unison sono disponibili per tutta una serie di sistemi operativi tra cui UNIX e Windows.

47.2.3 Interattivo vs. automatico

Con subversion, CVS WebDAV, e unison la sincronizzazione viene inizializzata manualmente dall'utente. Il vantaggio è che si ha maggior controllo sul processo di sincronizzazione ed è più facile risolvere dei conflitti. Dall'altra parte, se la sincronizzazione viene effettuata troppo di rado aumentano le probabilità che si verifichi un conflitto.

47.2.4 Il verificarsi e la risoluzione di conflitti

In subversion o CVS i conflitti si verificano solo raramente anche se sono diverse persone a lavorare ad un grande progetto. I documenti vengono costruiti riga dopo riga. Quando si verifica un conflitto, spesso ciò riguarda solo un client. Generalmente, nel caso di subversion o CVS i conflitti sono semplici da risolvere.

Unison comunica il verificarsi di conflitti e si potranno escludere i file imputati dal processo di sincronizzazione. Tuttavia non è così semplice allineare le modifiche come nel caso di subversion o CVS.

Mentre con subversion o CVS quando si verifica un conflitto, le modifiche possono essere assunte anche parzialmente, nel caso di WebDAV un check-in può essere eseguito solo se il processo di modifica nel suo intero non ha prodotto dei conflitti.

rsync non presenta delle funzionalità per trattare ed eliminare eventuali dei conflitti. L'utente dovrà fare attenzione a non sovrascrivere per errore dei file e risolvere manualmente i conflitti che affioriranno. Per andare sul sicuro, si potrà ricorrere ad applicazioni di versionamento come RCS.

47.2.5 Selezionare e aggiungere dei file

Unison sincronizza interi alberi di directory. I file che si aggiungono all'albero vengono inclusi automaticamente nel processo di sincronizzazione.

In subversion o CVS bisogna aggiungere esplicitamente nuovi file e directory tramite il comando `svn add` o `cvs add`. In tal modo si ha un maggior controllo sui file da sincronizzare. Dall'altra parte spesso si dimenticano i nuovi file, soprattutto se nell'output di `svn update`, `svn status` o `cvs update` si ignorano i '?' (punti interrogativi) a causa della mole dei file.

47.2.6 Lo storico

Subversion o CVS permettono inoltre di ricostruire versioni precedenti di un file. Ad ogni modifica potrete aggiungere un breve commento per poter meglio seguire e

rintracciare le varie modifiche apportate al file in passato. Questa funzionalità si rivela di particolare utilità nella stesura di tesi o di sorgenti.

47.2.7 Volume dei dati e spazio sul disco rigido richiesto

Su ogni computer interessato serve spazio a sufficienza per i dati dislocati. Per subversion o cvs serve inoltre dello spazio aggiuntivo per la banca dati (il cosiddetto repository) sul server. Visto che sul server viene memorizzato anche lo storico dei dati è necessario ulteriore spazio. Nel caso di file di testo, il fabbisogno non è eccessivo anche perché vengono memorizzate solo le righe modificate; mentre per file binari ad ogni modifica il fabbisogno cresce nella misura del volume del file.

47.2.8 GUI

Unison dispone di una interfaccia grafica che indica cosa il programma intende sincronizzare. Si può accettare la proposta o escludere singoli file dalla sincronizzazione. Inoltre è possibile confermare in modo interattivo i singoli processi nel modo testo.

Gli utente più esperti impiegano CVS di solito servendosi della riga di comando. Comunque vi sono anche interfacce grafiche per Linux (cervisia…) ed anche per Windows (wincvs). Tanti tool di sviluppo (p.es. kdevelop) ed editor di testo (p.es. emacs) supportano CVS o subversion. Grazie a questi front-end risolvere dei conflitti diventa davvero semplice.

47.2.9 User friedliness

unison e rsync sono semplici da utilizzare ed indicati anche per principianti. CVS o subversion sono già un po' più complessi nel loro utilizzo. Per un eventuale impiego si dovrebbe aver afferrato il modo di interagire tra il repository e i dati in locale. In locale si dovrebbe innazitutto avere comunque la versione aggiornata dei file, questo si ottiene con il comando `cvs update` o `svn update`. Dopo aver eseguito questo comando, con il comando `cvs commit` o `svn commit` i dati vanno rispediti nel repository. Se si segue sempre questa procedura CVS o subversion risultano essere semplici da utilizzare anche per principianti.

47.2.10 Sicurezza contro attacchi

La protezione contro l'intercettazione o addirittura la manipolazione dei dati durante il loro trasferimento dovrebbe essere sempre data. Sia per unison che CVS, rsync o subversion si può ricorrere a ssh (Secure Shell) per mettersi al riparo da eventuali attacchi. Evitate di utilizzare rsh (remote shell) con CVS o unison e anche gli accessi tramite il meccanismo *pserver* del CVS non sono consigliabili in rete non protette. subversion è per questi casi già più indicato, visto che offre i necessari meccanismi di sicurezza tramite l'utilizzo di Apache.

47.2.11 Sicurezza contro la perdita di dati

CVS viene utilizzato da già tempo da tanti sviluppatori per amministrare i propri progetti ed è estremamente stabile. Grazie allo storico, con CVS si è anche al riparo di determinati errori causati da disattenzioni dell'utente (p.es. cancellare per errore un file). Anche se subversion non gode della diffusione di CVS, viene già utilizzato in modo produttivo (si veda l'esempio dello stesso progetto subversion).

Unison è un prodotto relativamente recente ma è già molto stabile. L'utente dovrà fare molta attenzione per evitare degli errori: se ad esempio accetta di cancellare un file durante il processo di sincronizzazione, il file risulterà irrecuperabile.

Tabella 47.1 *Feature dei tool di sincronizzazione -- = molto scarso, - = scarso o non disponibile, o = mediocre, + = buono, ++ = molto buono, x = disponibile*

	unison	**CVS/subv.**	**rsync**	**mailsync**
Client/Server	uguale	C-S/C-S	C-S	uguale
Portabil.	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interattivo	x	x/x	x	-
Velocità	-	o/+	+	+
Conflitti	o	++/++	o	+
Selez. file	Directory	Selez./file,direct.	Directory	Mail box

	unison	CVS/subv.	rsync	mailsync
Storico	-	x/x	-	-
Spazio dis.	o	--	o	+
GUI	+	o/o	-	-
Difficoltà	+	o/o	+	o
Attacchi	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
Perdita di dati	+	++/++	+	+

47.3 Introduzione ad unison

Unison si adatta perfettamente ai fini della sincronizzazione e del trasferimento di interi alberi di directory. La sincronizzazione avviene in entrambi le direzioni e si lascia gestire facilmente tramite un front-end grafico (alternativamente potete utilizzare anche la versione console). Sussiste anche la possibilità di automatizzare il processo di sincronizzazione, cioé far svolgere il tutto senza che sia richiesto un intervento da parte dell'utente.

47.3.1 Presupposti

Unison deve essere installato sia sul client che sul server; con *server* in questi casi si intende un computer remoto (a differenza di CVS, si veda la Sezione 47.1.2, «CVS» (p. 772)).

Dato che nella seguente esposizione ci limiteremo all'impiego di unison con ssh, dovrà essere installato un client ssh sul client ed un server ssh sul server.

47.3.2 Utilizzo di Unison

Il principio di base di Unison consiste nel collegare due directory (cosiddette*roots*), o meglio collegare in senso simbolico - non si tratta un collegamento online. Facciamo un esempio: ammettiamo di avere il seguente layout di directory:

Client:	`/home/tux/dir1`
Server:	`/home/geeko/dir2`

Volete sincronizzare entrambi le directory. Sul client, l'utente è noto come tux e sul server invece come `geeko`. Innanzitutto si dovrebbe eseguire un test per verificare il corretto funzionamento della comunicazione tra il server e il client:

```
unison –testserver /home/tux/dir1 ssh://geeko@server//homes/geeko/dir2
```

Ecco le principali difficoltà che potrebbero sorgere a questo punto:

- le versioni di unison utilizzate sul client e sul server non sono compatibili
- il server non permette una connessione SSH
- nessuno dei due percorsi indicati esiste

Se tutto funziona come deve, si tralascia l'opzione `–testserver`. Durante la prima sincronizzazione unison non conosce ancora il rapporto che intercorre tra le due directory, e fa delle proposte per quando riguarda la direzione di trasferimento dei singoli file e directory. Le frecce nella colonna *Azione* indicano la direzione di trasferimento. Il punto interrogativo '?' indica che unison non riesce a fare una proposta riguardo alla direzione di trasferimento, dato che entrambi le versioni nel frattempo sono state modificate o sono nuove.

Con i tasti freccia si può impostare la direzione di trasferimento per ogni singola registrazione. Una volta stabilita la direzione di trasferimento per le registrazioni visualizzate, fate clic semplicemente su *Vai*.

Unison (ad es. per eseguire automaticamente la sincronizzazione nei casi evidenti) può ricevere all'avvio dei parametri dalla riga di comando. Un elenco completo dei parametri si ottiene con `unison ––-help`.

Esempio 47.1 *Il file ~/.unison/example.prefs*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

Ogni processo di sincronizzazione viene protocollato nella directory dell'utente `~/.unison`. In questa directory si possono immettere anche set di configurazione, per es. `~/.unison/example.prefs`. Per inizializzare la sincronizzazione basta semplicemente indicare il file come argomento della riga di comando: `unison example.prefs`

47.3.3 Ulteriore documentazione

La documentazione ufficiale su unison è davvero esaustiva, nel presente capitolo ci siamo limitati ad una breve introduzione. Sotto `http://www.cis.upenn.edu/~bcpierce/unison/` o nel pacchetto SUSE `unison` troverete un manuale completo.

47.4 Introduzione a CVS

CVS può essere utilizzato anche ai fini della sincronizzazione, quando si modificano frequentemente singoli file nel formato di testo ASCII oppure sorgenti di programmi. Con CVS si possono sincronizzare anche dati in altri formati (p.es. file JPEG), ma questo comporta un enorme volume di dati, visto che ogni variante di un file viene memorizzata permanentemente sul server CVS. Ed inoltre in questi casi non si sfrutta appieno il vero potenziale di CVS. Si consiglia di ricorrere a CVS per la sincronizzazione dei dati solo se tutte le postazioni di lavoro hanno accesso allo stesso server!

47.4.1 Impostare un server CVS

Il *server* è host su cui si trovano tutti i file validi, ovvero soprattutto la versione attuale di ogni file. Una una postazione di lavoro fissa può fungere da server. E' consigliabile eseguire regolarmente un back-up dei dati che risiedono sul server CVS (repository).

Si consiglia di impostare un server CVS in modo che agli utenti sia permesso di accedervi tramite SSH. Se l'utente è noto al server come `tux` ed il software del CVS è stato

installato sia sul server che sul client (p.es. un notebook), sul lato client bisogna impostare le seguenti variabili di ambiente:

```
CVS_RSH=ssh CVS_ROOT=tux@server:/serverdir
```

Con il comando `cvs init` si inizializza il server CVS dal lato client (basta farlo una sola volta).

Infine bisogna stabilire un nome per la sincronizzazione. Selezionate o create una directory sul client che dovrà contenere i file che dovranno essere amministrati da CVS (la directory può essere anche vuota). Il nome della directory è nel contempo il nome del processo di sincronizzazione. Nel nostro esempio utilizziamo il nome `synchome`. Per impostare il nome della sincronizzazione su `synchome` si deve immettere:

```
cvs import synchome tux wilber
```

Attenzione: molti comandi CVS richiedono un commento. A tale scopo CVS lancia un editor (più precisamente l'editor definito nella variabile di ambiente `$EDITOR`, altrimenti lancia il vi). Si può evitare che venga lanciato l'editor immettendo il commento già nella riga di comando, ad es

```
cvs import –m 'questa è una prova' synchome tux wilber
```

47.4.2 Utilizzare il CVS

A partire da questo momento si può effettuare da un computer qualsiasi il check out dal repository di sincronizzazione con `cvs co synchome`. Si avrà una nuova sottodirectory `synchome` sul client. Se si sono fatte delle modifiche che si vogliono comunicare al server, bisogna entrare nella directory `synchome` (o anche in una sottodirectory di synchome) ed immettere il seguente comando: `cvs commit`.

Con questo comando vengono trasmessi al server tutti i file della la directory (sottodirectory incluse). Per trasferire solo singoli file e/o singole directory, si dovranno indicare esplicitamente con un comando del tipo: `cvs commit file1 directory1`. Nuovi file o nuove directory vanno aggiunte alla repository tramite un comando del tipo: `cvs add file1 directory1`, prima di trasferirli sul server. Di conseguenza il commit di nuovi file e directory che si sono aggiunti si esegue tramite `cvs commit file1 directory1`.

Se cambiate postazione di lavoro, dovrete, se non lo avete già fatto durante delle sessioni di lavoro precedenti sulla stessa postazione, eseguire il check out del repository (si veda sopra).

La sincronizzazione con il server viene inizializzata con: `cvs update`. Sussiste inoltre la possibilità di eseguire l'update di singoli file e/o singole directory eseguendo `cvs update file1 directory1`. Se volete vedere in anteprima le differenze rispetto alle versioni memorizzate sul server, immettete `cvs diff` o `cvs diff file1 directory1`. In più avete anche la possibilità di farvi mostrare quali file verrebbero aggiornati, ecco il comando: `cvs -nq update`.

Durante l'update incontrerete tra l'altro le seguenti lettere indicanti lo stato del file:

U
: la versione locale è stata aggiornata.

M
: la versione locale è stata modificata.

P
: la versione locale è stata adattata (ingl. patched) in base alla versione sul server.

C
: il file locale non collima con la versione attuale nel repository.

?
: questo file non esiste nel CVS.

`M` indica un file che è stato modificato. Potete spedire la versione locale al server o cancellare il file locale e si esegue nuovamente un update. Se diversi utenti modificano lo stesso file nello stesso punto, CVS non è in grado di decidere quale versione utilizzare. In questi casi all'update si ha una `C` che indica la presenza di un conflitto.

In tal caso prendete spunto dai marcatori di conflitto e decidete quale delle due versioni scegliere. Visto che a volte non è per niente semplice prendere una tale decisione, potete anche optare di scartare le vostre modifiche, cancellare il file locale e immettere `cvs up` per recuperare la versione attuale dal server.

47.4.3 Ulteriore documentazione

Le possibilità di impiego di CVS sono immense e noi abbiamo fornito solo una breve introduzione. Per degli approfondimenti rimandiamo alla documentazione reperibile tra l'altro ai seguenti indirizzi:

```
http://www.cvshome.org/
http://www.gnu.org/manual/
```

47.5 Un'introduzione a subversion

Subversion è un sistema di controllo di versionamento a sorgente aperto che succede a CVS. Le caratteristiche già trattate di CVS si ritrovano generalmente anche in subversion che presenta tutti i vantaggi di CVS senza riproporrne gli svantaggi. Molte delle caratteristiche sono state già trattate nella Sezione 47.1.3, «subversion» (p. 773).

47.5.1 Configurare un server subversion

Impostare un repository su un server è un processo davvero semplice. subversion dispone di un proprio tool. Per generare un nuovo repository, immettete:

```
svnadmin create /percorso/del/repository
```

Per visualizzare ulteriori opzioni, immettete `svnadmin help`. A differenza di CVS, subversion non si basa su RCS ma su la banca dati Berkeley. *Non* create una repository su file system remoti come NFS, AFS o Windows SMB. La banca dati richiede dei meccanismi di locking POSIX che i file sytem menzionati non offrono.

Per visionare il contenuto di un repository, vi è il comando `svnlook`:

```
svnlook info /percorso/del/repository
```

Affinché anche altri utenti possano accedere al repository va configurato un server; potrà trattarsi di un server Web Apache con WebDAV o del server di subversion, svnserve. Se svnserve è in esecuzione si potrà accedere ad una repository tramite L'URL `svn://` o `svn+ssh://`. Tramite il file di configurazione `/etc/svnserve.conf` potete indicare gli utenti che dovranno autenticarsi se invocano `svn`.

Rispondere alla domanda quale sistema di versionamento scegliere non è facile, dato che vanno considerati una serie di fattori. Si consiglia di dare un'occhiata al manuale

di subversion (per maggiori informazioni, si veda la Sezione 47.5.3, «Ulteriore documentazione» (p. 786)).

47.5.2 Utilizzo

Per accedere ad un repository di subversion vi è il comando `svn` (simile a `cvs`). Se il server è stato configurato in modo corretto (con relativo repository) il contenuto di ogni client può essere visionato con:

```
svn list http://svn.example.com/percorso/del/progetto
```

oppure

```
svn list svn://svn.example.com/percorso/del/progetto
```

Con il comando `svn checkout` un dato progetto può essere salvato nella directory attuale (ingl. check out):

```
svn checkout http://svn./percorso/del/progetto nomeprogetto
```

Il check out crea una nuova sottodirectory `nomeprogetto` sul client, in cui poter eseguire tutta una serie di modiche come aggiungere, copiare, rinominare e cancellare dei file:

```
svn add file
svn copy vecchiofile nuovofile
svn move vecchiofile nuovofile
svn delete file
```

Questi comandi sono applicabili anche a delle directory. Inoltre subversion è in grado di indicare le cosiddette properties, ossia proprietà di un file o di una directory:

```
svn propset license GPL foo.txt
```

Nell'esempio precedente è stato impostato il valore `GPL` per la proprietà `license`. Le proprietà si lasciano visualizzare con `svn proplist`.

```
svn proplist --verbose foo.txt
Properties on 'foo.txt':
  license : GPL
```

Per salvare le modifiche sul server, immettete `svn commit`. Affinché un altro utente possa disporre delle vostre modifiche nella sua directory di lavoro, dovrà eseguire un `svn update`.

A differenza di CVS, lo stato di una directory di lavoro subversion può essere visualizzato anche *senza* accesso al repository con `svn status`. Le modifiche locali vengono visualizzate in cinque colonne, la prima è quella di maggiore rilevanza:

''
: Nessuna modifica

'A'
: Oggetto da aggiungere

'D'
: Oggetto da eliminare

'M'
: Oggetto modificato

'C'
: Oggetto in stato di conflitto

'I'
: Oggetto ignorato

'?'
: Oggetto non incluso nel controllo di versionamento

'!'
: Oggetto manca. Questo stato si ha se l'oggetto è stato eliminato o spostato senza ricorrere al comando `svn`.

'~'
: Oggetto amministrato come file è stato sostituito da una directory o viceversa.

La seconda colonna indica lo stato delle properties. Tutte le altre colonne vengono illustrate nel manuale di subversion.

Se vi dovesse sfuggire il parametro di un comando, provate con, `svn help`:

```
svn help proplist
proplist (plist, pl): List all properties on files, dirs, or revisions.
usage: 1. proplist [PATH...]
       2. proplist --revprop -r REV [URL]

  1. Lists versioned props in working copy.
```

```
  2. Lists unversioned remote props on repos revision.
...
```

47.5.3 Ulteriore documentazione

Innazitutto vi è la home page del progetto subversion che trovate al seguente indirizzo `http://subversion.tigris.org/`. Se installate il pacchetto `subversion-doc` nella directory `file:///usr/share/doc/packages/subversion/html/book.html` sarà a vostra disposizione un manuale in inglese completo che vale davvero la pena di leggere. Tra l'altro è anche disponibile online sotto `http://svnbook.red-bean.com/svnbook/index.html`.

47.6 Un'introduzione a rsync

rsync si propone ogni qualvolta si debbano trasmettere grandi volumi di dati con cadenze più o meno regolari. Cosa che si ha spesso quando si esegue un back-up, ovvero una copia di sicurezza. Un ulteriore campo di applicazione è rappresentato dai cosiddetti staging server, ovvero server su cui risiede l'intero albero directory di un server Web che viene specchiato con cadenze regolari sull'effettivo server Web in una «DMZ».

47.6.1 Configurazione e utilizzo

rsync può essere utilizzato in due modi diversi. rsync può essere utilizzato per archiviare e copiare dei file, a tal fine è richiesta solo una shell remota, come ad esempio ssh, sull'host meta. rsync può però fungere anche da `daemon` e mettere a disposizione delle directory nella rete.

Per utilizzare rsync non è richiesta una configurazione particolare. rsync permette di specchiare direttamente delle intere directory su di un altro host. Ad esempio con il seguente comando è possibile avere un back-up della directory home di tux sul server di back-up sun:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

Per il processo inverso si immette:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Fin qui il funzionamento non si distingue particolarmente da una comune applicazione per effettuare delle copie, come scp.

Per sfruttarne a fondo le potenzialità, rsync dovrebbe girare nel modo «rsync». A tal fine va avviato su un host il daemon rsyncd. In questo caso rsync si configura tramite il file `/etc/rsyncd.conf`. Se ad esempio intendete rendere accessibile la directory `/srv/ftp` tramite rsync potete utilizzare il file di configurazione riportato:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = Un esempio
```

In seguito si dovrà lanciare rsyncd con `rcrsyncd start` rsyncd può essere lanciato anche automaticamente durante il processo di boot, basta abilitare il servizio nell' editor dei runlevel di YaST oppure immettere manualmente il comando `insserv rsyncd`. Come alternativa rsyncd può essere lanciato anche da xinetd. Ciò si consiglia solo nel caso di server su cui non si utilizza spesso rsyncd.

Nell'esempio di sopra viene creato anche un file di log che protocolla tutte le connessioni, lo ritroverete sotto `/var/log/rsyncd.log`.

A questo punto si potrà seguire il transfer da un client, tramite il comando:

```
rsync -avz sun::FTP
```

Questo comando elenca tutti i file che si trovano sul server nella directory `/srv/ftp`. Questa richiesta riemerge anche nel file di log sotto `/var/log/syncd.log`. Per avviare il transfer va indicata una directory meta. Per indicare la directory attuale potete anche utilizzare un `.`, quindi:

```
rsync -avz sun::FTP .
```

Di default durante il processo di sincronizzazione eseguito tramite rsync non vengono eliminati dei file. Se si vuole forzare tale operazione, basta indicare in aggiunta l'opzione `--delete`. Per garantire che non vengano sovrascritti dei file aggiornati potete indicare l'opzione `--update`. Se dovessero verificarsi dei conflitti, questi dovranno essere risolti manualmente.

47.6.2 Ulteriore documentazione

Le indicazioni di maggior rilevanza su rsync sono contenute nelle pagine di manuale che potete visualizzare con `man rsync` e `man rsyncd.conf`. Per delle indicazioni di natura tecnica su rsync rimandiamo a `/usr/share/doc/packages/rsync/tech_report.ps`. Per delle informazioni aggiornate su rsync visitate il sito Web del progetto che trovate sotto `http://rsync.samba.org`.

47.7 Introduzione a mailsync

Mailsync assolve principalmente tre compiti:

- sincronizza e-mail memorizzati in locale con e-mail memorizzati su un server
- esegue la migrazione di mail box in un altro formato o su un altro server
- verifica l'integrità di una mail box o cerca i doppioni

47.7.1 Configurazione ed utilizzo

Mailsync distingue tra mail box in sé (un cosiddetto *store*) e il collegamento tra due mail box (un cosiddetto *channel*). La definizione degli store e dei channel viene archiviata nel file `~/.mailsync`. Seguono alcuni esempi relativi agli store.

Una semplice definizione ha ad es. il seguente aspetto:

```
store saved-messages {
   pat Mail/saved-messages
prefix  Mail/
}
```

dove `Mail/` è una sottodirectory nella directory home dell'utente, contente una cartella con le e-mail, tra l'altro la cartella `saved-messages`. Se si invoca mailsync con il comando `mailsync -m saved-messages` in `saved-messages` si avrà un indice con tutti i messaggi. Un altro esempio:

```
store localdir {
pat     Mail/*
```

```
prefix  Mail/
}
```

In questo caso invocando `mailsync -m localdir` verranno elencati tutti i messaggi salvati sotto `Mail/`. Il comando `mailsync localdir` elenca invece i nomi delle cartelle. La specificazione di uno store sul server IMAP p.es. ha il seguente aspetto:

```
store imapinbox {
server {mail.edu.harvard.com/user=gulliver}
ref    {mail.edu.harvard.com}
pat    INBOX
}
```

Nell'esempio riportato sopra vengono semplicemente indirizzate il folder, ossia cartella principale sul server IMAP. Uno store per le sottocartelle assumerebbe il seguente aspetto:

```
store imapdir {
server {mail.edu.harvard.com/user=gulliver}
ref {mail.edu.harvard.com}
pat INBOX.*
prefix  INBOX.
}
```

Se il server IMAP supporta connessioni cifrate, la specificazione del server dovrebbe essere modificata nel modo seguente:

```
server  {mail.edu.bocconi.it/ssl/user=gulliver}
```

o (se non conoscete il certificato del server) in

```
server {mail.edu.bocconi.it/ssl/novalidate-cert/user=gulliver}
```

Il prefisso viene spiegato in seguito.

Ora le cartelle sotto `Mail/` vanno connesse alle sottodirectory sul server IMAP:

```
channel cartella localdir imapdir {

msinfo .mailsync.info
}
```

Mailsync utilizza il file `msinfo` per tenere traccia dei messaggi già sincronizzati.

Invocando `mailsync cartella` si ottiene che:

- la mail box venga allineata su entrambi gli host
- il prefisso dai nomi delle cartelle che si creano durante il processo venga eliminato
- le cartelle vengano sincronizzate a due a due (o create se ancora non esistenti)

La cartella `INBOX.sent-mail` sul server IMAP viene quindi sincronizzata con la cartella locale `Mail/sent-mail` (ciò presuppone le definizioni di cui sopra). Infine viene eseguita la sincronizzazione delle singole cartelle nel modo seguente:

- se il messaggio esiste su entrambi gli host, non succede niente
- se il messaggio manca da una parte e si tratta di un messaggio nuovo, cioé non protocollato nel file `msinfo`, viene trasmesso lì dove manca
- se il messaggio esiste solo su una parte e si tratta di un messaggio già vecchio ovvero già protocollato nel file `msinfo`, viene cancellato da lì (dato che il messaggio che esisteva è stato cancellato sull' altro host)

Per avere una vista di insieme a priori dei messaggi che verranno trasmessi e quali cancellati durante la sincronizzazione, bisogna richiamare Mailsync contemporaneamente con un channel *ed* uno store: `mailsync cartella localdir`. In tal maniera si avrà un elenco dei messaggi che sono nuovi sull'host locale ed anche una lista di tutti i messaggi che verrebbero cancellati sul lato server IMAP durante la sincronizzazione. Inversamente con `mailsync cartella imapdir` si ottiene un'elenco dei messaggi nuovi sul lato IMAP ed anche un'elenco dei messaggi che verrebbero cancellati sull'host locale durante la sincronizzazione.

47.7.2 Possibili difficoltà

Nel caso si verifichi una perdita di dati, il modo più sicuro di procedere è quello i cancellare i relativi file di protocollo channel `msinfo`. In tal modo tutti i messaggi che esistono solo da una parte vengono considerati dei nuovi messaggi e verranno trasmessi durante la prossima sincronizzazione.

Saranno presi in considerazione per quanto riguarda la sincronizzazione solo quei messaggi che hanno una cosiddetta message ID. I messaggi sprovvisti di un tale identificativo verranno ignorati, cioé non verranno né trasmessi né cancellati. Spesso

la mancanza della message ID è dovuta a errori da ricondurre a dei programmi in fase di invio o creazione delle e-mail.

Su determinati server IMAP la cartella principale viene indirizzata tramite `INBOX`, e le sottocartelle tramite un nome qualsiasi (a differenza di INBOX ed INBOX.name). In tal modo per questi server IMAP non è possibile specificare un campione esclusivamente per le sottocartelle.

I driver per mail box (c-client) utilizzati da Mailsync, una volta trasmessi correttamente i messaggi ad un server IMAP, impostano una speciale indicazione di stato (status flag) per cui alcuni programmi di posta elettronica come mutt non riescono ad riconoscere i nuovi messaggi come tali. Per evitare che ciò avvenga vi è l'opzione `-n`.

47.7.3 Ulteriore documentazione

Nel `README` contenuto nel pacchetto `mailsync` sotto `/usr/share/doc/packages/mailsync/` sono reperibili ulteriori informazioni ed indicazioni. Di particolare interesse in questo contesto è anche l'RFC 2076 «Common Internet Message Headers».

48 Samba

Con Samba è possibile configurare un computer Unix come file server e server di stampa per i computer che eseguono DOS, Windows e OS/2. L'evoluzione di Samba ha generato un prodotto completo e piuttosto complesso. Oltre a illustrare la funzionalità di base, in questo capitolo vengono introdotte le nozioni di base sulla configurazione di Samba e vengono descritti i moduli YaST che è possibile utilizzare per configurare Samba nella rete.

Ulteriori informazioni su Samba sono disponibili nella documentazione digitale. Nella riga di comando immettere `apropos samba` per visualizzare la documentazione oppure, se nel computer è installato Samba, sfogliare la directory `/usr/share/doc/packages/samba` per visualizzare esempi e altra documentazione in linea. Nella sottodirectory `examples` è disponibile una configurazione di esempio con commenti (`smb.conf.SuSE`).

Di seguito sono illustrate alcune importanti nuove funzionalità della versione 3 inclusa del pacchetto `samba`:

- Supporto per Active Directory.
- Supporto Unicode migliorato.
- Revisione completa del meccanismo di autenticazione interno.
- Supporto migliorato per il sistema di stampa di Windows 200x e XP.
- Possibilità di configurazione dei server come membri nei domini di Active Directory.

- Adozione di un dominio di NT 4 per consentire la migrazione da quest'ultimo a un dominio Samba.

SUGGERIMENTO: Migrazione a Samba 3.

Per la migrazione da Samba 2.x a Samba 3 è necessario considerare alcuni aspetti specifici. Nella documentazione HOWTO di Linux su Samba è incluso un intero capitolo dedicato a questo argomento. Dopo l'installazione del pacchetto `samba-doc`, la documentazione HOWTO è disponibile nel percorso `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Samba utilizza il protocollo SMB (Server Message Block) basato sui servizi NetBIOS. Microsoft ha rilasciato questo protocollo su pressione di IBM per consentire ad altri produttori di software di stabilire connessioni a una rete di domini Microsoft. Con Samba il funzionamento del protocollo SMB si basa sul protocollo TCP/IP, pertanto è necessario installare TCP/IP su tutti i client.

NetBIOS è un'interfaccia software (API) progettata ai fini della comunicazione tra computer, mediante la quale viene fornito un servizio nomi. Consente ai computer connessi alla rete di riservare nomi per se stessi, in modo che in seguito possano essere indirizzati per nome. Non è disponibile un processo centrale per il controllo dei nomi e qualsiasi computer della rete può riservare tutti i nomi necessari, se questi non sono già in uso. L'attuale interfaccia NetBIOS può essere implementata per diverse architetture di rete. Esiste un'implementazione che funziona relativamente a livello di hardware di rete, denominata NetBEUI, alla quale viene spesso fatto riferimento come NetBIOS. I protocolli di rete implementati con NetBIOS sono IPX di Novell (NetBIOS tramite TCP/IP) e TCP/IP.

I nomi NetBIOS inviati tramite TCP/IP sono completamente diversi dai nomi utilizzati nel file `/etc/hosts` o dai nomi definiti tramite DNS. NetBIOS utilizza infatti una convenzione di denominazione completamente indipendente. Per facilitare l'amministrazione, si consiglia tuttavia di utilizzare nomi corrispondenti ai nomi host DNS, utilizzati di default da Samba.

Il protocollo SMB è supportato da tutti i sistemi operativi comuni, ad esempio Mac OS X, Windows e OS/2. Il protocollo TCP/IP deve essere installato in tutti i computer. Con Samba viene fornito un client per le varie versioni di UNIX. Per Linux è disponibile un modulo del kernel per SMB che consente l'integrazione delle risorse di SMB nel livello sistema di Linux.

I server SMB forniscono spazio hardware al client per mezzo delle condivisioni. Una condivisione include una directory e le relative sottodirectory nel server. Viene esportata per mezzo di un nome ed è possibile accedervi utilizzando il relativo nome. Il nome della condivisione può essere un nome qualsiasi e non deve necessariamente corrispondere alla directory di esportazione. Viene assegnato un nome anche alla stampante, alla quale i client possono accedere utilizzando questo nome.

48.1 Configurazione del server

Se si prevede di utilizzare Samba come server, installare `samba`. Avviare i servizi richiesti per Samba con `rcnmb start && rcsmb start` e interromperli con `rcsmb stop && rcnmb stop`.

Il file di configurazione principale di Samba, `/etc/samba/smb.conf`, può essere diviso in due parti logiche. Nella sezione `[global]` sono presenti le impostazioni centrali e globali, mentre nelle sezioni `[share]` sono contenute le singole condivisioni di file e stampanti. Grazie a questo approccio è possibile impostare in modo diverso o globale i dettagli relativi alle condivisioni nella sezione `[global]` e migliorare la trasparenza strutturale del file di configurazione.

48.1.1 Sezione global

Per soddisfare i requisiti di configurazione della rete in modo che altri computer possano accedere al server Samba tramite SMB in un ambiente Windows, è necessario apportare alcune modifiche ai parametri della sezione `[global]` riportati di seguito.

workgroup = TUX-NET
: In questa riga il server Samba viene assegnato a un gruppo di lavoro. Sostituire `TUX-NET` con un gruppo di lavoro appropriato all'ambiente di rete in uso. Il server Samba viene identificato con il relativo nome DNS, a meno che tale nome sia stato assegnato a un altro computer nella rete. Se il nome DNS non è disponibile, impostare il nome del server mediante `netbiosname=MYNAME`. Per ulteriori informazioni su questo parametro, vedere `man smb.conf`.

os level = 2
: Questo parametro consente di definire se il server Samba tenterà di assumere il ruolo di LMB (Local Master Browser) per il gruppo di lavoro a cui appartiene.

Scegliere un valore molto basso per evitare qualsiasi interferenza nella rete Windows esistente causata da un server Samba configurato in modo scorretto. Per ulteriori informazioni su questo importante argomento, vedere i file `BROWSING.txt` e `BROWSING-Config.txt` nella sottodirectory `textdocs` della documentazione relativa al pacchetto.

Se nella rete non sono presenti altri server SMB, ad esempio un server Windows NT o 2000, e si desidera che sul server Samba venga creato un elenco di tutti i sistemi presenti nell'ambiente locale, impostare il parametro `os level` su un valore più alto, ad esempio `65`. Il server Samba verrà quindi scelto come LMB per la rete locale.

Quando si modifica questa impostazione, considerare con attenzione l'impatto che potrebbe avere su un ambiente di rete Windows esistente. Effettuare prima i test delle modifiche in un ambiente di rete isolato o in un'ora del giorno in cui il traffico di rete è limitato.

wins support e wins server
Per integrare il server Samba in una rete Windows esistente con un server WINS attivo, abilitare l'opzione `wins server` e impostare il relativo valore sull'indirizzo IP del server WINS.

Se i computer Windows sono connessi a sottoreti separate e devono continuare a riconoscersi reciprocamente, è necessario configurare un server WINS. Per convertire un server Samba in un server WINS, impostare l'opzione `wins support = Yes`. Assicurarsi che questa impostazione sia abilitata in un solo server Samba della rete. Le opzioni `wins server` e `wins support` non devono mai essere abilitate contemporaneamente nel file `smb.conf`.

48.1.2 Condivisioni

Negli esempi seguenti viene illustrato come rendere disponibili ai client SMB un'unità CD-ROM e le directory utente (`homes`).

[cdrom]
Per evitare che l'unità CD-ROM sia resa accidentalmente disponibile, queste righe sono disattivate mediante segni di commento (in questo caso punti e virgola). Rimuovere i punti e virgola nella prima colonna per condividere l'unità CD-ROM con Samba.

Esempio 48.1 *Condivisione di un CD-ROM.*

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` e `comment`

La voce `[cdrom]` corrisponde al nome della condivisione visibile a tutti i client SMB nella rete. Per descrivere la condivisione, è possibile aggiungere una voce `comment`.

`path = /media/cdrom`

`path` consente l'esportazione della directory `/media/cdrom`.

Per mezzo di una configurazione di default molto restrittiva questo tipo di condivisione viene reso disponibile solo agli utenti presenti nel sistema. Per rendere la condivisione disponibile a tutti gli utenti, aggiungere la riga `guest ok = yes` alla configurazione. Questa impostazione consente di assegnare autorizzazioni di lettura a tutti gli utenti della rete. Si consiglia di utilizzare questo parametro con la massima precauzione, specialmente nella sezione `[global]`.

`[homes]`

La condivisione `[home]` è estremamente importante in questo caso. Se l'utente dispone di un account e di una password validi per il file server Linux e di una propria home directory, può essere connesso a tale condivisione.

Esempio 48.2 *Condivisione homes.*

```
[homes]
 comment = Home Directories
 valid users = %S
 browseable = No
 read only = No
 create mask = 0640
 directory mask = 0750
```

[homes]

A condizione che per nessun'altra condivisione venga utilizzato il nome di condivisione dell'utente che si connette al server SMB, viene generata dinamicamente una condivisione mediante le direttive della condivisione `[homes]`. Il nome della condivisione risultante è il nome utente.

valid users = %S
: `%S` viene sostituito con il nome reale della condivisione non appena viene stabilita una connessione. Per una condivisione `[homes]` questo nome corrisponde sempre al nome utente. I diritti di accesso alla condivisione di un utente, di conseguenza, vengono limitati esclusivamente all'utente.

browseable = No
: Questa impostazione rende la condivisione invisibile nell'ambiente di rete.

read only = No
: Per default, Samba impedisce l'accesso in scrittura a tutte le condivisioni esportate per mezzo del parametro `read only = Yes`. Per rendere scrivibile una condivisione, impostare il valore `read only = No` che è sinonimo di `writeable = Yes`.

create mask = 0640
: I sistemi non basati su Microsoft Windows NT non riconoscono il concetto di autorizzazioni di UNIX, pertanto non sono in grado di assegnare autorizzazioni durante la creazione di un file. Il parametro `create mask` definisce le autorizzazioni di accesso assegnate ai nuovi file creati. Questa impostazione viene applicata solo alle condivisioni scrivibili. In effetti significa che il proprietario dispone di autorizzazioni di lettura e scrittura, mentre i membri del gruppo primario del proprietario dispongono di autorizzazioni di lettura. `valid users = %S` impedisce l'accesso in lettura anche se al gruppo sono assegnate autorizzazioni di lettura. Per consentire l'accesso in lettura o scrittura al gruppo, disattivare la riga `valid users = %S`.

48.1.3 Livelli di sicurezza

Il protocollo SMB ha origine dall'ambiente DOS e Windows ed è direttamente correlato al problema della sicurezza. L'accesso a ogni condivisione può essere protetto mediante una password. Per il controllo delle autorizzazioni in SMB sono disponibili tre modi:

Sicurezza a livello di condivisione (security = share):
: Una password viene assegnata stabilmente a una condivisione. Chiunque conosca questa password può accedere alla condivisione.

Sicurezza a livello utente (security = user):
Questa variazione introduce il concetto dell'utente in SMB. Ogni utente deve registrarsi nel server con la propria password, dopodiché il server può concedere l'accesso a singole condivisioni esportate in base ai nomi utente.

Sicurezza a livello di server (security = server):
Per i client il funzionamento del server Samba avviene apparentemente a livello di utente, mentre in realtà tutte le query relative alle password vengono passate a un altro server in modalità livello utente che procede all'autenticazione. Questa impostazione richiede un parametro aggiuntivo (`password server =`).

La distinzione tra sicurezza a livello di server, utente e condivisione si applica a tutto il server. Nella configurazione di un server non è possibile applicare la sicurezza a livello di condivisione a singole condivisioni e la sicurezza a livello di utente ad altre condivisioni. È tuttavia possibile eseguire un server Samba separato per ogni indirizzo IP configurato nel sistema.

Ulteriori informazioni su questo argomento sono disponibili nella documentazione HOWTO di Linux su Samba. Nel caso di più server in un sistema prestare attenzione alle opzioni `interfaces` e `bind interfaces only`.

SUGGERIMENTO

Per le attività di amministrazione più semplici del server Samba è inoltre disponibile il programma swat che fornisce una semplice interfaccia Web con la quale configurare il server Samba in modo agevole. In un browser Web aprire `http://localhost:901` ed eseguire il login come utente `root`. È tuttavia necessario attivare swat anche nei file `/etc/xinetd.d/samba` e `/etc/services`. Per eseguire questa operazione, in `/etc/xinetd.d/samba` modificare la riga `disable` in `disable = no`. Ulteriori informazioni su swat sono disponibili nella documentazione.

48.2 Samba come server di login

Nelle reti con predominanza di client Windows è spesso preferibile che gli utenti possano registrarsi solo con un account e una password validi. È possibile ottenere questo risultato con un server Samba. In una rete basata su Windows questo task viene gestito da un server Windows NT configurato come controller di dominio primario (PDC). Le voci

che è necessario creare nella sezione `[global]` di `smb.conf` sono riportate nell'Esempio 48.3, «Sezione global nel file smb.conf.» (p. 800).

Esempio 48.3 *Sezione global nel file smb.conf.*

```
[global]
  workgroup = TUX-NET
  domain logons = Yes
  domain master = Yes
```

Se vengono utilizzate password cifrate ai fini della verifica, che corrisponde all'impostazione di default nelle installazioni gestite correttamente di Microsoft Windows 9x, Microsoft Windows NT 4.0 dal Service Pack 3 e tutti i prodotti successivi, il server Samba dovrebbe essere in grado di gestirle. La voce `encrypt passwords = yes` nella sezione `[global]` abilita questa impostazione (di default in Samba versione 3). È inoltre necessario che gli account utente e le password siano in un formato di cifratura conforme a Windows. A questo scopo utilizzare il comando `smbpasswd -a name`. Creare l'account di dominio per i computer, necessario secondo il concetto di dominio di Windows NT, mediante i comandi seguenti:

Esempio 48.4 *Configurazione di un account computer.*

```
useradd hostname\$
smbpasswd -a -m hostname
```

Con il comando `useradd` viene aggiunto un segno di dollaro. Il comando `smbpasswd` consente di inserirlo automaticamente quando si utilizza il parametro `-m`. Nell'esempio di configurazione con commenti (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) sono incluse impostazioni che rendono automatico questo task.

Esempio 48.5 *Configurazione automatica di un account computer.*

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Per garantire l'esecuzione corretta di questo script da parte di Samba, scegliere un utente di Samba con le autorizzazioni di amministratore necessarie. Per effettuare questa operazione, selezionare un utente e aggiungerlo al gruppo `ntadmin`. A tutti gli utenti appartenenti a questo gruppo di Linux potrà quindi essere assegnato lo stato `Domain Admin` mediante il comando:

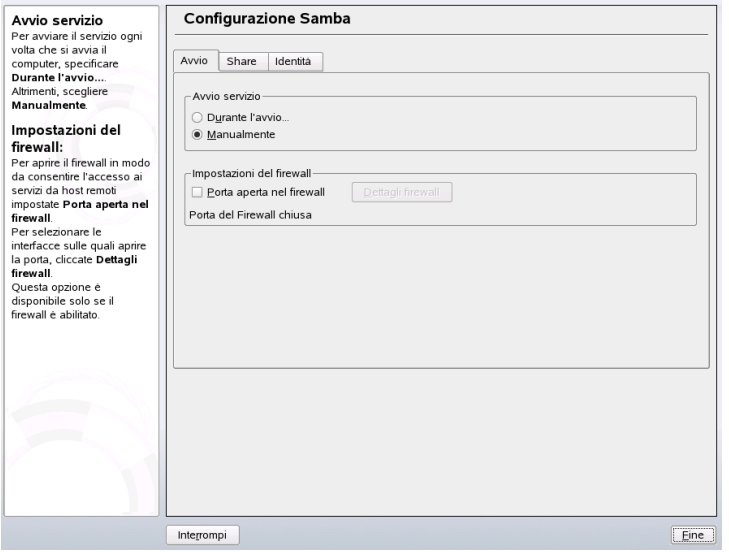
```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Ulteriori informazioni su questo argomento sono disponibili nel capitolo 12 della documentazione HOWTO di Linux su Samba disponibile nel percorso `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

48.3 Configurazione di un server Samba con YaST

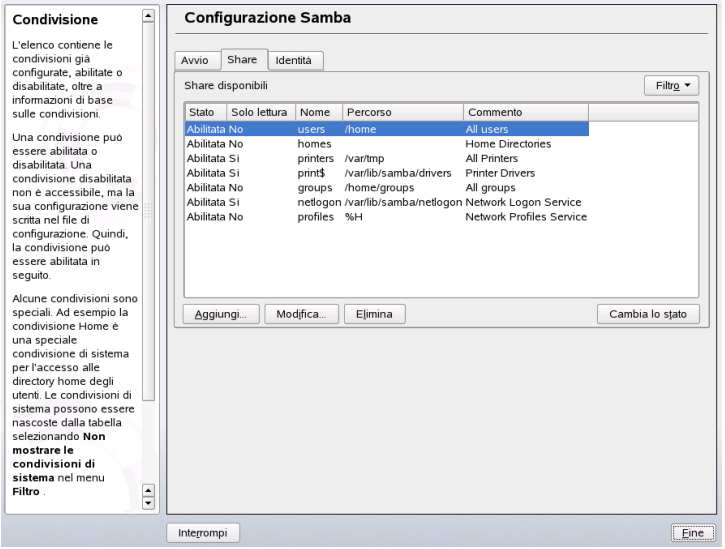
Iniziare la configurazione del server con la selezione del gruppo di lavoro o del dominio che dovrà essere controllato dal nuovo server Samba. Selezionarne uno esistente da *Gruppo di lavoro o nome di dominio* o immetterne uno nuovo. Nel passaggio successivo specificare se il server dovrà fungere da PDC (controller di dominio primario) o da BDC (controller di dominio di backup).

Figura 48.1 *Configurazione Samba - Avvio*



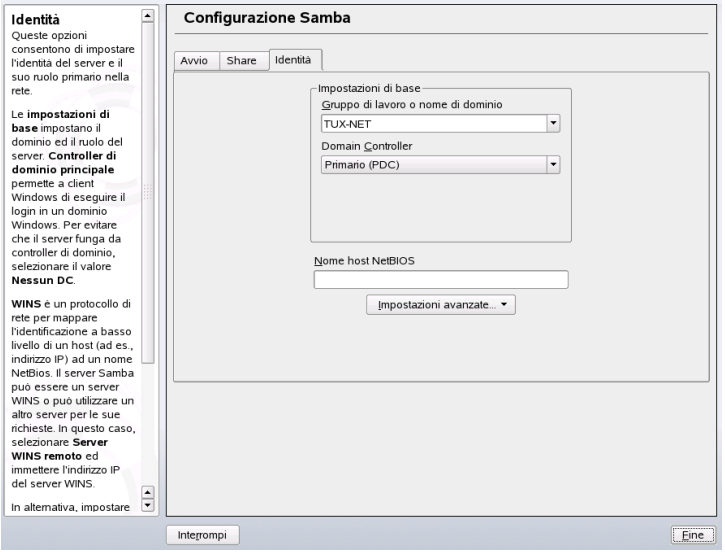
Attivare Samba in *Avvio* come illustrato nella Figura 48.1, «Configurazione Samba - Avvio» (p. 801). Utilizzare *Porta aperta nel firewall* e *Dettagli firewall* per modificare il firewall sul server in modo che le porte per i servizi `netbios-ns`, `netbios-dgm`, `netbios-ssn` e `microsoft-ds` siano aperte su tutte le interfacce esterne e interne per assicurare il funzionamento uniforme del server Samba.

Figura 48.2 *Configurazione Samba - Condivisione*



In *Condivisione* (Figura 48.2, «Configurazione Samba - Condivisione» (p. 802)) determinare le condivisioni Samba da attivare. Utilizzare *Cambia lo stato* per passare da *Attivo* a *Inattivo* e viceversa. Fare clic su *Aggiungi* per aggiungere nuove condivisioni.

Figura 48.3 *Configurazione Samba - Identità*



Nella sezione *Identità*, illustrata nella Figura 48.3, «Configurazione Samba - Identità» (p. 803), determinare il dominio al quale è associato l'host (*Impostazioni di base*) e la possibilità di utilizzare un nome host alternativo nella rete (*Nome host NetBIOS*).

48.4 Configurazione dei client

I client possono accedere al server Samba solo tramite TCP/IP. Non è infatti possibile utilizzare NetBEUI e NetBIOS tramite IPX con Samba.

48.4.1 Configurazione di un client Samba con YaST

Configurare un client Samba per accedere alle risorse (file o stampanti) nel server Samba. Immettere il dominio o il gruppo di lavoro nella finestra di dialogo *Gruppo di lavoro SAMBA*. Fare clic su *Sfoglia* per visualizzare tutti i gruppi e i domini disponibili che possono essere selezionati con il mouse. Se si seleziona *Utilizza anche informazioni SMB per autenticazione Linux* l'autenticazione utente viene eseguita sul server Samba.

Dopo aver completato tutte le impostazioni, fare clic su *Fine* per terminare la configurazione.

48.4.2 Windows 9x e ME

In Windows 9x e ME è già incluso il supporto predefinito per TCP/IP che tuttavia non viene installato di default. Per aggiungere il protocollo TCP/IP, passare a *Pannello di controllo → Sistema* e scegliere *Aggiungi → Protocolli → TCP/IP da Microsoft*. Dopo aver riavviato il computer Windows, per individuare il server Samba fare doppio clic sull'icona del desktop dell'ambiente di rete.

SUGGERIMENTO

Per utilizzare una stampante nel server Samba, installare il driver della stampante standard o Apple-PostScript dalla versione di Windows corrispondente. È preferibile collegare il driver della stampante alla coda della stampante Linux che accetta il formato di input PostScript.

48.5 Ottimizzazione

Nella configurazione di esempio inclusa nella versione di Samba è disponibile, tra l'altro, l'ottimizzazione `socket options`, la cui configurazione di default si riferisce a una rete Ethernet locale. Per ulteriori informazioni su `socket options`, fare riferimento alla relativa sezione della documentazione di `smb.conf` e alla documentazione di `socket(7)`. Ulteriori informazioni sono disponibili nel capitolo relativo all'ottimizzazione delle prestazioni di Samba della documentazione HOWTO di Linux su Samba.

La configurazione standard inclusa nel file `/etc/samba/smb.conf` è stata creata allo scopo di fornire impostazioni utili basate sulle impostazioni di default utilizzate dal team Samba. Non è tuttavia possibile fornire una configurazione pronta all'uso, specialmente per quanto riguarda la configurazione della rete e il nome del gruppo di lavoro. La configurazione di esempio con commenti `examples/smb.conf.SuSE` contiene informazioni utili per l'adattamento ai requisiti locali.

SUGGERIMENTO

Nella documentazione HOWTO di Linux su Samba fornita dal team Samba è inclusa una sezione relativa alla risoluzione dei problemi. Nella parte V del documento viene inoltre fornita una guida dettagliata per controllare la configurazione in uso.

Indice

Simboli

A

B

C

D

E

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y