Red Hat Linux 9

Red Hat Linux Customization Guide

Red Hat Linux 9: Red Hat Linux Customization Guide


Red Hat, Inc.

1801 Varsity Drive
Raleigh NC 27606-2072 USA
Telefono: +1 919 754 3700
Telefono: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 Stati Uniti

rhl-cg(IT)-9-Print-RHI (2003-02-20T01:08)

Il codice GPG della chiave security@redhat.com è:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Sommario

Introduzione

Benvenuti nella *Red Hat Linux Customization Guide*.

La *Red Hat Linux Customization Guide* contiene le informazioni necessarie per personalizzare il sistema Red Hat Linux in base alle vostre esigenze. Se cercate una guida dettagliata per la configurazione e la personalizzazione del vostro sistema, questo è il manuale che fa per voi. In questa guida sono illustrati molti argomenti di livello intermedio, quali:

- Configurazione di una scheda di interfaccia di rete (NIC)
- Esecuzione di un'installazione kickstart
- Configurazione di condivisioni di Samba
- Gestione del software con RPM
- Ottenere informazioni dal sistema
- Aggiornamento del kernel

Questo manuale è suddiviso nelle seguenti categorie principali:

- Installazione
- Rete
- Configurazione del sistema
- Gestione dei pacchetti

La lettura di questa guida presuppone una conoscenza di base del sistema Red Hat Linux. Se desiderate approfondire gli argomenti di base, come la configurazione del desktop o l'esecuzione di CD audio, consultate la *Red Hat Linux Getting Started Guide*. Se invece desiderate una guida su argomenti più complessi, una panoramica del filesystem di Red Hat Linux per esempio, consultate la *Red Hat Linux Reference Guide*.

Le versioni in formato HTML e PDF dei manuali ufficiali di Red Hat Linux sono disponibili su CD e online all'indirizzo http://www.redhat.com/docs/.

Nota Bene

Questo manuale riporta le informazioni più recenti, tuttavia è consigliabile leggere le *Release Note di Red Hat Linux* per informazioni che potrebbero non essere state disponibili prima del completamento della documentazione e che sono disponibili sul CD 1 di Red Hat Linux e online all'indirizzo:

```
http://www.redhat.com/docs/manuals/linux
```

1. Modifiche al manuale

Il manuale è stato aggiornato per includere le nuove caratteristiche di Red Hat Linux 9 e gli argomenti indicati dai nostri lettori. Tra le numerose modifiche apportate a questo manuale troverete:

Implementazione del disco Quotas

Questo nuovo capitolo spiega come configurare e gestire il disco quotas.

Configurazione di autenticazione

Questo capitolo spiega come usare lo **Strumento di Configurazione per l'Autenticazione**.

Configurazione utente

Questo capitolo é stato esteso per includere le utility della linea di comando per la gestione degli utenti e dei gruppi ed anche fornire una spiegazione delle conseguenze quando si aggiunge un nuovo utente al sistema.

Samba

Questo capitolo é stato esteso per poter includere il nuovo **Strumento di configurazione del server Samba**.

Configurazione della stampante

Questo capitolo é stato riscritto per la nuova interfaccia **Strumento di configurazione della stampante**, il nuovo **GNOME Print Manager**, e la nuova icona della stampante trasporta e rilascia "drag and drop" posizionata sul pannello.

kickstart

Le opzioni kickstart sono state aggiornate e includono le nuove opzioni in Red Hat Linux 9; anche il capitolo **Kickstart Configurator** è stato aggiornato e contiene le nuove caratteristiche.

Configurazione di rete

Questo capitolo é stato aggiornato per l'ultimissima interfaccia **Strumento di amministrazione di rete** e per i nuovi contenuti.

Configurazione dell'orario e della data

Questo capitolo é stato spostato su *Red Hat Linux Getting Started Guide*.

2. Convenzioni del documento

Consultando il presente manuale, vedrete alcune parole stampate con caratteri, dimensioni e stili differenti. Si tratta di un metodo sistematico per mettere in evidenza determinate parole; lo stesso stile grafico indica l'appartenenza a una specifica categoria. I tipi di parole rappresentate in questo modo possono essere:

`comando`

I comandi di Linux (e di altri sistemi operativi) vengono evidenziati così. Questo stile indica che potete digitare la parola o la frase nella linea di comando e premere [Invio] per eseguire il comando. A volte un comando contiene parole che dovrebbero essere rappresentate con uno stile diverso (come i nomi dei file). In questi casi, tali parole vengono considerate come parte integrante del comando e, dunque, l'intera frase viene visualizzata con lo stile del comando. Per esempio:

Utilizzate il comando `cat testfile` per visualizzare il contenuto di un file chiamato `testfile`, nella directory corrente.

`nome del file`

I nomi dei file, delle directory, dei percorsi e dei pacchetti RPM vengono rappresentati con questo stile grafico. Ciò significa che un file o una directory particolari hanno questo nome nel sistema Red Hat Linux. Per esempio:

Il file `.bashrc` nella vostra directory home contiene le definizioni e gli alias della shell bash per uso personale.

Il file `/etc/fstab` contiene le informazioni relative ai diversi dispositivi e filesystem di sistema.

Installate il pacchetto RPM `webalizer` per utilizzare un programma di analisi per il file di log del server Web.

applicazione

Questo stile grafico indica che il programma citato è un'applicazione per l'utente finale "end user" (contrariamente al software di sistema). Per esempio:

Utilizzate **Mozilla** per navigare sul Web.

[tasto]

I tasti della tastiera sono rappresentati in questo modo. Per esempio:

Per utilizzare la funzionalità [Tab], inserite una lettera e poi premete il tasto [Tab]. Viene visualizzato l'elenco dei file che iniziano con quella lettera.

[tasto]-[combinazione]

Una combinazione di tasti viene rappresentata in questo modo. Per esempio:

La combinazione [Ctrl]-[Alt]-[Backspace] chiude la sessione grafica e vi riporta alla schermata di login o nella console.

testo presente in un'interfaccia grafica

Un titolo, una parola o una frase di una schermata o di una finestra dell'interfaccia grafica, viene mostrato con questo stile: serve per identificare una particolare schermata o elemento dell'interfaccia grafica, per esempio il testo associato a una casella di controllo o a un campo). Qualche esempio:

Selezionate la casella di controllo **Richiedi password** se desiderate che lo screen saver richieda una password prima di scomparire.

livello superiore di un menu o di una finestra dell'interfaccia grafica

Quando vedete una parola scritta con questo stile grafico, si tratta della parola posta al livello superiore di un menu a tendina. Facendo clic sulla parola nella schermata dell'interfaccia grafica, dovrebbe comparire il resto del menu. Per esempio:

In corrispondenza di **File** in un terminale di GNOME è visualizzata l'opzione **Nuova scheda** che vi consente di aprire più prompt della shell nella stessa finestra.

Se dovete digitare una sequenza di comandi da un menu dell'interfaccia grafica, vi compare uno stile simile al seguente esempio:

Per avviare l'editor di testo **Emacs** fate clic sul **pulsante del menu principale** (sul pannello) => **Applicazioni** => **Emacs**.

pulsante di una schermata o una finestra dell'interfaccia grafica

Questo stile indica che il testo si trova su un pulsante in una schermata dell'interfaccia grafica e può essere selezionato con un clic del mouse. Per esempio:

Fate clic sul pulsante **Indietro** per tornare all'ultima pagina Web visualizzata.

`output del computer`

Quando trovate un testo scritto con questo stile grafico, si tratta del testo visualizzato dal computer sulla linea di comando: risposte a comandi che avete digitato, messaggi di errore e prompt interattivi di richiesta di input nel corso di script o programmi. Per esempio:

Utilizzate il comando `ls` per visualizzare il contenuto di una directory:

```
$ls
Desktopabout.htmllogspaulwesterberg.png
Mailbackupfilesmailreports
```

L'output restituito dal computer in risposta al comando (in questo caso, il contenuto della directory) viene mostrato con questo stile grafico.

`prompt`

Questo è lo stile con cui viene visualizzato un prompt, ovvero uno dei modi utilizzati dal computer per indicare che è pronto per ricevere un vostro input. Qualche esempio:

```
$
```

```
#
```

```
[stephen@maturin stephen]$
```

```
leopard login:
```

`input dell'utente`

Il testo che l'utente deve digitare sulla linea di comando o in un'area di testo di una schermata di un'interfaccia grafica è visualizzato con questo stile, come nell'esempio che segue:

Per avviare il programma di installazione in modalità di testo, dovete digitare il comando **`text`** al prompt `boot:`.

Inoltre, noi adottiamo diverse strategie per attirare la vostra attenzione su alcune informazioni particolari. In base all'importanza che tali informazioni hanno per il sistema, questi elementi verranno definiti "Nota Bene", "Suggerimento", "Importante", "Attenzione" o "Avvertenza". Per esempio:

Nota Bene

Ricordate che Linux distingue le minuscole dalle maiuscole. In altre parole, una rosa non è una ROSA né una rOsA.

Suggerimento

La directory `/usr/share/doc` contiene documentazione aggiuntiva per i pacchetti installati sul sistema.

Importante

Se modificate il file di configurazione DHCP, le modifiche non avranno effetto se non si riavvia il demone DHCP.

Attenzione

Non effettuate operazioni standard come utente root. Si consiglia di utilizzare sempre un account utente normale, a meno che non dobbiate amministrare il sistema.

Avvertenza

Se decidete di effettuare il partizionamento automatico, l'installazione server rimuove tutte le partizioni esistenti su tutti i dischi fissi installati. Non optate per questo tipo di installazione a meno che siate sicuri di non avere dati da salvare.

3. Prossimamente

La *Red Hat Linux Customization Guide* fa parte del crescente impegno di Red Hat nel fornire un supporto utile e immediato agli utenti di Red Hat Linux. Le prossime edizioni saranno sempre aggiornate e conterranno informazioni dettagliate sui nuovi tool e applicazioni sviluppati.

3.1. Inviateci suggerimenti!

Se individuate delle imprecisioni nella *Red Hat Linux Customization Guide*, o se pensate di poter contribuire al miglioramento di questo manuale, inviate i vostri suggerimenti al seguente indirizzo: (http://www.redhat.com/bugzilla) in relazione al componente `rhl-cg`.

Assicuratevi di menzionare l'identificatore del manuale:

```
rhl-cg(IT)-9-Print-RHI (2003-02-20T01:08)
```

In questo modo sapremo esattamente a quale manuale vi riferite.

Nel riportare un'imprecisione, cercate di essere il più specifici possibile: indicate il paragrafo e alcune righe di testo, in modo da agevolare la ricerca dell'errore.

4. Registrazione per ottenere l'assistenza

Se siete in possesso di un'edizione di Red Hat Linux 9, ricordatevi di registrarvi per godere dei benefici che vi spettano in qualità di clienti di Red Hat.

A seconda del prodotto Red Hat Linux ufficiale che avete acquistato, avrete diritto a tutti o ad alcuni dei benefici seguenti:

- Supporto Red Hat — il team di supporto vi fornirà assistenza in merito a questioni legate all'installazione.
- Red Hat Network — vi permette di aggiornare facilmente i pacchetti che avete installato e di ricevere avvisi relativi alla sicurezza specifici per il vostro sistema. Per maggiori dettagli, visitate il sito http://rhn.redhat.com.
- *Under the Brim: The Red Hat E-Newsletter* — Ogni mese, riceverete, direttamente da Red Hat, le ultime novità e le informazioni più aggiornate.

Per registrarvi, andate all;indirizzo http://www.redhat.com/apps/activate/. Troverete l'ID del prodotto su una scheda di colore nero, rosso e bianco all'interno della vostra confezione di Red Hat Linux

Per maggiori informazioni sull'assistenza tecnica per la versione ufficiale di Red Hat Linux, consultate l'appendice *Ottenere assistenza tecnica* nella *Red Hat Linux Installation Guide*.

Buona fortuna e grazie per aver scelto Red Hat Linux!

Il team di documentazione di Red Hat

I. File System

File system si riferiscono ai file e alle directory memorizzate su di un computer. Un file system puó avere formati diversi chiamati *tipi di file system*. Questi formati determinano come vengono memorizzate le informazioni come file o directory. Alcuni tipi di file system memorizzano delle copie redundant dei dati, mentre altri tipi rendono possibile un accesso piú veloci ai dischi fissi. Questa parte mostra i file system di tipo ext3, swap, RAID, e LVM. Inoltre viene riportato anche la utility `parted`, per la gestione delle partizioni.

Sommario

Capitolo 1.

Il filesystem ext3

A partire dalla versione 7.2 di Red Hat Linux, il filesystem predefinito è cambiato dal formato ext2 al filesystem *ext3* di tipo journaling.

1.1. Caratteristiche del filesystem ext3

Il filesystem ext3 è essenzialmente una versione avanzata del filesystem ext2. I miglioramenti apportati forniscono i seguenti vantaggi:

Disponibilità

Dopo una inaspettata mancanza di corrente o un crash del sistema (anche noto come *arresto di sistema non corretto*), è necessario che ogni filesystem ext2 montato sul computer sia controllato per la sua consistenza mediante il programma `e2fsck`. Si tratta di un processo che richiede molto tempo e che può ritardare significativamente l'avvio del sistema, in particolare con volumi di grandi dimensioni che contengono molti file. In questo periodo di tempo non è possibile accedere ai dati dei volumi.

Il servizio journaling fornito dal filesystem ext3 consente di evitare l'esecuzione del processo sopra descritto in caso di arresto non corretto del sistema. La verifica della consistenza in ext3 può avvenire solo in caso di alcuni problemi hardware, come quelle del disco fisso. Il tempo di recupero necessario al filesystem ext3 dopo un arresto del sistema non corretto non dipende dalla dimensione del filesystem o dal numero di file, ma piuttosto dalla dimensione del *journal* utilizzato per mantenere la compatibilità. La dimensione predefinita del journal richiede circa un secondo per il ripristino, in base alla velocità dell'hardware.

Integrità dei dati

Il filesystem ext3 garantisce una maggiore integrità dei dati nel caso in cui si verifichi un arresto del sistema non convenzionale. Il filesystem ext3 consente di scegliere il tipo e il livello di protezione per i vostri dati. Per default, Red Hat Linux 9 configura i volumi ext3 in modo tale che mantengano un elevato livello di integrità dei dati in relazione allo stato del filesystem.

Velocità

Benché riscriva alcuni dati più di una volta, ext3 ha, nella maggior parte dei casi, un velocità maggiore rispetto a ext2, perché il journaling di ext3 ottimizza lo spostamento della testina del disco fisso. Potete scegliere tra tre modalità di journaling per ottimizzare la velocità, ma in questo modo occorre scendere a compromessi con l'integrità dei dati.

Facilità di transizione

È semplice passare da ext2 a ext3 e trarre benefici da un filesystem di tipo journaling robusto, senza il bisogno di riformattare. Per ulteriori informazioni su come eseguire questa operazione, consultate la Sezione 1.3.

Se eseguite una nuova installazione di Red Hat Linux 9, il filesystem predefinito assegnato alle partizioni Linux del sistema sarà ext3. Se effettuate l'aggiornamento da una versione di Red Hat Linux che utilizza le partizioni ext2, il programma di installazione vi consentirà di convertire queste partizioni in ext3 senza alcuna perdita di dati. Per ulteriori informazioni, consultate l'Appendice intitolata *Aggiornamento del sistema* nella *Red Hat Linux Installation Guide*.

Le sezioni che seguono forniranno istruzioni dettagliate per la creazione e la regolazione delle partizioni ext3. Se disponete di partizioni ext2 in cui è in esecuzione Red Hat Linux 9, potete ignorare le sezioni relative al partizionamento e alla formattazione e passare direttamente a la Sezione 1.3.

1.2. Creazione di un filesystem ext3

Dopo l'installazione è talvolta necessario creare un nuovo filesystem ext3. Se, per esempio, aggiungete un nuovo disco fisso a un sistema Red Hat Linux, potete partizionare l'unità e utilizzare il filesystem ext3.

Per la creazione di un filesystem ext3 occorre attenersi alle seguenti istruzioni:

1. Create la partizione mediante il comando `parted` o `fdisk`.
2. Formattate la partizione del filesystem ext3 mediante il comando `mkfs`.
3. Assegnate un'etichetta alla partizione mediante il comando `e2label`.
4. Create il mount point.
5. Aggiungete la partizione al file `/etc/fstab`.

Per informazioni sull'esecuzione di queste istruzioni, consultate il Capitolo 5.

1.3. Conversione in un filesystem ext3

Il programma `tune2fs` può aggiungere un journal a un filesystem ext2 esistente senza modificare i dati già presenti nella partizione. Se il filesystem è già montato durante la transizione, il journal sarà visibile come file `.journal` nella directory root del filesystem. Al contrario, se il filesystem non è montato, il registro sarà nascosto e non verrà visualizzato.

Per convertire un filesystem ext2 in ext3, connettetevi come root e digitate:

```
/sbin/tune2fs -j /dev/hdbX
```

Nel comando riportato sopra sostituite /dev/*hdb* con il nome della periferica e *X* con il numero della partizione.

Dopo avere effettuato questa operazione, assicuratevi di cambiare il tipo di partizione da ext2 a ext3 nel file `/etc/fstab`.

Se eseguite la transizione del filesystem di root, dovrete utilizzare l'immagine `initrd` (o RAM disk) per l'avvio. Per effettuare questa operazione, eseguite il programma `mkinitrd`. Per informazioni sull'utilizzo del comando `mkinitrd`, digitate `man mkinitrd`. Assicuratevi inoltre che la configurazione GRUB o LILO carichi il file `initrd`.

Se non effettuate questa modifica, il sistema si avvierà comunque, ma il filesystem verrà montato come ext2 e non come ext3.

1.4. Ripristinare un filesystem ext2

Dato che ext3 è relativamente nuovo, alcune utilità non lo supportano ancora. Potrebbe, per esempio, essere necessario ridurre una partizione con `resize2fs`, che non supporta ancora il tipo ext3. In questo caso può essere necessario ripristinare temporaneamente un filesystem ext2.

Per ripristinare una partizione, è innanzitutto necessario smontare la partizione connettendovi come root e digitando:

```
umount /dev/hdbX
```

Nel comando riportato sopra sostituite /dev/*hdb* con il nome della periferica e *X* con il numero della partizione. Nella parte restante di questa sezione, i comandi di esempio utilizzeranno *hdb1* per questi valori.

Successivamente modificate il tipo di filesystem a ext2 digitando il comando riportato di seguito come root:

```
/sbin/tune2fs -O ^has_journal /dev/hdb1
```

Verificate la presenza di eventuali errori nella partizione digitando il comando riportato di seguito come root:

```
/sbin/e2fsck -y /dev/hdb1
```

Montate quindi di nuovo la partizione come filesystem ext2 digitando:

```
mount -t ext2 /dev/hdb1 /mount/point
```

Nel comando riportato sopra sostituite */mount/point* con il mount point della partizione.

Rimuovete quindi il file `.journal` a livello di root della partizione sostituendo la directory in cui è montato e digitando:

```
rm -f .journal
```

È ora disponibile la partizione ext2.

Se modificate in modo permanente una partizione ext2, ricordate di aggiornare il file `/etc/fstab`.

redhat.

Capitolo 2.

Spazio di swap

2.1. Che cos'è lo spazio di swap?

Lo *spazio di swap* in Linux è utilizzato quando la memoria fisica (RAM) è piena. Se il sistema necessita di una quantità maggiore di risorse di memoria e la memoria fisica è piena, le pagine inattive memorizzate verranno spostate nello spazio di swap. Anche se questo tipo di spazio può essere considerato utile per computer con una piccola quantità di RAM, non dovrebbe essere considerato un sostituto per una quantità maggiore di RAM. Lo spazio di swap si trova nei dischi fissi, che hanno un accesso più lento rispetto alla memoria fisica.

Lo spazio di swap può essere una partizione di swap dedicata (opzione consigliata), un file swap o una combinazione di partizioni e di file swap.

La dimensione dello spazio di swap dovrebbe essere uguale al doppio della RAM del vostro computer o a 32 MB, in base alla quantità più grande, ma non superiore a 2048 MB (o 2 GB).

2.2. Aggiunta dello spazio di swap

Talvolta è necessario aggiungere più spazio di swap dopo l'installazione. Potreste, per esempio, aggiornare la quantità di RAM del vostro sistema da 64 MB a 128 MB, ma con soli 128 MB di spazio swap disponibili. Potrebbe essere utile aumentare la quantità di spazio di swap a 256 MB se eseguite molte operazioni o utilizzate molte applicazioni che richiedono una grande quantità di memoria.

Sono disponibili due opzioni: aggiungere una partizione o un file swap. È consigliabile aggiungere una partizione di swap, ma talvolta non è semplice se non c'è spazio libero disponibile.

Per aggiungere una partizione di swap (presumendo che `/dev/hdb2` sia la partizione che desiderate aggiungere):

1. Il disco fisso non deve essere in uso (le partizioni non devono essere montate e lo spazio di swap non deve essere abilitato). Il modo più semplice di effettuare questa operazione è quello di avviare il sistema in modalità rescue. Per informazioni sull'avvio in modalità rescue, consultate il Capitolo 9. Quando viene richiesto di montare il file system, selezionate **Ignora**.

   In alternativa se l'unità non contiene alcuna partizione in uso, potete smontare tutte le partizioni e disattivare tutto lo spazio di swap del disco fisso con il comando `swapoff`.

2. Create la partizione di swap mediante `parted` o `fdisk`. L'utilizzo di `parted` è più semplice di `fdisk`. Per questo motivo verranno fornite informazioni solo su `parted`. Per creare una partizione di swap con `parted`:

   - Connettetevi come root e al prompt della shell digitate il comando `parted /dev/`*`hdb`*, in cui /dev/*`hdb`* è il nome del dispositivo per il disco fisso in cui è disponibile dello spazio libero.
   - Al prompt `(parted)` digitate **`print`** per visualizzare le partizioni esistenti e la quantità di spazio libero. I valori iniziali e finali sono espressi in megabyte. Determinate la quantità di spazio libero che si trova nel disco fisso e quanta ne desiderate allocare per una nuova partizione di swap.
   - Al prompt `(parted)` digitate **`mkpartfs`** ***`tipo-parte`*** **`linux-swap`** ***`inizio fine`***, in cui *`tipo-parte`* è una delle partizioni primarie, estese o logiche, *`inizio`* è il punto iniziale della partizione e *`fine`* ne rappresenta è il punto finale.


Avvertenza

Le modifiche hanno effetto immediato. Prestate quindi attenzione durante la digitazione.

- Uscite da `parted` digitando **`quit`**.

3. Ora che disponete della partizione di swap, utilizzate il comando `mkswap` per impostare la partizione. Connettetevi come root e al prompt della shell digitate quanto riportato di seguito:
   ```
   mkswap /dev/hdb2
   ```
4. Per abilitare immediatamente la partizione di swap, digitate il comando riportato di seguito:
   ```
   swapon /dev/hdb2
   ```
5. Per abilitarlo in fase di avvio, modificate `/etc/fstab` per includere quanto riportato di seguito:
   ```
   /dev/hdb2               swap                    swap    defaults        0 0
   ```
   Al successivo avvio del sistema verrà abilitata la nuova partizione di swap.
6. Dopo avere aggiunto la nuova partizione di swap e averla abilitata, accertatevi che sia effettivamente attiva visualizzando l'output del comando `cat/proc/swaps` o `free`.

Per aggiungere un file swap:

1. Determinate la dimensione del nuovo file swap e moltiplicatela per 1024 per stabilire la dimensione del blocco. Per esempio, la dimensione del blocco di un file swap di 64 MB è 65536.
2. Connettetevi come root e al prompt della shell digitate il comando riportato di seguito con `count` uguale alla dimensione del blocco desiderata:
   ```
   dd if=/dev/zero of=/swapfile bs=1024 count=65536
   ```
3. Impostate il file swap utilizzando il comando:
   ```
   mkswap /swapfile
   ```
4. Per abilitare immediatamente il file swap, ma non automaticamente all'avvio, digitate quanto segue:
   ```
   swapon /swapfile
   ```
5. Per abilitarlo in fase di avvio, modificate `/etc/fstab` per includere quanto riportato di seguito:
   ```
   /swapfile               swap                    swap    defaults        0 0
   ```
   Al successivo avvio del sistema, verrà abilitato il nuovo file swap.
6. Dopo avere aggiunto il nuovo file swap e averlo abilitato, accertatevi che sia effettivamente attivo visualizzando l'output del comando `cat/proc/swaps` o `free`.

2.3. Rimozione dello spazio di swap

Per rimuovere una partizione di swap:

1. Il disco fisso non deve essere in uso (le partizioni non devono essere montate e lo spazio di swap non deve essere abilitato). Il modo più semplice di effettuare questa operazione è quello di avviare il sistema in modalità rescue. Per informazioni sull'avvio in modalità rescue, consultate il Capitolo 9. Quando richiesto di montare il file system, selezionate **Ignora**.

   In alternativa se l'unità non contiene alcuna partizione in uso, potete smontare tutte le partizioni e disattivare tutto lo spazio di swap del disco fisso con il comando `swapoff`.
2. Connettetevi come root e al prompt della shell eseguite il comando riportato di seguito per accertarvi che la partizione di swap sia disabilitata. `/dev/hdb2` è la partizione di swap:
   ```
   swapoff /dev/hdb2
   ```
3. Rimuovete la voce relativa dal file `/etc/fstab`.

4. Rimuovete la partizione mediante il comando `parted` o `fdisk`. In questo contesto verrà esaminato solo `parted`. Per rimuovere la partizione con `parted`:
   - Connettetevi come root e al prompt della shell digitate il comando `parted /dev/`*`hdb`*, in cui /dev/*`hdb`* è il nome del dispositivo per il disco fisso con la partizione swap da rimuovere.
   - Al prompt `(parted)` digitate **`print`** per visualizzare le partizioni esistenti e determinare il numero minore di partizioni di swap che desiderate eliminare.
   - Al prompt `(parted)` digitate **`rm`** ***`MINOR`***, in cui *`MINOR`* è il numero minore delle partizioni che desiderate rimuovere.

      **Avvertenza**

     Le modifiche hanno effetto immediato. È quindi necessario digitare il numero minore corretto.
   - Digitate **`quit`** per uscire da `parted`.

Per rimuovere un file swap attenetevi alla seguente procedura:

1. Connettetevi come root e al prompt della shell eseguite il comando riportato di seguito per disabilitare il file swap (in cui `/swapfile` è il file swap):
   ```
   swapoff /swapfile
   ```
2. Rimuovete la voce relativa dal file `/etc/fstab`.
3. Rimuovete il file vero e proprio:
   ```
   rm /swapfile
   ```

2.4. Spostamento dello spazio di swap

Per spostare lo spazio di swap da un punto all'altro, attenetevi alle istruzioni per la rimozione dello spazio di swap e seguite le indicazioni per l'aggiunta dello spazio di swap.

Capitolo 3.

RAID (Redundant Array of Independent Disks)

3.1. Che cos'è RAID?

L'idea base di RAID è la combinazione di molteplici unità disco piccole e poco costose in un array, per migliorare le prestazioni e la ridondanza non conseguibili con un'unità singola, costosa e di maggiori dimensioni. Questo array di unità disco compare al computer come un'unica unità logica per la memorizzazione dei dati.

RAID è un metodo in cui le informazioni vengono distribuite a vari dischi, utilizzando tecniche come *disk striping* (RAID livello 0), *disk mirroring* (RAID livello 1) *disk striping con parità* (RAID livello 5) per ottenere ridondanza, ridurre la latenza e/o aumentare la larghezza di banda per la lettura o la scrittura dei dischi e accrescere la capacità di ripristino dopo un crash del sistema.

Il concetto fondamentale di RAID è la distribuzione uniforme dei dati in ogni unità dell'array. Per farlo, occorre suddividere i dati in vari *blocchi* di uguali dimensioni (spesso 32K o 64K, anche se sono disponibili in altre dimensioni). Ogni blocco viene scritto in un disco fisso a seconda del livello RAID utilizzato. Per la lettura dei dati vale invece il procedimento inverso e si ha l'illusione che le varie unità siano in effetti un unico disco.

3.2. A chi è consigliato l'uso di RAID?

Chiunque abbia bisogno di avere a disposizione grandi quantità di dati (per esempio un amministratore di sistema) può trarre molti vantaggi dall'uso della tecnologia RAID. Tra le ragioni principali per l'uso di RAID figurano:

- Maggiore velocità
- Capacità superiore di memorizzazione con l'uso di un unico disco virtuale
- Impatto minore in caso di errori nei dischi

3.3. RAID hardware e RAID software

RAID può essere implementato in due modi: tramite hardware o tramite software.

3.3.1. RAID hardware

Il sistema basato su hardware gestisce il sottosistema RAID indipendentemente dall'host e presenta a quest'ultimo solo un unico disco per ogni array RAID.

Un dispositivo RAID hardware si connette, per esempio, a un controller SCSI e presenta gli array RAID come un'unica unità SCSI. Un sistema RAID esterno sposta tutta l'"intelligenza" RAID in un controller che si trova in un sottosistema esterno del disco. L'intero sottosistema è collegato all'host mediante un controller SCSI normale e compare all'host come un singolo disco.

I controller RAID possono inoltre avere la forma di schede che *agiscono* come un controller SCSI per il sistema operativo ma che gestiscono autonomamente tutte le comunicazioni del disco effettive. In questi casi, le unità disco vanno inserite nel controller RAID proprio come in un controller SCSI, solo che in seguito tali unità vengono aggiunte alla configurazione del controller RAID e il sistema operativo non ne riconoscerà mai la differenza.

3.3.2. RAID software

Il RAID software implementa i vari livelli RAID nel codice disco del kernel (dispositivo a blocchi). Rappresenta la soluzione più economica, poiché non sono richiesti né schede costose né chassis hot-swap. [1] Il RAID software funziona anche con i dischi IDE o SCSI più economici. Grazie alle veloci CPU disponibili, le prestazioni del RAID software superano quelle del RAID hardware.

Il driver MD nel kernel Linux è un esempio di soluzione RAID del tutto indipendente dall'hardware. Le prestazioni di un array basato sul software dipendono dalle prestazioni e dal carico della CPU del server.

Per informazioni sulla configurazione del RAID software nel programma d'installazione di Red Hat Linux, consultate il Capitolo 10.

Per chi desidera maggiori informazioni sul RAID software, ecco un elenco delle caratteristiche più importanti:

- Processo di ricostruzione con modalità di threading
- Configurazione basata su kernel
- Portabilità di array tra macchine Linux senza obbligo di ricostruzione
- Ricostruzione di array tramite risorse del sistema di riserva
- Supporto unità hot-swappable
- Rilevamento automatico della CPU per usufruire di determinate ottimizzazioni del CPU

3.4. Livelli RAID e supporto lineare

RAID supporta diverse configurazioni che comprendono i livelli 0, 1, 4, 5 e la modalità lineare. Questi tipi di RAID sono definiti nel seguente modo:

- *Livello 0* — è spesso definito "striping" (a strisce). Si tratta di una tecnica di mappatura dei dati suddivisa in strisce e basata sulle prestazioni. Ciò significa che i dati scritti nell'array vengono suddivisi in strisce e scritti nei dischi membri dell'array, consentendo elevate prestazioni di I/O a bassi costi senza, però, fornire ridondanza. La capacità di memorizzazione di un array di livello 0 è pari alla capacità complessiva dei dischi membri di un RAID hardware o alla capacità complessiva delle partizioni membri in un RAID software.
- *Livello 1* — è definito anche "mirroring" ed è il più utilizzato. Questo livello fornisce ridondanza scrivendo gli stessi dati in ogni disco membro dell'array, ovvero effettuando una copia "identica" in ogni disco. Il mirroring resta un metodo molto diffuso per via della sua semplicità e del livello elevato di disponibilità dei dati. Il livello 1 opera con due o più dischi che possono utilizzare un accesso parallelo per indici elevati di trasferimento dati durante la lettura ma che operano indipendentemente per offrire maggiori operazioni I/O. Il livello 1 fornisce un'ottima affidabilità dei dati e accresce le prestazioni delle applicazioni a lettura intensiva a un costo però relativamente alto. [2] La capacità di memorizzazione dei dati è pari alla capacità di uno dei dischi rigidi copiati nel RAID hardware o di una delle partizioni copiate nel RAID software.

1. Uno chassis hot-swap vi consente di rimuovere un'unità disco senza spegnere il sistema.
2. Il livello 1 è piuttosto costoso perché scrive le stesse informazioni su tutti i dischi dell'array e ciò comporta un minore spazio su disco. Se per esempio avete installato il livello 1 RAID in modo tale che la vostra partizione di root (/) si trovi in due dischi da 40 GB, possedete in totale 80 GB, ma potete accedere solo a 40 GB. Gli altri fungono da "immagine" dei primi 40 GB.

- *Livello 4* — il livello 4 utilizza la parità [3] concentrata in un unico disco per proteggere i dati. È più adatta a operazioni I/O che a grandi trasferimenti di dati. Poiché il disco di parità può rappresentare un collo di bottiglia, il livello 4 è usato spesso in combinazione con altre tecnologie, come la cache write-back. Sebbene in alcuni schemi di partizionamento RAID il livello 4 rappresenti un'opzione, non lo è invece nelle installazioni RAID consentite in Red Hat Linux.[4] La capacità di memorizzazione di un RAID hardware di livello 4 è pari alla capacità complessiva dei dischi membri meno la capacità di un disco membro. La capacità di memorizzazione di un RAID software di livello 4 equivale alla capacità totale delle partizioni membri meno la dimensione di una delle partizioni (se sono di dimensioni uguali).
- *Livello 5* — si tratta del tipo più diffuso di RAID. Distribuendo la parità in alcuni o in tutti i dischi membri di un array, il livello 5 elimina la possibilità di colli di bottiglia durante la scrittura dei dati, tipici invece del livello 4. L'unico collo di bottiglia nelle prestazioni si verifica con il processo di calcolo della parità. Con le CPU e i RAID software più moderni questo non è, tuttavia, un problema così grave. Come con il livello 4, si ha come risultato delle prestazioni asimmetriche. La capacità di memorizzazione del RAID hardware di livello 5 è pari alla capacità dei dischi membri meno la capacità di un disco membro. La capacità di memorizzazione del RAID software di livello 5 corrisponde alla capacità delle partizioni membri meno la dimensione di una delle partizioni (se sono di dimensioni uguali).
- *RAID lineare* — la modalità lineare è un semplice insieme di unità che costituiscono un'unità virtuale più grande. Nel RAID lineare i blocchi di dati vengono allocati in modo sequenziale. Da un'unità membro si passa all'unità successiva solo al totale riempimento della prima. Questo insieme non offre vantaggi dal punto di vista delle prestazioni, poiché è improbabile che qualsiasi operazione I/O venga divisa tra le unità membri. Il RAID lineare inoltre non offre ridondanza e, in realtà, diminuisce l'affidabilità — se un disco membro si rovina, l'intero array non può essere utilizzato. La capacità è rappresentata dal totale di tutti i dischi membri.

3. Le informazioni sulla parità sono calcolate in base ai contenuti dei dischi membri dell'array. Queste informazioni possono essere utilizzate per ricostruire i dati se si verifica un errore nel disco dell'array. I dati ricostruiti possono poi essere utilizzati per soddisfare le richieste I/O del disco rovinato prima che venga sostituito e per reinserire i dati nel disco dopo la sostituzione.

4. Il livello 4 dispone della stessa quantità di spazio del livello 5, tuttavia il livello 5 presenta più vantaggi. È per questo motivo che il livello 4 non è supportato.

Capitolo 4.

Logical Volume Manager (LVM)

A partire da Red Hat Linux 8.0, LVM (Logical Volume Manager) è disponibile per l'allocazione del disco fisso.

LVM è un metodo di allocazione dello spazio del disco fisso in volumi logici che possono essere facilmente ridimensionati al contrario delle partizioni.

Con LVM il disco fisso o una serie di dischi fissi viene allocata a uno o più *volumi fisici*. Un volume fisico non può essere disteso su più di una unità.

I volumi fisici sono combinati in *gruppi di volumi logici*, a eccezione della partizione `/boot`, che non può trovarsi in un gruppo di volumi logici perché il boot loader non è in grado di leggerla. Se desiderate che la partizione root `/` si trovi su un volume logico, sarà necessario creare una partizione `/boot` separata che non fa parte di un gruppo di volumi.

Dato che un volume fisico non può essere disteso su più di una unità, se desiderate che il gruppo di volumi logici sia disteso su più di una unità, è necessario creare uno o più volumi fisici per unità.

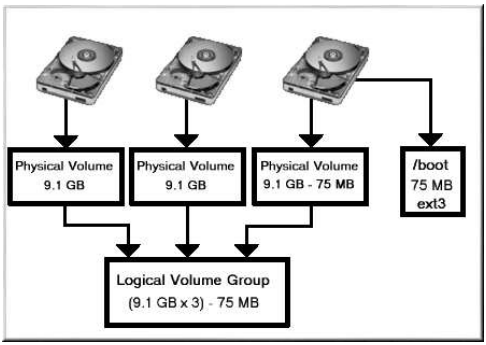

Figura 4-1. Gruppo di volumi logici

Il gruppo di volumi logici è suddiviso in *volumi logici*, a cui sono assegnati mount point come `/home` e `/` e tipi di file system come ext3. Quando le "partizioni" raggiungono la capacità completa, potete aggiungere spazio libero del gruppo di volumi logici al volume logico per aumentare la dimensione della partizione. Un nuovo disco fisso aggiunto al sistema può essere aggiunto al gruppo di volumi logici e i volumi logici che costituiscono le partizioni possono essere espansi.

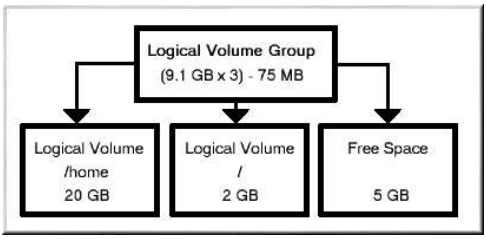

Figura 4-2. Volumi logici

Se, d'altro canto, un sistema viene partizionato con il file system ext3, il disco fisso viene suddiviso in partizioni di dimensioni stabilite. Se una partizione è piena, non è semplice espanderne la dimensione. Anche se la partizione viene spostata in un'altro disco fisso, lo spazio del disco fisso originale deve essere riallocato come partizione diversa o non utilizzata.

Il supporto LVM deve essere compilato nel kernel. Il kernel predefinito per Red Hat Linux 9 è compilato con il supporto LVM.

Per informazioni sulla configurazione dell'LVM durante il processo di installazione di Red Hat Linux, consultate il Capitolo 11.

redhat.

Capitolo 5.

Gestione dello spazio su disco

Dopo avere installato il sistema Red Hat Linux, si potrebbe visualizzare la tabella delle partizioni esistenti, modificare la dimensione, rimuovere o aggiungere le partizioni dallo spazio libero o da dischi fissi aggiuntivi. L'utilità `parted` consente di eseguire queste operazioni. Questo capitolo spiega come utilizzare `parted` per eseguire operazioni relative al file system. In alternativa potete utilizzare `fdisk` per eseguire la maggior parte delle attività descritte, a eccezione del ridimensionamento delle partizioni. Per ulteriori informazioni su `fdisk`, fate riferimento alla pagina man o a quella delle informazioni relativa a `fdisk`.

Se desiderate visualizzare la quantità di spazio su disco del sistema o verificarne l'impiego, consultate la Sezione 26.3.

Per utilizzare l'utility `parted`, è necessario che sia installato il pacchetto `parted`. Per avviare il comando `parted`, connettetevi come root e al prompt della shell digitate il comando `parted` *`/dev/hdb`*, in cui *`/dev/hdb`* rappresenta il nome del dispositivo per l'unità che desiderate configurare. Verrà visualizzato il prompt `(parted)`. Digitate `help` per visualizzare un elenco di comandi disponibili.

Se desiderate creare, rimuovere o ridimensionare una partizione, il dispositivo non deve essere in uso (le partizioni non devono essere montate e lo spazio di non deve essere abilitato). Il modo più semplice di effettuare questa operazione è quello di avviare il sistema in modalità rescue. Per informazioni sull'avvio in modalità rescue, consultate il Capitolo 9. Quando vi viene richiesto di montare il file system, selezionate **Ignora**.

In alternativa le partizioni non in uso contenute nell'unità possono essere smontate con il comando `umount` ed è possibile disabilitare tutto lo spazio di swap del disco fisso con il comando `swapoff`.

La Tabella 5-1 contiene un elenco di comandi `parted` comuni. Le sezioni che seguono spiegano alcuni di questi comandi in maggiore dettaglio.

Comando	Descrizione
`check` *`numero-minore`*	Esegue una semplice verifica del file system.
`cp` *`da a`*	Copia il file system da una partizione all'altra, mentre *`da`* e *`a`* rappresentano i numeri minori delle partizioni.
`help`	Visualizza l'elenco dei comandi disponibili.
`mklabel` *`etichetta`*	Crea un'etichetta del disco per la tabella delle partizioni.
`mkfs` *`numero-minore tipo-file-system`*	Crea un file system di tipo *`tipo-file-system`*
`mkpart` *`tipo-parte tipo-fs mb-inizio mb-fine`*	Crea una partizione senza creare un nuovo file system.
`mkpartfs` *`tipo-parte tipo-fs mb-inizio mb-fine`*	Crea una partizione e il file system specificato.
`move` *`numero-minore mb-inizio mb-fine`*	Sposta la partizione.
`print`	Visualizza la tabella delle partizioni.

Comando	Descrizione
`quit`	Esce da `parted`.
`resize` *`numero-minore mb-inizio mb-fine`*	Ridimensiona la partizione da *`mb-inizio`* a *`mb-fine`*.
`rm` *`numero-minore`*	Rimuove la partizione.
`select` *`dispositivo`*	Seleziona un dispositivo diverso da configurare.
`set` *`numero-minore flag stato`*	Imposta la flag di una partizione, mentre lo *`stato`* può essere attivo o disattivato.

Tabella 5-1. comandi di `parted`

5.1. Visualizzazione della tabella delle partizioni

Dopo l'avvio di `parted`, digitate il comando riportato di seguito per visualizzare la tabella delle partizioni:

```
print
```

Verrà visualizzata una tabella simile a quella riportata di seguito:

```
Disk geometry for /dev/hda: 0.000-9765.492 megabytes
Disk label type: msdos
Minor    Start       End     Type      Filesystem  Flags
1          0.031   101.975  primary   ext3        boot
2        101.975   611.850  primary   linux-swap
3        611.851   760.891  primary   ext3
4        760.891  9758.232  extended              lba
5        760.922  9758.232  logical   ext3
```

La prima riga presenta la dimensione del disco, la seconda visualizza il tipo di etichetta del disco e l'output rimanente mostra la tabella delle partizioni. In questa tabella il numero **Minor** è il numero di partizione. La partizione con il numero minore 1 corrisponde, per esempio, al file `/dev/hda1`. I valori **Inizio** e **Fine** sono espressi in megabyte. **Tipo** può essere un valore primario, esteso o logico. Il **Filesystem** è il tipo di file system, che può essere rappresentato da ext2, ext3, FAT, hfs, jfs, linux-swap, ntfs, reiserfs, hp-ufs, sun-ufs o xfs. La colonna **Flags** elenca i flag impostati per la partizione. I flag disponibili sono boot, root, swap, hidden, raid, lvm o lba.

Suggerimento

Per selezionare un dispositivo diverso senza dover riavviare il comando `parted`, utilizzando il comando `select` seguito dal nome del dispositivo, per esempio `/dev/hdb`. Potrete quindi visualizzare la relativa tabella delle partizioni o configurarlo.

5.2. Creazione di una partizione

Avvertenza

Non tentate di creare una partizione per un dispositivo in uso.

Prima di creare una partizione, eseguite l'avvio in modalità rescue (o smontate tutte le partizioni del dispositivo e disattivate tutto lo spazio di swap).

Avviate il comando `parted`, dove /dev/*hda* rappresenta il dispositivo in cui creare la partizione:

```
parted /dev/hda
```

Visualizzate la tabella delle partizioni corrente per determinare se è disponibile spazio libero sufficiente:

```
print
```

In caso contrario, potete ridimensionare una partizione esistente. Per informazioni, consultate la Sezione 5.4.

5.2.1. Creazione della partizione

Dalla tabella delle partizioni determinate i punti iniziale e finale della nuova partizione e il tipo di partizione. Potete disporre solo di quattro partizioni primarie (senza partizione estesa) in un dispositivo. Se sono necessarie più di quattro partizioni, potete disporre di tre partizioni primarie, una estesa e più partizioni logiche all'interno di quella estesa. Per una descrizione generale delle partizioni del disco, consultate l'appendice relativa all'*introduzione al partizionamento del disco* nella *Red Hat Linux Installation Guide*.

Per creare, per esempio, una partizione primaria con un file system ext3 da 1024 megabyte a 2048 megabyte in un disco fisso, digitate il comando riportato di seguito:

```
mkpart primary ext3 1024 2048
```

Suggerimento

Se, al contrario, utilizzate il comando `mkpartfs`, il file system verrà creato dopo la partizione. Tuttavia, `parted` non supporta la creazione di un file system ext3. Per questo motivo, se desiderate creare un file system ext3, utilizzate il comando `mkpart` e create il file system con il comando `mkfs` come verrà descritto in seguito. Il comando `mkpartfs` funziona per il tipo di file system linux-swap.

Le modifiche hanno effetto subito dopo avere premuto [Invio], quindi è consigliabile controllare il comando prima di eseguirlo.

Dopo avere creato la partizione, utilizzate il comando `print` per confermare che si trova nella tabella delle partizioni con il tipo di partizione, il tipo di file system e la dimensione corretti. Ricordate inoltre il numero minore della partizione per essere in grado di assegnarle un'etichetta. Dovrebbe anche essere possibile visualizzare l'output di

```
cat /proc/partitions
```

per assicurarvi che il kernel riconosca la nuova partizione.

5.2.2. Formattazione della nuova partizione

La partizione non dispone ancora del file system. Create il file system mediante il comando riportato di seguito:

```
/sbin/mkfs -t ext3 /dev/hdb3
```


Avvertenza

La formattazione della partizione cancellerà in modo permanente tutti i dati attualmente presenti in tale partizione.

5.2.3. Assegnazione di un'etichetta alla partizione

Assegnate quindi un'etichetta alla partizione. Se, per esempio, la nuova partizione fosse `/dev/hda3` e desiderate assegnarle l'etichetta `/work` utilizzate il comando riportato di seguito:

```
e2label /dev/hda3 /work
```

Per default, il programma di installazione di Red Hat Linux utilizza il mount point della partizione come etichetta per fare in modo che si tratti di un elemento unico. Potete comunque utilizzare qualsiasi etichetta.

5.2.4. Creazione del mount point

Connettetevi come root e create il mount point:

```
mkdir /work
```

5.2.5. Aggiunta al file `/etc/fstab`

Connettetevi come root e modificate il file `/etc/fstab` per includere la nuova partizione. La nuova riga dovrebbe essere simile a quella riportata di seguito:

```
LABEL=/work           /work                   ext3    defaults        1 2
```

La prima colonna dovrebbe contenere `LABEL=` seguito dall'etichetta assegnata alla partizione. La seconda colonna dovrebbe contenere il mount point per la nuova partizione e la colonna successiva il tipo di file system, per esempio ext3 o swap. Se sono necessarie ulteriori informazioni sul formato, consultate la pagina man relativa al comando `man fstab`.

Se la quarta colonna è rappresentata dal termine `defaults`, la partizione verrà montata in fase di avvio. Per montare la partizione senza riavviare, connettetevi come root e digitate il comando:

```
mount /work
```

5.3. Rimozione di una partizione


Avvertenza

Non tentate di rimuovere una partizione in un dispositivo in uso.

Prima di rimuovere una partizione, eseguite l'avvio in modalità rescue oppure smontate tutte le partizioni del dispositivo e disattivate lo spazio di swap.

Avviate il comando `parted`, dove /dev/*hda* rappresenta il dispositivo in cui rimuovere la partizione:

```
parted /dev/hda
```

Visualizzate la tabella delle partizioni corrente per determinare il numero minore della partizione da rimuovere:

```
print
```

Rimuovete la partizione con il comando `rm`. Per rimuovere, per esempio, la partizione con il numero minore 3 utilizzate il comando riportato di seguito:

```
rm 3
```

Le modifiche hanno effetto subito dopo avere premuto [Invio], quindi è consigliabile controllare il comando prima eseguirlo.

Dopo avere rimosso la partizione, utilizzate il comando `print` per confermare l'avvenuta rimozione dalla tabella delle partizioni. Dovrebbe anche essere possibile visualizzare l'output di

```
cat /proc/partitions
```

per assicurarvi che il kernel sappia che la partizione è stata rimossa.

L'ultima fase è costituita dalla rimozione della partizione dal file `/etc/fstab`. Localizzate la riga che dichiara la partizione rimossa ed eliminatela dal file.

5.4. Ridimensionamento di una partizione

 **Avvertenza**

Non tentate di ridimensionare una partizione in un dispositivo in uso.

Prima di ridimensionare una partizione, eseguite l'avvio in modalità rescue oppure smontate tutte le partizioni del dispositivo e disattivate lo spazio di swap.

Avviate il comando `parted`, dove /dev/*hda* rappresenta il dispositivo in cui ridimensionare la partizione:

```
parted /dev/hda
```

Visualizzate la tabella delle partizioni corrente per determinare il numero minore della partizione da ridimensionare oltre ai punti iniziale e finale della partizione stessa:

```
print
```

 **Avvertenza**

Lo spazio utilizzato della partizione da ridimensionare non deve essere superiore alla nuova dimensione.

Per ridimensionare la partizione, utilizzate il comando `resize` seguito dal numero minore della partizione, dal punto iniziale e dal punto finale espressi in megabyte. Per esempio:

```
resize 3 1024 2048
```

Al termine del ridimensionamento della partizione, utilizzate il comando `print` per confermare che il ridimensionamento è avvenuto in modo corretto e che il tipo di partizione e il file system sono appropriati.

Dopo il riavvio del sistema in modalità normale, utilizzate il comando `df` per assicurarvi che la partizione sia stata montata e che venga riconosciuta con la nuova dimensione.

Capitolo 6.

Implementazione del disk Quotas

In aggiunta al controllo dello spazio del disco usato su di un sistema (consultare la Sezione 26.3.1), lo spazio del disco puó essere ristretto implementando il disco quotas, tale implementazione consente all'amministratore del sistema di essere allertato prima che un utente consumi troppo spazio o una partizione diventi piena.

Il disk quotas puó essere configurato sia per utenti singoli che per gruppi di utenti. Questo tipo di flessibilitá rende possibile che un utente possa avere una piccola quota da gestire per un file "personal" (come ad esempio email e riporti), permettendo ai progetti sui quali l'utente lavora, di avere piú quotas (assumendo che vengano assegnati ai progetti, i propri gruppi).

In aggiunta, il quotas puó essere impostato non solo per controllare il numero dei blocchi del disco, ma anche per controllare il numero di inode. Perché gli inode sono usati per contenere informazioni inerenti ai file, ció permette un controllo sui numeri di file che possono essere creati.

The `quota` RPM must be installed to implement disk quotas. For more information on installing RPM packages, refer to Parte V.

6.1. Configurazione del Disk Quotas

Per implementare il disk quotas, usare le seguenti fasi:

1. Abilitare quotas per ogni file system, modificando `/etc/fstab`
2. Rimontare il file system
3. Creare i file quotas e generate la tabella d'uso del disco
4. Assegnare quotas

Ogni singolo passo viene analizzato in dettaglio nelle seguenti sezioni.

6.1.1. Abilitazione di Quotas

Come root, usare l'editor di testo di vostra scelta, aggiungere l'opzione `usrquota` e/o `grpquota` ai file system che richiedono quotas:

```
LABEL=/           /              ext3    defaults        1 1
LABEL=/boot       /boot          ext3    defaults        1 2
none              /dev/pts       devpts  gid=5,mode=620  0 0
LABEL=/home       /home          ext3    defaults,usrquota,grpquota 1 2
none              /proc          proc    defaults        0 0
none              /dev/shm       tmpfs   defaults        0 0
/dev/hda2         swap           swap    defaults        0 0
/dev/cdrom        /mnt/cdrom     udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0          /mnt/floppy    auto    noauto,owner,kudzu 0 0
```

In questo esempio, il file system `/home` possiede sia l'utente che il gruppo quotas entrambi abilitati.

6.1.2. Rimontare i file system

Dopo aver aggiunto le opzioni `userquota` e `grpquota`, rimontare ogni file system sul quale é stato modificato la entry `fstab`. Se il file system non é usato in alcun processo, usare il comando `umount` seguito da `mount` per rimontare il file system. Se invece esso é usato, il metodo piú facile per rimontare il file system é quello di riavviare il sistema.

6.1.3. Creazione dei file Quota

Dopo che ogni file sistem "abilitato-quota" é stato rimontato, il sistema é capace di lavorare con il disk quotas. Tuttavia, il file system per se stesso, non é pronto per il supporto di quotas. La fase successiva é quella di eseguire il comando `quotacheck`.

Il comando `quotacheck` esamina i file systema "abilitati-quota" e costruisce una tabella dell'uso del disco corrente per file system. La tabella viene usata per aggiornare la copia dell'uso del disco del sistema operativo. In aggiunta, i file del disk quota del file system, vengono aggiornati.

Per creare i file quota (`aquota.user` e `aquota.group`) sul file system, usare l'opzione `-c` del comando `quotacheck`. Per esempio, se l'utente o il gruppo quotas sono abilitati per la partizione `/home`, creare i file nella `/home` directory:

```
quotacheck -acug /home
```

L'opzione `-a` significa che tutti i file system non-NFS in `/etc/mtab` sono controllati per vedere se i quotas sono abilitati. L'opzione `-c` specifica che i file quota dovrebbero essere creati per ogni file system abilitati ai quotas, la `-u` specifica il controllo di utenti quotas, e l'opzione `-g` specifica di controllare per gruppi di quotas.

Se non sono specificate le opzioni `-u` o `-g`, viene creato solo l'utente del file quota. Se solo `-g` viene specificato, viene creato allora solo il gruppo quota.

Dopo che vengono creati i file, eseguite il seguente comando per generare la tabella dell'uso corrente del disco, per file system ai quali é abilitato il quotas:

```
quotacheck -avug
```

Le opzioni usate sono le seguenti:

- `a` — Controllare tutti i file system abilitati-quota montati in modo locale.
- `v` — Mostrate le informazioni sulla stato verbose, durante la prosecuzione del controllo quota
- `u` — Controllare le informazioni dell'utente del disk quota
- `g` — Controllare le informazioni del gruppo del disk quota

Dopo che `quotacheck` ha terminato l'esecuzione, i file quota corrispondenti al quotas abilitato (utente e/o gruppo) sono popolati con dei dati, per ogni file system abilitati-quota, come ad esempio `/home`.

6.1.4. Assegnare quotas ad un utente

L'ultima fase é quella di assegnare il disk quotas con il comando `edquota`.

Per configurare il quota per un utente, come utente root in un prompt della shell, eseguire il comando:

```
edquota username
```

Effettuare questa fase per ogni utente sul quale volete implementare il quota. Per esempio, se il quota é abilitato in `/etc/fstab` per la partizione `/home` (`/dev/hda3`) e il comando `edquota testuser` é eseguito, viene mostrato quanto segue nell'editor configurato come il default per il sistema:

```
Disk quotas for user testuser (uid 501):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/hda3                    440436          0          0      37418        0        0
```

Nota Bene

L'editor di testo definito dalla variabile dell'ambiente EDITOR é usato da `edquota`. Per cambiare l'editor, impostare la variabile dell'ambiente EDITOR per il percorso completo dell'editor di vostra scelta.

La prima colonna é il nome del file system che ha abilitato un quota. La seconda colonna mostra il numero di blocchi l'utente stá usando. Le successive due colonne sono usate per impostare i limiti soft e hard del blocco per l'utente sul file system. La colonna `inodes` mostra il numero di inodes che l'utente stá utilizzando. Le ultime due colonne sono usate per impostare i limiti inode soft e hard, per l'utente sul file system.

Un limite hard é l'ammontare massimo di spazio del disco che un utente o un gruppo puó utilizzare. Una volta raggiunto questo limite, non si puó utilizzare nessun altro spazio.

Il limite soft definisce l'ammontare massimo di spazio che puó essere usato. Tuttavia, a differenza del limite hard, il limite soft puó essere superato per un certo limite di tempo. Quel periodo é chiamato *periodo di grazia*. Tale periodo puó essere espresso in secondi, minuti, ore, settimane e mesi.

Se uno dei valori é impostato su zero, quel limite non é impostato. Cambiare i limiti desiderati, nell'editor di testo. Per esempio:

```
Disk quotas for user testuser (uid 501):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/hda3                    440436     500000     550000      37418        0        0
```

Per verificare che il quota per un utente sia stato impostato, usare il comnado:

```
quota testuser
```

6.1.5. Assegnare quota ad un gruppo

Quotas puó anche essere assegnato ad un gruppo. Per esempio, per assegnare un quota per il gruppo `devel`, usare il comando (il gruppo deve esistere prima di impostare il quota):

```
edquota -g devel
```

Questo comando mostra il quota esistente per il gruppo in un editor di testo:

```
Disk quotas for group devel (gid 505):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/hda3                    440400          0          0      37418        0        0
```

Modificare i limiti, salvare il file, e configurare poi il quota.

Per verificare che il gruppo del quota é stato impostato, usare il comando:

```
quota -g devel
```

6.1.6. Assegnare quotas ad un file system

Per assegnare quota ad ogni file system abilitato per quotas, usare il comando:

```
edquota -t
```

Come gli altri comandi `edquota`, esso apre il quotas corrente per il file system nell'editor di testo:

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
  Filesystem             Block grace period     Inode grace period
  /dev/hda3                     7days                  7days
```

Cambiare il periodo di grazia del blocco o dell'inode, salvare i cambiamenti, e uscire dall'editore di testo.

6.2. Gestione del Disk Quotas

Se vengono implementati i quota, essi necessitano di manutenzione, e cioé controllando se si eccede i quota e assicurarsi che gli stessi siano accurati. Naturalmente, se gli utenti eccedono sistematicamente i loro quota o raggiungono i loro limiti soft, esso non dipende dall'amministratore del sistema. Egli puó aiutare un utente nell'uso di minor spazio o aumentare il disk quota se necessario.

6.2.1. Riportare su di un Disk Quotas

Creare un riporto sull'uso del disco, comporta l'esecuzione della utility `repquota`. Per esempio, il comando `repquota /home` fornisce il seguente output:

```
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --      36       0       0              4     0     0
tfox      --     540       0       0            125     0     0
testuser  --  440400  500000  550000          37418     0     0
```

Per visualizzare l'uso del disco per tutti i file system abilitati-quota, usare il comando:

```
repquota -a
```

Anche se il riporto é facile da leggere, bisognerebbe spiegare alcuni punti. Il `--` visualizzato dopo ogni utente, é un mezzo semplice per determinare se il blocco o l'inode é stato superato. Se il limite soft é stato superato, apparirá un `+` al posto del corrispondente `-`; il primo `-` rappresenta il limite del blocco, e il secondo rappresenta il limite dell'inode.

Le colonne `grace` sono normalmente vuote. Se il limite soft é stato superato, la colonna contiene l'ammontare del tempo di grazia o grace restante. Se tale periodo é terminato, apparirá `none` al suo posto.

6.2.2. Mantenere dei quota accurati

Se un file system non viene montato in modo pulito (per esempio, a causa di un crash del sistema) é necessario eseguire `quotacheck`. Tuttavia, `quotacheck` puó essere eseguito in modo regolare, anche se il sistema non ha avuto problemi. L'esecuzione periodica di questi comandi mantiene i quota molto piú accurati (le opzioni usate sono state descritte in la Sezione 6.1.1):

```
quotacheck -avug
```

Il modo piú semplice per eseguirlo periodicamente, é quello di usare `cron`. Come utente root, potete usare sia il comando `crontab -e` per organizzare periodicamente un `quotacheck` o posizionare uno script che esegue `quotacheck` in qualsiasi delle seguenti directory (usando l'intervallo che si addice meglio alle vostre esigenze):

- `/etc/cron.hourly`
- `/etc/cron.daily`
- `/etc/cron.weekly`
- `/etc/cron.monthly`

Le statistiche piú accurate che si possono ottenere, si hanno quando i file system non sono in uso attivo. Il task di cron dovrebbe essere programmato quando il file system viene usato poco. Se questo periodo varia a seconda dei file system con quota, eseguire `quotacheck` per ognuno di esso in momenti diversi con task cron multipli.

Consultare Capitolo 28 per maggiori informazioni sulla configurazione di `cron`.

6.2.3. Abilitare e disabilitare

É possibile disabilitare quota senza impostarli a zero. Per eseguire tale compito, usare il seguente comando:

```
quotaoff -vaug
```

Se non vengono specificate le opzioni `-u` o `-g`, vengono disabilitati solo i quota dell'utente. Se viene specificato solo `-g`, vengono disabilitati solo i quota del gruppo.

Per abilitare quota, usare il comando `quotaon` con le stesse opzioni.

Per esempio, abilitare i quota dell'utente e del gruppo per tutti i file system:

```
quotaon -vaug
```

Per abilitare i quota per un file system specifico, come ad esempio `/home`:

```
quotaon -vug /home
```

Se non vengono specificate le opzioni `-u` o `-g`, vengono disabilitati solo i quota dell'utente. Se viene specificato solo `-g`, vengono disabilitati solo i quota del gruppo.

6.3. Risorse aggiuntive

Per maggiori informazioni sui disk quota, consultate le seguenti risorse.

6.3.1. Documentazione installata

- Le pagine man `quotacheck`, `edquota`, `repquota`, `quota`, `quotaon`, e `quotaoff`

6.3.2. Libri relativi

- *Red Hat Linux System Administration Primer* — Disponibile su http://www.redhat.com/docs e su CD di documentazione, questo manuale contiene delle informazioni sulla gestione della memorizzazione (incluso i disk quota) per amministratori di sistema Red Hat Linux nuovi.

II. Informazioni inerenti l'installazione

Il *Red Hat Linux Installation Guide* spiega l'installazione di Red Hat Linux ed alcuni troubleshooting post-installazione di base. Tuttavia, sono riportate in questo manuale anche delle opzioni di installazione avanzate. Questa sezione fornisce le istruzioni per *kickstart* (una tecnica di installazione automatica), le modalitá di recupero del sistema (come effettuare l'avvio del vostro sistema se esso non effettua tale avvio in un runlevel normale), come configurare RAID durante l'installazione, e come configurare LVM durante l'installazione. Usate questa sezione insieme con il *Red Hat Linux Installation Guide* per effettuare qualsiasi di questi compiti avanzati di installazione.

Sommario

redhat.

Capitolo 7.

Installazioni kickstart

7.1. Cosa sono le installazioni kickstart?

Molti amministratori di sistema preferirebbero utilizzare un metodo di installazione automatico per installare Red Hat Linux sulle proprie macchine. Per rispondere a tale esigenza, Red Hat ha creato il metodo di installazione kickstart. Con l'uso di kickstart, un amministratore di sistema può creare un singolo file contenente le risposte a tutte le domande che vengono poste durante un'installazione standard di Red Hat Linux.

I file kickstart possono essere memorizzati su un unico server e letti dai singoli computer durante l'installazione. Questo metodo d'installazione può supportare l'uso di un singolo file kickstart per installare Red Hat Linux su varie macchine, rendendolo così ideale per gli amministratori di rete e di sistema.

Il metodo kickstart vi permette di automatizzare l'installazione di Red Hat Linux.

7.2. Come eseguire un'installazione kickstart?

Le installazioni kickstart richiedono l'installazione del software da un CD o da un disco fisso locale oppure via rete tramite i protocolli NFS, FTP o HTTP.

Per utilizzare kickstart occorre:

1. Creare un file kickstart.
2. Creare un dischetto di avvio con il file kickstart oppure rendere il file disponibile sulla rete.
3. Rendere disponibile l'albero di installazione.
4. Avviare l'installazione kickstart.

Il presente capitolo illustra in dettaglio le procedure presentate.

7.3. Creazione di un file kickstart

Ora che avete qualche nozione sul processo d'installazione basato sul metodo kickstart, possiamo esaminare il file kickstart. Il file kickstart è un semplice file di testo, contenente un elenco di elementi, ognuno dei quali è identificato da una parola chiave. Potete creare questo file modificando una copia del file `sample.ks` che si trova nella directory `RH-DOCS` del CD di documentazione di Red Hat Linux, usando l'applicazione **Kickstart Configurator**; o creandone uno nuovo. Il programma di installazione di Red Hat Linux crea anche un file kickstart campione basato sulle opzioni selezionate durante l'installazione e che viene inserito nel file `/root/anaconda-ks.cfg`. Potete anche modificarlo con qualunque editor di testo o word processor con cui sia possibile salvare il file in formato ASCII.

Prima di creare il file kickstart dovete tenere presente alcuni punti importanti:

- Le sezioni devono essere specificate *in ordine*. Gli elementi all'interno delle sezioni non devono essere in un ordine specifico se non specificato diversamente. L'ordine delle sezioni è il seguente:
  - Sezione comando — per ottenere un elenco delle opzioni di kickstart, consultate la la Sezione 7.4. È necessario includere le opzioni richieste.

- Sezione `%packages` — per maggiori dettagli, consultate la Sezione 7.5.
- Sezioni `%pre` e `%post` — queste due sezioni non sono strettamente necessarie o non devono seguire un ordine particolare. Per maggiori dettagli, consultate la Sezione 7.6 e la Sezione 7.7.

- Le opzioni non richieste possono essere omesse.
- Se omettete una qualsiasi opzione richiesta, il programma di installazione vi richiede una risposta correlata all'opzione, proprio come durante un'installazione standard. Una volta fornita tale risposta, l'installazione prosegue senza ulteriori richieste (a meno che, ovviamente, non venga individuata un'altra opzione mancante).
- Le righe che iniziano con il simbolo cancelletto ("#") vengono considerate come commenti e dunque ignorate.
- Per gli *aggiornamenti* di kickstart, sono richieste le seguenti opzioni:
  - Lingua
  - Supporto per la lingua
  - Metodo di installazione
  - Specifiche del dispositivo (qualora sia necessario un dispositivo per eseguire l'installazione)
  - Configurazione della tastiera
  - La parola chiave `upgrade`
  - Configurazione del boot loader

  Se viene specificata qualsiasi altra opzione per un aggiornamento, queste opzioni verranno ignorate (compresa la selezione dei pacchetti).

7.4. Opzioni di kickstart

Le seguenti opzioni possono essere inserite in un file kickstart. Se preferite usare un'interfaccia grafica per la creazione del vostro file kickstart, potete utilizzare l'applicazione **Kickstart Configurator**. Per maggiori dettagli, consultate il Capitolo 8.

Nota Bene

Se l'opzione è seguita dal carattere di uguale (=), dopo di esso occorre specificare un valore. Nei comandi di esempio, le opzioni in parentesi ([]) sono argomenti facoltativi per il comando.

`autostep` (opzionale)

Simile a `interactive`, con la differenza che questo comando passa automaticamente alla schermata successiva. Viene utilizzato soprattutto per le operazioni di debugging.

`auth` o `authconfig` (obbligatorio)

Configura le opzioni di autenticazione per il sistema. È simile al comando `authconfig`, che può essere eseguito dopo l'installazione. Per default, le password sono cifrate, e non viene attivata la modalità shadow.

`--enablemd5`

Utilizza la cifratura md5 per le password utente.

`--enablenis`

Attiva il supporto NIS. Per default `--enablenis` usa qualsiasi dominio accessibile dalla rete. Un dominio va sempre impostato manualmente tramite l'opzione `--nisdomain=`.

`--nisdomain=`

Il nome del domino NIS da utilizzare per i servizi NIS.

`--nisserver=`

Server da utilizzare per i servizi NIS (default).

`--useshadow` o `--enableshadow`

Usa password shadow.

`--enableldap`

Attiva il supporto LDAP nel file `/etc/nsswitch.conf`. Il sistema cerca le informazioni degli utenti (UID, directory home, shell, ecc.) da una directory LDAP. Per usare questa opzione dovete aver installato il pacchetto `nss_ldap` e occorre inoltre che specifichiate un sever e un DN di base con `--ldapserver=` e `--ldapbasedn=`.

`--enableldapauth`

Attiva il metodo di autenticazione LDAP. Il modulo `pam_ldap` viene utilizzato per l'autenticazione e per il cambio delle password nella directory LDAP. È necessario aver installato il pacchetto `nss_ldap`. Dovete inoltre specificare un server e un DN di base con `--ldapserver=` e `--ldapbasedn=`.

`--ldapserver=`

Se avete indicato `--enableldap` oppure `--enableldapauth`, specifica il nome del server LDAP da utilizzare. L'opzione viene impostata nel file `/etc/ldap.conf`.

`--ldapbasedn=`

Specifica il DN (distinguished name) nell'albero della directory LDAP in cui sono archiviate le informazioni dell'utente, se avete indicato `--enableldap` o `--enableldapauth`. Questa opzione viene impostata nel file `/etc/ldap.conf`.

`--enableldaptls`

Utilizza le ricerche TLS (Transport Layer Security). Questa opzione consente a LDAP di inviare nomi utente e password cifrati a un server LDAP prima dell'autenticazione.

`--enablekrb5`

Usa Kerberos 5 per autenticare gli utenti. Il sistema Kerberos non conosce le directory home, gli UID o le shell, perciò se abilitate l'opzione Kerberos, dovete rendere noti a questa postazione di lavoro gli account degli utenti, abilitando LDAP, NIS o Hesiod o usando il comando `/usr/sbin/useradd` affinché la workstation li riconosca. Per poter usare questa opzione dovete aver installato il pacchetto `pam_krb5`.

`--krb5realm=`

Il realm di Kerberos 5 a cui appartiene la workstation.

`--krb5kdc=`

KDC che risponde alle richieste dei client kerberos. Se avete più KDC, separate i loro nomi con una virgola (,).

`--krb5adminserver=`

Il KDC nel realm che sta eseguendo kadmind. Questo server gestisce la modifica delle password e le altre richieste di amministrazione. Se avete più di un KDC, questo server va eseguito sul KDC master.

`--enablehesiod`

Attiva il supporto Hesiod per la ricerca della directory home, dell'UID e della shell degli utenti. Per maggiori informazioni sul servizio e le sue impostazioni, consultate il file `/usr/share/doc/glibc-2.x.x/README.hesiod`, incluso nel pacchetto `glibc`. Hesiod è un'estensione del DNS e usa i record del DNS per la memorizzazione delle informazioni sugli utenti, sui gruppi di utenti e altro ancora.

`--hesiodlhs`

L'opzione Hesiod LHS ("left-hand side") viene impostata nel file `/etc/hesiod.conf`. È utilizzata dalla libreria Hesiod per determinare il nome del DNS per la ricerca delle informazioni, in modo analogo all'uso di un DN da parte di LDAP.

`--hesiodrhs`

L'opzione Hesiod RHS ("right-hand side") viene impostata nel file `/etc/hesiod.conf`. Questa opzione è usata dalla libreria Hesiod per determinare il nome del DNS per la ricerca delle informazioni, in modo analogo all'uso di un DN da parte di LDAP.

Suggerimento

Per la ricerca delle informazioni sull'utente "jim", la libreria Hesiod cerca *jim.passwd<LHS><RHS>*, che dovrebbe corrispondere a un record TXT simile, nell'aspetto a (`jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`). Per quanto riguarda i gruppi, la situazione è identica e viene usato: *jim.group<LHS><RHS>*.

La ricerca degli utenti e dei gruppi in base al numero avviene creando un file "501.uid", come CNAME per "jim.passwd" e un file "501.gid" come CNAME per "jim.group". Ricordatevi che davanti a LHS e RHS non viene posto il carattere [.] quando la libreria determina il nome da cercare. LHS e RHS iniziano solitamente con un punto.

`--enablesmbauth`

Abilita l'autenticazione di utenti sulla base di un server SMB (di norma un server Samba o Windows). Il supporto per l'autenticazione con SMB non conosce la directory home, l'UID o la shell degli utenti, dunque per poter usare questa opzione dovete rendere noti gli account utente alla workstation abilitando LDAP, NIS o Hesiod o utilizzando il comando `/usr/sbin/useradd`. Per usare questa opzione dovete aver installato il pacchetto `pam_smb`.

`--smbservers=`

Indica il nome del (o dei) server da usare per l'autenticazione di tipo SMB. Quando specificate più di un server, separate ogni nome con una virgola (,).

`--smbworkgroup=`

Indica il nome del workgroup per i server SMB.

`--enablecache`

Abilita il servizio `nscd`, che memorizza le informazioni di cache sugli utenti e sui gruppi e informazioni di altro genere. Questo si rivela particolarmente utile se distribuite informazioni relative a utenti e gruppi nella rete usando NIS, LDAP o Hesiod.

`bootloader` (obbligatorio)

Specifica quale boot loader installare (LILO o GRUB) e il modo in cui installarlo. Questa opzione È obbligatoria sia per le installazioni sia per gli aggiornamenti. Per gli aggiornamenti, se `--useLilo` non è specificato e LILO è il boot loader attualmente in funzione, esso verrà sostituito da GRUB. Per conservare LILO durante gli aggiornamenti, utilizzate il comando `bootloader--upgrade`.

`--append=`

Specifica i parametri del Kernel. Per specificare parametri multipli, separateli con gli spazi. Per esempio:

```
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
```

`--location=`

Indica dove viene memorizzato il record di avvio. Dei valori validi possono essere: **`mbr`** (default), **`partition`** (installa il boot loader sul primo settore della partizione che contiene il kernel) o **`none`** (che non installa il boot loader).

`--password=`

Se state utilizzando GRUB, questo comando imposta la password del boot loader GRUB su quella specificata con questa opzione. È consigliabile utilizzarlo per limitare l'accesso alla shell di GRUB, dove è possibile trasmettere opzioni arbitrarie del kernel.

`--md5pass=`

Se state usando GRUB, il comando è simile a `--password=`, solo che la password dovrebbe essere già criptata.

`--useLilo`

Usa LILO invece di GRUB come boot loader.

`--linear`

Se state utilizzando LILO, potete usare l'opzione `linear`, che serve solo per la compatibilità con le opzioni precedenti ed è ormai utilizzata come default.

`--nolinear`

Se state utilizzando LILO, potete usare l'opzione `nolinear`; l'opzione di default è linear.

`--lba32`

Se usate LILO, potete imporre l'utilizzo della modalità lba32 invece dell'autorilevamento.

`--upgrade`

Aggiorna la configurazione del boot loader esistente, conservando le vecchie entry. Quest'opzione è disponibile solo per gli aggiornamenti.

`clearpart` (facoltativo)

Rimuove le partizioni dal sistema prima di crearne di nuove. Per default, non viene rimossa alcuna partizione.

Nota Bene

Se utilizzate il comando `clearpart`, allora non potete usare il comando `--onpart` su una partizione logica.

`--linux`

Cancella tutte le partizioni Linux.

`--all`

Cancella tutte le partizioni dal sistema.

`--drives=`

Specifica da quali unità vanno cancellate dalle partizioni. Per esempio, il seguente cancella le partizioni sui primi due dispositivi sul controller IDE primario:

```
clearpart --drives hda,hdb
```

`--initlabel`

Inizializza l'etichetta del disco secondo il default stabilito per la vostra architettura (`msdos` per x86 e `gpt` per Itanium). È utile per evitare che il programma di installazione chieda se deve inizializzare l'etichetta del disco in caso di installazione su un nuovo disco fisso.

`device` (opzionale)

Sulla maggior parte dei sistemi PCI il programma d'installazione effettua correttamente l'autorilevamento per le schede Ethernet e SCSI. Sui sistemi meno recenti e su alcuni sistemi PCI, è necessario specificare il tipo di periferica. Il comando device, che indica al programma di installazione di installare moduli aggiuntivi, ha il seguente formato:

```
device <type> <moduleName> --opts=<options>
```

<tipo>

Sostituire con **`scsi`** o **`eth`**.

<NomeModulo>

Sostituire con il nome del modulo del kernel da installare.

`--opts`

Opzioni da passare al modulo del kernel. È possibile trasmettere opzioni multiple solo tra virgolette. Per esempio:

```
--opts="aic152x=0x340 io=11"
```

`deviceprobe` (facoltativo)

Impone il rilevamento del bus del PCI e carica moduli per tutti i dispositivi trovati, laddove sia disponibile un modulo.

`driverdisk` (facoltativo)

I dischetti dei driver possono essere utilizzati durante le installazioni kickstart. Dovete copiarne il contenuto nella directory di root di una partizione sul disco fisso del sistema. Utilizzate poi il comando `driverdisk` per indicare al programma di installazione dove cercare il dischetto dei driver.

`driverdisk <partition> [--type=<fstype>]`

<partizione>

Partizione che contiene il dischetto dei driver.

`--type=`

Tipo di File system (per esempio, vfat o ext2).

`firewall` (facoltativo)

Questa configurazione corrisponde alla schermata **Configurazione del firewall** nel programma d'installazione:

`firewall <securitylevel> [--trust=] <incoming> [--port=]`

<livellosicurezza>

Sostituire con uno dei livelli di sicurezza seguenti:

- `--high`
- `--medium`
- `--disabled`

`--trust=`

Indicando un dispositivo, come eth0, consentite a tutto il traffico in entrata da quel dispositivo di attraversare il firewall. Per indicare più di un dispositivo, usate `--trust eth0 --trust eth1`. NON usate un formato separato da virgola, come `--trust eth0, eth1`.

<inentrata>

Sostituite con nessuna delle seguenti alternative (o con più di una) per autorizzare i servizi specificati ad attraversare il firewall.

- `--dhcp`
- `--ssh`
- `--telnet`
- `--smtp`
- `--http`
- `--ftp`

`--port`

Potete specificare che le porte siano autorizzate ad attraversare il firewall utilizzando il formato porta:protocollo. Per esempio, se desiderate consentire che l'accesso IMAP attraversi il firewall, digitate `imap:tcp`. Potete inoltre indicare il numero di porte in modo esplicito. Per esempio, per autorizzare all'attraversamento i pacchetti UDP sulla porta 1234, specificate `1234:udp`. Se volete indicare più di una porta, separatele con delle virgole.

`install` (facoltativo)

Indica al sistema di installare un nuovo sistema al posto di aggiornarne uno esistente. Si tratta della modalità di default. Dovete specificare il tipo di installazione: `cdrom`, `harddrive`, `nfs` o `url` (per installazioni via ftp o http). Il comando `install` e il comando del metodo d'installazione devono essere righe separate.

`cdrom`

Installa dalla prima unità CD-ROM sul sistema.

`harddrive`

Installa da un albero di installazione Red Hat su un'unità locale (vfat o ext2).

- `--partition=`

  Partizione da cui installare (per esempio, sbd2).

- `--dir=`

  Directory contenente l'albero d'installazione di `RedHat`.

Per esempio:

```
harddrive --partition=hdb2 --dir=/tmp/install-tree
```

`nfs`

Installa dal server NFS specificato.

- `--server=`

  Server dal quale installare (hostname o IP).

- `--dir=`

  Directory contenente l'albero d'installazione di `RedHat`.

Per esempio:

```
nfs --server=nfsserver.example.com --dir=/tmp/install-tree
```

`url`

Installa da un albero di installazione Red Hat su un server remoto via FTP o HTTP.

Per esempio:

```
url --url http://<server>/<dir>
```

oppure:

```
url --url ftp://<username>:<password>@<server>/<dir>
```

`interactive` (facoltativo)

Utilizza le informazioni fornite nel file kickstart durante l'installazione, autorizzando nel contempo il controllo e la modifica dei valori dati. Vi viene mostrata ogni schermata del programma di installazione con i valori presi dal file kickstart. Potete accettare i valori facendo clic sul pulsante **Avanti** oppure potete cambiarli e poi fare clic su **Avanti** per continuare. Vedere anche `autostep`.

`keyboard` (obbligatorio)

Imposta il tipo di tastiera del sistema. Ecco un elenco delle tastiere disponibili sulle macchine i386, Itanium e Alpha:

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-nodeadkeys, dk, dk-latin1, dvorak, es, et,
fi, fi-latin1, fr, fr-latin0, fr-latin1, fr-pc, fr_CH, fr_CH-latin1,
gr, hu, hu101, is-latin1, it, it-ibm, it2, jp106, la-latin1, mk-utf,
no, no-latin1, pl, pt-latin1, ro_win, ru, ru-cp1251, ru-ms, ru1, ru2,
ru_win, se-latin1, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querty, slovene, trq, ua,
uk, us, us-acentos
```

Il file `/usr/lib/python2.2/site-packages/rhpl/keyboard_models.py` contiene questa lista ed é parte del pacchetto `rhpl`.

`lang` (obbligatorio)

Imposta la lingua da usare durante l'installazione. Per esempio, per impostare la lingua italiana, il file kickstart deve contenere le linee seguenti:

```
lang en_US
```

Il file `/usr/share/redhat-config-language/locale-list` fornisce un elenco dei codici della lingu valida nella prima colonna di ogni riga ed é parte del pacchetto `redhat-config-languages`.

`langsupport` (obbligatorio)

Imposta la lingua o le lingue da installare nel sistema. Con `langsupport` si possono usare gli stessi codici lingua usati con `lang`.

Se desiderate installare una sola lingua, occorre specificarlo. Per esempio, per installare e utilizzare il francese `fr_FR`:

```
langsupport fr_FR
```

`--default`

Se desiderate installare il supporto lingua per più di una lingua, dovrete indicare il valore di default.

Per installare l'inglese e il francese e usare, per esempio, l'inglese come lingua predefinita dovete procedere così:

```
langsupport --default=en_US fr_FR
```

Se utilizzate `--default` con un'unica lingua, tutte le altre lingue saranno installate con riferimento alla lingua specificatamente impostata come predefinita.

`lilo` (sostituito da `bootloader`)

Avvertenza

Questa opzione è stata sostituita da `bootloader` ed è disponibile solo per consentire la compatibilità con le versioni precedenti. Si veda `bootloader`.

Specifica come installare il boot loader sul sistema. Per default, LILO esegue l'installazione sull'MBR del primo disco e installa un sistema dual-boot se viene trovata una partizione DOS. Il sistema DOS/Windows si avvia se l'utente digita **dos** al prompt di `LILO:`.

`--append <parametri>`

Specifica i parametri del kernel.

`--linear`

Usa l'opzione di LILO `linear` solo per la compatibilità con le versioni precedenti (questa opzione è quella usata di default).

`--nolinear`

Usa l'opzione di LILO `nolinear`. L'opzione usata di default è ora `linear`.

`--location=`

Specifica dove viene scritto il record di avvio di LILO. I valori validi sono `mbr` (default) o `partition` (installa il loader di avvio sul primo settore della partizione contenente il kernel). Se non è specificata alcuna posizione, LILO non viene installato.

`--lba32`

Impone l'utilizzo della modalità lba32 al posto dell'autorilevamento.

`lilocheck` (opzionale)

Se l'opzione `lilocheck` è presente, il programma di installazione controlla se LILO è già presente nell'MBR del primo disco fisso e se lo rileva, riavvia il sistema. In questo caso non viene compiuta alcuna installazione. Ciò impedisce a kickstart di reinstallare un sistema già installato.

`logvol` (optional)

Crea un volume logico per la gestione LVM (Logical Volume Managment) con la sintassi:

```
logvol mountpoint --vgname=name --size=size --name=name
```

Crea innanzi tutto la partizione, quindi il gruppo di volume logico e infine il volume logico stesso. Per esempio:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`mouse` (obbligatorio)

Configura il mouse per il sistema, sia in modalità testo sia in modalità grafica. Le opzioni sono:

`--device=`

Specifica il dispositivo su cui si trova il mouse (per es. `--device ttyS0`).

`--emulthree`

Se questa opzione viene impostata, il sistema grafico X Window usa simultaneamente il tasto sinistro e quello destro del mouse per emulare il tasto centrale (se ne consiglia l'uso nel caso di mouse a due tasti).

Dopo l'opzione, va indicato il tipo di mouse, scegliendone uno tra i seguenti:

```
alpsps/2, ascii, asciips/2, atibm, generic, generic3, genericps/2,
generic3ps/2, genericwheelps/2, genericusb, generic3usb, genericwheelusb,
```

```
geniusnm, geniusnmps/2, geniusprops/2, geniusscrollps/2, geniusscrollps/2+,
thinking, thinkingps/2, logitech, logitechcc, logibm, logimman,
logimmanps/2, logimman+, logimman+ps/2, logimmusb, microsoft, msnew,
msintelli, msintellips/2, msintelliusb, msbm, mousesystems, mmseries,
mmhittab, sun, none
```

Questa lista puó essere trovata nel file `/usr/lib/python2.2/site-packages/rhpl/mouse.py`, che é parte del pacchetto `rhpl`.

Se il comando del mouse viene indicato senza argomenti, o viene omesso, il programma d'installazione cerca di rilevare automaticamente il tipo di mouse collegato al computer. Questa procedura funziona per la maggior parte dei mouse moderni.

`network` (opzionale)

Configura le informazioni di rete per il sistema. Se l'installazione kickstart non richiede il networking (in altre parole non è installata via NFS, HTTP o FTP), il networking non viene configurato per il sistema. Se l'installazione richiede il networking e le informazioni non vengono fornite nel file kickstart, il programma d'installazione di Red Hat Linux suppone che l'installazione debba avvenire tramite eth0 via indirizzo IP dinamico (BOOT/DHCP) e configura il sistema finale, installato per determinare in modo dinamico l'indirizzo IP. L'opzione `network` configura le informazioni di networking per le installazioni kickstart via rete e per il sistema installato.

`--bootproto`

`dhcp`, `bootp` o `static`.

Il default è `dhcp`. Le impostazioi `dhcp` e `bootp` vengono trattate nello stesso modo.

Il metodo DHCP si serve di un server DHCP per ottenere la propria configurazione di rete. Com'è intuibile, il metodo BOOTP si serve di un server BOOTP. Per indicare al sistema di utilizzare DHCP:

```
network --bootproto=dhcp
```

Invece, per indicare alla macchina di utilizzare BOOTP per ottenere i parametri di configurazione per la propria rete, inserite la linea che segue nel file kickstart:

```
network --bootproto=bootp
```

Il metodo statico richiede che tutte le informazioni relative alla rete siano inserite nel file kickstart. Come suggerisce il nome stesso, queste informazioni sono statiche e saranno utilizzate durante l'installazione, nonché in seguito. La linea per il networking statico è più complessa, poiché deve contenere tutte le informazioni relative alla configurazione di rete. Dovete specificare l'indirizzo IP, la maschera di rete, il gateway e il server dei nomi. Ecco un esempio (il backslash \ indica che tutto si trova sulla stessa linea):

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 \
--gateway=10.0.2.254 --nameserver=10.0.2.1
```

Se utilizzate il metodo statico, dovete tenere presente le due restrizioni qui sotto indicate:

- Tutte le informazioni statiche sulla configurazione del networking devono essere specificate su *un'unica* riga. Non è possibile, per esempio, andare a capo usando un backslash ("\").
- Potete specificare solo un server di nomi. Comunque, potete utilizzare la sezione `%post` del file kickstart (vedere la Sezione 7.7) per aggiungere, se necessario, altri server di nomi.

`--device=`

Utilizzato per selezionare un dispositivo Ethernet specifico da installare. Il comando `--device=` non è efficace a meno che il file kickstart non sia un file locale (come per esempio

ks=floppy), poichè il programma di installazione configurerà la rete in modo da trovare il file kickstart. Per esempio:

```
network --bootproto=dhcp --device=eth0
```

--ip=

Indirizzo IP per la macchina da installare.

--gateway=

Gateway di default come indirizzo IP.

--nameserver=

Server di nomi primario, come indirizzo IP.

--nodns

Non configura alcun server DNS

--netmask

Maschera di rete per il sistema installato

--hostname

Nome dell'host per il sistema installato

part o partition (necessario per le installazioni, ignorato per gli aggiornamenti)

Crea una partizione sul sistema.

Se è presente più di un'installazione Red Hat Linux nel sistema in partizioni diverse, il programma di installazione vi richiede quale installazione aggiornare.

Avvertenza

Tutte le partizioni create saranno formattate nel corso del processo di installazione, a meno che non siano in uso --noformat e --onpart.

<mntpoint>

La sezione *<mntpoint>* indica il punto in cui la partizione viene montata e deve avere una delle seguenti forme:

- */<percorso>*

  Per esempio: /, /usr, /home

- swap

  La partizione viene usata come spazio di swap.

  Per determinare la dimensione della partizione swap automaticamente, utilizzate l'opzione --recommended:

  ```
  swap --recommended
  ```

  La partizione swap generata in modo automatico avrà una dimensione minima non inferiore alla quantità di RAM del sistema e non superiore al doppio della stessa.

- raid.*<id>*

  La partizione viene usata per il RAID software (si veda raid).

- pv.*<id>*

La partizione verrà utilizzata per l'LVM si veda `logvol`).

`--size=`

La dimensione minima della partizione, misurata in megabyte. Indicate un valore intero, come per esempio 500. Non aggiungete MB dopo il numero.

`--grow`

Indica alla partizione di "allargarsi" e di occupare tutto lo spazio disponibile oppure di raggiungere la dimensione massima impostata.

`--maxsize=`

Imposta la dimensione massima della partizione nel caso sia stata selezionata l'opzione grow. Specificate un valore intero e non aggiungete MB dopo il numero.

`--noformat`

Indica al programma di installazione di non formattare la partizione, da usare con il comando `--onpart`.

`--onpart=` or `--usepart=`

Posiziona la partizione sul dispositivo *già esistente*. Per esempio:

```
partition /home --onpart=hda1
```

inserisce `/home` su `/dev/hda1`, che deve già essere presente.

`--ondisk=` o `--ondrive=`

Impone che la partizione sia creata sul disco specificato. Per esempio, `--ondisk=sdb` crea la partizione sul secondo disco presente sul sistema.

`--asprimary`

Impone l'allocazione automatica della partizione come partizione primaria, se così non può essere, la partizione non viene creata.

`--bytes-per-inode=`

Il numero specificato rappresenta il numero di byte per inode sul filesystem quando viene creato. Va indicato in numeri decimali. Questa opzione è utile per le applicazioni in cui desiderate aumentare il numero di inode sul filesystem.

`--type=` (sostituita da `fstype`)

Questa opzione non è più disponibile. Utilizzate `fstype`.

`--fstype=`

Imposta il tipo di filesystem per la partizione. Dei valori validi sono **`ext2`**, **`ext3`**, **`swap`** e **`vfat`**.

`--start=`

Specifica il cilindro di partenza per la partizione. Richiede che venga specificata un'unità con `--ondisk=` oppure `ondrive=`. Richiede inoltre che il cilindro finale venga specificato con `--end=` o che la dimensione della partizione venga specificata con `--size=`.

`--end=`

Specifica il cilindro finale per la partizione. È necessario che il cilindro di partenza venga specificato con `--start=`.

`--badblocks`

Stabilisce che la partizione venga controllata per rilevare eventuali settori difettosi.

Nota Bene

Se dovesse fallire la fase di partizionamento del disco, compare il messaggio di diagnostica sulla console virtuale 3.

`raid` (opzionale)

Assembla un dispositivo RAID software. Questo comando ha la forma seguente:

```
raid <mntpoint> --level=<level> --device=<mddevice> <partitions*>
```

<mntpoint>

Indica la posizione in cui è montato il filesystem RAID. Se si tratta di `/`, il livello RAID deve essere 1, a meno che non sia presente una partizione boot (`/boot`). Se tale partizione esiste ed è di livello 1, la partizione root (`/`) può essere di qualsiasi tipo. La sezione *<partizioni*>* (che indica la possibilità di elencare partizioni multiple), elenca gli identificatori RAID da aggiungere all'array RAID.

`--level=`

Livello RAID da usare (0, 1, o 5).

`--device=`

Nome del dispositivo RAID da utilizzare (come per esempio md0 o md1). I dispositivi RAID variano da md0 a md7 e ognuno di essi può essere usato una volta sola.

`--spares=`

Indica il numero di unità spare allocate per l'array RAID. Le unità spare (di riserva) vengono utilizzate per ricostruire l'array in caso di problemi.

`--fstype=`

Imposta il tipo di filesystem per l'array RAID. Dei valori validi sono ext2, ext3, swap e vfat.

`--noformat`

Non formatta l'array RAID.

L'esempio riportato di seguito spiega come creare la partizione RAID di livello 1 per `/` e un RAID di livello 5 per `/usr`, presumendo che esistano tre dischi SCSI sul sistema. Crea inoltre tre partizioni swap, una su ogni unità.

```
part raid.01 --size=60 --ondisk=sda
part raid.02 --size=60 --ondisk=sdb
part raid.03 --size=60 --ondisk=sdc
part swap --size=128 --ondisk=sda
part swap --size=128 --ondisk=sdb
part swap --size=128 --ondisk=sdc
part raid.11 --size=1 --grow --ondisk=sda
```

```
part raid.12 --size=1 --grow --ondisk=sdb
part raid.13 --size=1 --grow --ondisk=sdc
raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

`reboot` (opzionale)

Riavvia al termine dell'installazione (nessun argomento presente). Di solito, kickstart visualizza un messaggio e aspetta che l'utente prema un tasto, prima di effettuare il riavvio.

`rootpw` (obbligatorio)

Imposta la password di root del sistema su <*password*>.

`rootpw [--iscrypted] <password>`

`--iscrypted`

Se questa opzione è presente, la password viene considerata già cifrata.

`skipx` (facoltativo)

Se questa opzione è presente, X non viene configurato sul sistema installato.

`text` (opzionale)

Esegue l'installazione kickstart in modalità testo. Per default, le installazioni kickstart vengono eseguite in modalità grafica.

`timezone` (obbligatorio)

Imposta il fuso orario del sistema su <*fusoorario*> che può essere scelto tra i fusi elencati in `timeconfig`.

`timezone [--utc] <timezone>`

`--utc`

Se presente, il sistema presuppone che nell'orologio hardware sia impostata l'ora UTC (meridiano di Greenwich).

`upgrade` (opzionale)

Indica al sistema di aggiornare un sistema esistente invece di installarne uno nuovo. Dovete specificare la posizione dell'albero di installazione, scegliendo tra cdrom, disco fisso, nfs o url (per ftp e http). Per i dettagli si veda `install`.

`xconfig` (opzionale)

Configura il sistema X Window. Se questa opzione non è specificata, l'utente dovrà configurare manualmente X durante l'installazione, se X era già installato. Questa opzione non dovrebbe essere utilizzata se X non viene installato sul sistema finale.

`--noprobe`

Non rileva il monitor.

`--card=`

Usa la scheda specificata. Il nome della scheda grafica deve essere presente nell'elenco contenuto in `/usr/share/hwdata/Cards` dal pacchetto `hwdata`. L'elenco delle schede puó anche essere trovato sulla schermata **X Configuration** del **Configurazione Kickstart**. Se questa opzione non è specificata, allora il programma di installazione rileva il bus PCI per la scheda. Poiché AGP fa parte del bus PCI, le schede AGP vengono rilevate se è presente il supporto. L'ordine di rilevamento viene determinato in base all'ordine di scansione PCI della scheda madre.

`--videoram=`

Specifica la quantità di RAM video contenuta nella scheda video.

`--monitor=`

Usa il monitor specificato. Il monitor deve essere presente nell'elenco dei monitor in `/usr/share/hwdata/MonitorsDB` dal pacchetto `hwdata`. L'elenco delle schede puó anche essere trovato sulla schermata **X Configuration** del **Configurazione Kickstart**. Questa opzione viene ignorata se sono forniti `--hsync` o `--vsync`. Se non vengono indicate informazioni sul monitor, il programma di installazione cerca di rilevarlo automaticamente.

`--hsync=`

Indica la frequenza orizzontale del monitor.

`--vsync=`

Specifica la frequenza verticale del monitor.

`--defaultdesktop=`

Imposta il desktop di default GNOME o KDE (e presuppone che GNOME e/o KDE siano stati installati tramite il comando `%packages`).

`--startxonboot`

Usa un login grafico sul sistema installato.

`--resolution=`

Indica la risoluzione di default per il sistema X Window sul sistema installato. Dei valori validi sono 640x480, 800x600, 1024x768, 1152x864, 1280x1024, 1400x1050 e 1600x1200. Assicuratevi di specificare una risoluzione compatibile con la scheda video e il monitor.

`--depth=`

Indica la profondità di colore di default per il sistema X Window sul sistema installato. Dei valori validi sono 8, 16, 24 e 32. Assicuratevi di specificare una profondità di colore compatibile con la scheda video e il monitor.

`volgroup` (optional)

Crea un gruppo LVM (Logical Volume Management) con la sintassi:

```
volgroup name partition
```

Crea innanzi tutto la partizione, quindi il gruppo di volume logico e infine il volume logico stesso. Per esempio:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`zerombr` (opzionale)

Se viene specificato `zerombr` e l'unico argomento indicato è `yes`, qualsiasi tabella delle partizioni non valida trovata sui dischi viene inizializzata. Attivando questa opzione, viene rimosso il contenuto dei dischi con le tabelle delle partizioni non valide. Questo comando dovrebbe avere la forma seguente:

```
zerombr yes
```

Nessun'altra forma risulta valida.

`%include`

Utilizzate il comando `%include` *`/path/to/file`* per inserire nel file kickstart il contenuto di un altro file, come se tale contenuto si trovasse nella posizione del comando `%include` all'interno del file kickstart.

7.5. Selezione dei pacchetti

Tramite il comando `%packages` è possibile creare una sezione nel file kickstart dove specificare quali pacchetti installare durante (questa opzione è valida solo per l'installazione e non per l'aggiornamento).

I pacchetti possono essere specificati tramite il nome del componente o del singolo pacchetto. Il programma di installazione definisce vari componenti che raggruppano i pacchetti. Consultate il file `RedHat/base/comps.xml` presente su qualsiasi CD Red Hat Linux se desiderate un elenco dei gruppi. Ogni gruppo possiede un numero identificativo, un valore visualizzabile dall'utente, il nome, la descrizione e un elenco dei pacchetti. In tale elenco, i pacchetti segnalati come obbligatori sono sempre installati se il pacchetto è stato selezionato; quelli segnalati come predefiniti sono installati per default se il pacchetto ` stato selezionato; infine, quelli segnalati come facoltativi devono essere appositamente selezionati per poter essere installati, anche se il gruppo risulta selezionato.

Nella maggior parte dei casi, è sufficiente creare un elenco dei gruppi desiderati e non dei singoli pacchetti. I gruppi `Core` e `Base` sono sempre selezionati per default, dunque non è necessario specificarli nella sezione `%packages`.

Ecco un esempio di una selezione `%packages`:

```
%packages
@ X Window System
@ GNOME Desktop Environment
@ Graphical Internet
@ Sound and Video
galeon
```

Come potete vedere, i gruppi sono indicati uno per linea con un simbolo `@`, uno spazio e poi l'intero nome del gruppo come specificato nel file `comps.xml`. Specificate i pacchetti singoli senza aggiungere altri caratteri (la linea `galeon` nell'esempio riportato sopra indica un pacchetto singolo).

Potete inoltre specificare quali pacchetti non installare tra quelli elencati di default:

```
@ Games and Entertainment
-kdegames
```

Sono disponibili due opzioni per l'opzione `%packages`.

`--resolvedeps`

Installate i pacchetti riportati in elenco e risolvete in modo automatico le dispendenze. SE questa opzione non é specificata, e sono presenti le dipendenze del pacchetto, l'installazione automatizzata si interromperá richiamando l'utente. Per esempio:

```
%packages --resolvedeps
```

`--ignoredeps`

Ignorate le dipendenze non risolte e installate i pacchetti elencati senza le dipendenze. Per esempio:

```
%packages --ignoredeps
```

`--ignoremissing`[1]

Ignorate i pacchetti e i gruppi mancanti invece di fermare l'installazione se il sistema vi richiede di abbandonare o continuare l'installazione stessa.Per esempio:

```
%packages --ignoremissing
```

7.6. Script di pre-installazione

In questa sezione si possono aggiungere i comandi da eseguire immediatamente dopo il caricamento del file `ks.cfg`. Questa sezione va inserita alla fine del file kickstart (dopo i comandi) e deve iniziare con il comando `%pre`. Potete accedere alla rete all'interno della sezione `%pre`. Comunque, il *servizio dei nomi* non è ancora stato configurato, pertanto è necessario utilizzare gli indirizzi IP numerici.

Nota Bene

Lo script di pre-installazione non viene eseguito nell'ambiente di cambiamento di root.

`--interpreter /usr/bin/python`

Vi consente di specificare un linguaggio di scripting diverso, quale Python. Sostituite `/usr/bin/python` con il linguaggio di scripting da voi scelto.

7.6.1. Esempio

Ecco un esempio di una sezione `%pre`:

```
%pre

#!/bin/sh

hds=""
mymedia=""

for file in /proc/ide/h*
do
  mymedia=`cat $file/media`
  if [ $mymedia == "disk" ] ; then
      hds="$hds `basename $file`"
  fi
done

set $hds
numhd=`echo $#`

drive1=`echo $hds | cut -d' ' -f1`
```

1. Questa opzione é nuova per Red Hat Linux 9.

```
drive2=`echo $hds | cut -d' ' -f2`

#Write out partition scheme based on whether there are 1 or 2 hard drives

if [ $numhd == "2" ] ; then
  #2 drives
  echo "#partitioning scheme generated in %pre for 2 drives" > /tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
  echo "part /boot --fstype ext3 --size 75 --ondisk hda" >> /tmp/part-include
  echo "part / --fstype ext3 --size 1 --grow --ondisk hda" >> /tmp/part-include
  echo "part swap --recommended --ondisk $drive1" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 1 --grow --ondisk hdb" >> /tmp/part-include
else
  #1 drive
  echo "#partitioning scheme generated in %pre for 1 drive" > /tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
  echo "part /boot --fstype ext3 --size 75" >> /tmp/part-includ
  echo "part swap --recommended" >> /tmp/part-include
  echo "part / --fstype ext3 --size 2048" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 2048 --grow" >> /tmp/part-include
fi
```

Questo script determina il numero di dischi fissi presenti nel sistema e scrive un file di testo con un schema di partizionamento diverso a seconda che ne abbia uno o due. Invece di tenere un set di comandi di partizionamento nel file kickstart, inserite la linea:

```
%include /tmp/part-include
```

Verranno utilizzati i comandi di partizionamento selezionati nello script.

7.7. Script di post-installazione

Avete la possibilità di aggiungere dei comandi da eseguire sul sistema una volta completata l'installazione. Questa sezione deve trovarsi alla fine del file kickstart e deve iniziare con il comando `%post`. La presente sezione è utile per funzioni quali i'installazione di software aggiuntivo e la configurazione di un ulteriore server di nomi.

Nota Bene

Se avete configurato la rete con IP statico, compreso un server di nomi, potete accedere alla rete e risolvere indirizzi IP nella sezione `%post`. Se avete configurato la rete con metodo DHCP, il file `/etc/resolv.conf` non è stato completato quando l'installazione esegue la sezione `%post`. Potete accedere alla rete, ma non potete risolvere indirizzi IP. Pertanto, se state utilizzando DHCP, dovete specificare gli indirizzi IP nella sezione `%post`.

Nota Bene

Lo script di post-installazione viene eseguito in un ambiente chroot, pertanto non sarà possibile eseguire attività quali la copia di script o file RPM dall'unità utilizzata per l'installazione.

`--nochroot`

Vi permette di specificare i comandi che volete eseguire al di fuori dell'ambiente "chroot".

Il seguente esempio copia il file `/etc/resolv.conf` nel filesystem appena installato.

```
%post --nochroot
cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
```

`--interpreter /usr/bin/python`

Vi consente di specificare un linguaggio di scripting diverso, quale Python. Sostituite `/usr/bin/python` con il linguaggio di scripting da voi scelto.

7.7.1. Esempi

Attivare e disattivare servizi:

```
/sbin/chkconfig --level 345 telnet off
/sbin/chkconfig --level 345 finger off
/sbin/chkconfig --level 345 lpd off
/sbin/chkconfig --level 345 httpd on
```

Eseguire uno chiamato `runme` da una condivisione NFS:

```
mkdir /mnt/temp
mount 10.10.0.2:/usr/new-machines /mnt/temp
open -s -w -- /mnt/temp/runme
umount /mnt/temp
```

Aggiungere un utente al sistema:

```
/usr/sbin/useradd bob
/usr/bin/chfn -f "Bob Smith" bob
/usr/sbin/usermod -p 'kjdf$04930FTH/ ' bob
```

7.8. Rendere disponibile un file kickstart

Un file kickstart va collocato in una delle posizioni seguenti:

- Su un dischetto di avvio
- On a boot CD-ROM
- Su una rete

Normalmente il file di configurazione kickstart viene copiato sul dischetto di avvio o reso disponibile via rete. Il secondo metodo è quello più utilizzato, poiché la maggior parte delle installazioni kickstart viene usata su computer in rete.

Osserviamo nel dettaglio le posizioni in cui si può collocare il file.

7.8.1. Creazione di un dischetto d'avvio kickstart

Per effettuare l'installazione kickstart tramite dischetto, è necessario creare un file `ks.cfg` e collocarlo nella directory superiore del dischetto d'avvio. Fate riferimento alla sezione *Come creare un dischetto di avvio per installazione* nel *Red Hat Linux Installation Guide* per istruzioni sulla creazione del dischetto di avvio. Poiché i dischetti di avvio Red Hat Linux sono in formato MS-DOS, per copiare il file kickstart in Linux basta digitare il comando `mcopy`:

```
mcopy ks.cfg a:
```

Altrimenti per copiare il file potete utilizzare Windows. Potete inoltre montare il dischetto di avvio MS-DOS e copiare il file con il comando `cp`.

7.8.2. Creazione di un CD-ROM di avvio di Kickstart

Per effettuare una installazione kickstart basata su CD-ROM, il file kikcstart deve essere nominato `ks.cfg` e deve essere posizionato nella directory superiore del CD-ROM di avvio. Dato che un CD-ROM é di sola lettura, il file deve essere aggiunto alla directory usata per creare l'immagine scritta sul CD-ROM. Consultare la sezione *Come creare un CD-ROM di avvio per l'installazione* nel *Red Hat Linux Installation Guide* per maggiori istruzioni sulla creazione di un CD-ROM di avvio; tuttavia, prima di creare il file d'immagine `file.iso`, copiare il file kickstart `ks.cfg` sulla directory `isolinux/`.

7.8.3. Rendere il file kickstart disponibile sulla rete

Le installazioni kickstart via rete sono molto diffuse, poiché gli amministratori di sistema possono facilmente automatizzare in modo rapido e indolore il processo di installazione su numerosi computer in rete. Di norma, l'approccio più comune prevede che l'amministratore disponga di un server BOOTP/DHCP e di un server NFS nella rete locale. Il server BOOTP/DCHP viene utilizzato per fornire al computer client le informazioni relative alla propria rete, mentre i file utilizzati nel corso dell'installazione sono forniti dal server NFS. Spesso, ma non necessariamente, questi due server funzionano sulla stessa macchina fisica.

Per effettuare un'installazione kickstart via rete, dovete avere un server BOOTP/DHCP nella vostra rete, che fornisce le informazioni di configurazione per la macchina sulla quale state installando Red Hat Linux. Il server BOOTP/DHCP viene utilizzato per trasmettere al client le informazioni di rete, così come la posizione del file kickstart.

Se un file kickstart viene specificato nel server BOOTP/DHCP, il client prova a montare via NFS il percorso del file e copia sul client il file specificato usandolo come file kickstart. Le impostazioni esatte richieste variano a seconda del tipo di server BOOTP/DHCP che usate.

Vi illustriamo un esempio tratto dal file `dhcpd.conf` per attivare un server DHCP distribuito con Red Hat Linux:

```
filename "/usr/new-machine/kickstart/";
next-server blarg.redhat.com;
```

Sostituite il valore che segue a `filename` con il nome del file kickstart (o della directory che lo contiene) e il valore che si trova dopo `next-server` con il nome del server NFS.

Se il nome del file restituito dal server BOOTP/DHCP termina con uno slash ("/"), allora viene interpretato solo come percorso. In questo caso il client monta il percorso usando il server NFS e cerca un file particolare, ovvero:

```
<ip-addr>-kickstart
```

La sezione <*indirizzo-ip*> del nome del file dovrebbe essere sostituita con l'indirizzo IP del client, scritto in decimali separati da un punto. Per esempio, il nome del file per il computer con l'indirizzo IP 10.10.0.1 è `10.10.0.1-kickstart`.

Se non specificate un nome del server, il client cerca di usare il server che fornisce il servizio BOOTP/DHCP anche come server NFS. Se non viene specificato il nome del percorso o del file, il client cerca di montare il percorso `/kickstart` dal server BOOTP/DHCP e cerca il file kickstart usando il nome del file <*indirizzo-ip*>`-kickstart` sopra descritto.

7.9. Rendere disponibile l'albero di installazione

L'installazione kickstart deve accedere a un *albero di installazione*, cioè una copia dei CD di Red Hat Linux binari con la stessa struttura di directory.

Se eseguite un'installazione da CD, inserite il CD 1 di Red Hat Linux nel computer prima di iniziare l'installazione kickstart.

Se eseguite un'installazione da disco fisso, accertatevi che le immagini ISO dei CD di Red Hat Linux binari si trovino sul disco fisso del computer.

Se eseguite un'installazione via rete (NFS, FTP o HTTP), dovete rendere l'albero di installazione disponibile sulla rete. Per maggiori dettagli, consultate la sezione *Preparing for a Network Installation* della *Red Hat Linux Installation Guide*.

7.10. Avvio di un'installazione kickstart

Per lanciare un'installazione kickstart, avviate il sistema dal dischetto di avvio di Red Hat Linux dal CD-ROM di avvio o dal CD-ROM #1 di Red Hat Linux e inserite un comando di avvio speciale al prompt. Il programma d'installazione vá alla ricerca di un file kickstart se l'argomento della linea di comando `ks` viene passata al kernel.

Boot Diskette

Se il file kickstart risiede in un dischetto di avvio come descritto in la Sezione 7.8.1, avviare il sistema con il dischetto nell'unitá, e inserire il seguente comando al prompt `boot:`:

```
linux ks=floppy
```

CD-ROM #1 and Diskette

Il comando **`linux ks=floppy`** funziona anche se il il file `ks.cfg` si trova nel filesystem vfat o ext2 su un dischetto floppy e se avviate Red Hat Linux da CD-ROM #1.

Vi è un comando di avvio alternativo per lanciare Red Hat Linux da CD-ROM #1 e avere il file kickstart in un file sistem vfat o ext2 su un dischetto floppy. Per fare ció, inserire il seguente camando al prompt `boot:`:

```
linux ks=hd:fd0:/ks.cfg
```

Con il disco Driver

Se vi occorre usare una unitá disco con kickstart, specificare l'opzione anche **`dd`**. Per esempio, per disabilitare un dischetto di avvio e usare una unitá disco, inserire il seguente comando al prompt `boot:`:

```
linux ks=floppy dd
```

Boot CD-ROM

Se il file kickstart é su di un CD-ROM di avvio come descritto in la Sezione 7.8.2, inserire il CD-ROM nel sistema, avviarlo e inserire il seguente comando al prompt `boot:` (dove `ks.cfg` é il nome del file kickstart):

```
linux ks=cdrom:/ks.cfg
```

Altre opzioni per iniziare una installazione kickstart, sono le seguenti:

`ks=nfs:`<*`server`*>`:/`<*`percorso`*>

Il programma di installazione cerca il file kickstart sul server NFS <*server*>, come file <*percorso*>. Il programma di installazione utilizza DHCP per configurare la scheda Ethernet. Per esempio, se il server NFS è server.example.com e il file kickstart

si trova nella condivisione NFS `/mydir/ks.cfg`, il comando di avvio corretto è `ks=nfs:server.example.com:/mydir/ks.cfg`.

`ks=http://<server>/<percorso>`

Il programma di installazione cerca il file kickstart sul server HTTP *<server>*, come file *<percorso>*. Il programma di installazione utilizzerà DHCP per configurare la scheda Ethernet. Per esempio, se il vostro server HTTP è server.example.com e il file kickstart si trova nella directory HTTP `/mydir/ks.cfg`, il comando di avvio corretto è `ks=http://server.example.com:/mydir/ks.cfg`.

`ks=floppy`

Il programma d'installazione cerca il file `ks.cfg` sul filesystem vfat o ext2 del floppy nell'unità `/dev/fd0`.

`ks=floppy:/<path>`

Il programma d'installazione cercherá per il file kickstart sul dischetto in `/dev/fd0`, come file *<path>*.

`ks=hd:<device>:/<file>`

Il programma d'installazione monta il filesystem sul *<dispositivo>* (che deve essere di tipo vfat o ext2) e cerca il file di configurazione kickstart come *<file>* all'interno di quel fiesystem (per esempio, `ks=hd:sda3/mydir/ks.cfg`).

Nota Bene

La seconda colonna é un cambio di sintassi per Red Hat Linux 9.

`ks=file:/<file>`

Il programma d'installazione cerca di leggere il file *<file>* dal filesystem senza eseguire alcun montaggio. Di norma, viene utilizzato quando il file kickstart si trova già nell'immagine `initrd`.

`ks=cdrom:/<percorso>`

Il programma d'installazione cerca il file kickstart sul CD, come file *<percorso>*.

`ks`

Se `ks` viene usato da solo, il programma di installazione configura la scheda di rete Ethernet utilizzando il server DHCP. Il sistema usa il "bootServer" fornito dal server DHCP come server NFS per leggere il file kickstart (per default, viene utilizzato lo stesso del server DHCP). Il nome del file kickstart può essere uno tra i seguenti:

- Se DHCP è specificato e il file di avvio comincia con uno slash `/`, il file di avvio fornito da DHCP viene cercato sul server NFS.
- Se DHCP è specificato e il file di avvio comincia con qualcosa che non sia lo slash (`/`), il file di avvio fornito da DHCP viene cercato nella directory `/kickstart` sul server NFS.
- Se DHCP non ha specificato alcun file di avvio, allora il programma di installazione cerca di leggere il file `/kickstart/1.2.3.4-kickstart`, dove *1.2.3.4* sta per l'indirizzo IP numerico della macchina che state installando.

`ksdevice=<`*`dispositivo`*`>`

Il programma di installazione utilizza questo dispositivo di rete per connettersi alla rete. Per esempio, per avviare un'installazione con il file kickstart su un server NFS connesso al sistema tramite il dispositivo eth1, digitate il comando `ks=nfs:<`*`server:`*`>:/<`*`percorso`*`> ksdevice=eth1` al prompt di avvio `boot:`.

Capitolo 8.

Configurazione Kickstart

Configurazione Kickstart vi consente di creare un file kickstart usando l'interfaccia grafica utente, in modo che non dobbiate ricordare la sintassi corretta del file.

Per utilizzare **Configurazione Kickstart**, il sistema X Window deve essere in esecuzione. Per avviare **Configurazione Kickstart**, selezionate il **Pulsante del menu principale** (sul pannello) => **Tool di sistema => Kickstart** oppure digitate il comando `/usr/sbin/redhat-config-kickstart`.

Mentre create un file kickstart, in qualsiasi momento potete selezionare **File => Anteprima** per visualizzare un'anteprima delle vostre selezioni attuali.

8.1. Configurazione di base

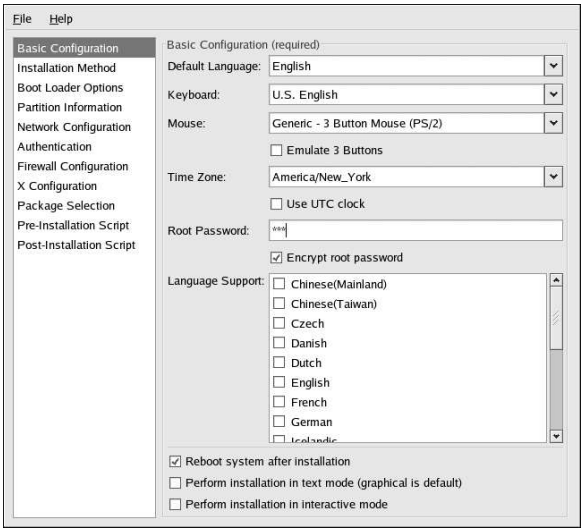

Figura 8-1. Configurazione di base

Dal menu **Lingua** scegliete la lingua da utilizzare durante l'installazione e come lingua predefinita a installazione ultimata.

Dal menu **Tastiera** selezionate il tipo di tastiera che desiderate utilizzare per il sistema.

Dal menu **Mouse** scegliete il mouse per il sistema. Se scegliete **No Mouse**, non viene configurato alcun mouse. Se scegliete **Ricerca Mouse**, il programma di installazione tenterà di rilevare automaticamente il mouse. Il rilevamento funziona per la maggior parte dei mouse moderni.

Se possedete un mouse a due tasti, potete emulare un mouse a tre tasti selezionando **Emulazione 3 pulsanti**. Se viene selezionata questa opzione, facendo clic contemporaneamente con il tasto destro e il tasto sinistro si ottiene l'effetto del terzo tasto.

Dal menu **Fuso orario** scegliete il fuso orario da utilizzare per il sistema. Per configurare il sistema in modo da usare UTC, selezionare **Usare l'orologio UTC**.

All'interno della casella di inserimento **Password di root** digitate la password di root desiderata per il sistema. Se volete salvare la password come password cifrata nel file, selezionate **Criptare password di root**. Una volta che il file è stato salvato, la password in formato testo che avete digitato viene criptata e salvata nel file kickstart. Non dovete inserire una password già criptata né tantomeno indicare al sistema di criptarla.

Per installare altre lingue in aggiunta a quella selezionata dal menu a tendina **Lingua**, controllate l'lenco **Language Support**. La lingua selezionata dal menu a tendina **Lingua** è quella utilizzata per default dopo l'installazione; tuttavia, è possibile cambiare la lingua predefinita tramite il **Strumento di configurazione della lingua** (`redhat-config-language`) a installazione ultimata.

Se scegliete **Riavviare il sistema dopo l'installazione**, il sistema viene riavviato automaticamente una volta terminata l'installazine.

Per default, le installazioni kickstart vengono eseguite in modalità grafica. Per modificare questa impostazione predefinita e utilizzare, dunque, la modalità testo, fate clic nella casella di spunta **Eseguire l'installazione in modalità testo**.

È possibile eseguire un'installazione kickstart in modalità interattiva. Ciò significa che il programma di installazione utilizzerà tutte le opzioni preconfigurate nel file kickstart, ma a ogni schermata vi consentirà di visualizzarle prima di passare alla schermata successiva. Per passare da una schermata all'altra, fate clic sul pulsante **Avanti** dopo aver approvato le impostazioni. Se le opzioni preconfigurate non vi soddisfano, potete cambiarle prima di continuare l'installazione. Se preferite questo tipo di installazione, fate clic sulla casella di spunta **Eseguire l'installazione in modalità interattiva**.

8.2. Metodo di installazione

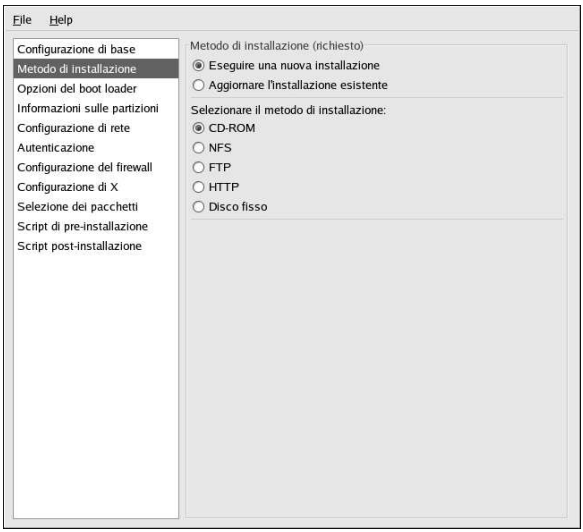

Figura 8-2. Metodo di installazione

La schermata **Metodo di installazione** vi permette di scegliere tra un'installazione completa e un aggiornamento. Se scegliete quest'ultimo, le pagine **Informazioni sulle partizioni** e **Selezione dei pacchetti** vengono disattivate. Non hanno il supporto per gli aggiornamenti di kickstart.

In questa schermata selezionate anche il tipo di installazione kickstart da eseguire, scegliendo tra le opzioni seguenti.

- **CD-ROM** — scegliete questa opzione se desiderate installare Red Hat Linux tramite i CD-ROM di Red Hat Linux.
- **NFS** — scegliete questa opzione se desiderate installare Red Hat Linux da una directory condivisa con il protocollo NFS. Compaiono due caselle di inserimento per il server NFS e la directory NFS. Inserite il nome di dominio completamente qualificato o l'indirizzo IP del server NFS. Per la directory NFS, inserite il nome della directory NFS contenente la directory dell'albero di installazione `RedHat`. Per esempio, se il vostro server NFS contiene la directory `/mirrors/redhat/i386/RedHat`, inserite `/mirrors/redhat/i386` per la directory NFS.
- **FTP** — scegliete questa opzione se desiderate installare Red Hat Linux da un server FTP. Compaiono due caselle di inserimento per il server FTP e per la directory FTP. Inserite il nome di dominio completamente qualificato o l'indirizzo IP del server FTP. Per la directory FTP, inserite il nome della directory FTP contenente la directory `RedHat`. Per esempio, se il vostro server FTP contiene la directory `/mirrors/redhat/i386/RedHat`, inserite `/mirrors/redhat/i386` per la directory FTP.
- **HTTP** — scegliete questa opzione se desiderate installare Red Hat Linux da un server HTTP. Compaiono due caselle di inserimento per il server HTTP e per la directory HTTP. Inserite il nome di dominio completamente qualificato o l'indirizzo IP del server HTTP. Per la directory HTTP, inserite il nome della directory HTTP contenente la directory `RedHat`. Per esempio, se il vostro server HTTP contiene la directory `/mirrors/redhat/i386/RedHat`, inserite `/mirrors/redhat/i386` per la directory HTTP.
- **Disco fisso** — scegliete questa opzione se desiderate installare Red Hat Linux da un disco fisso. Compaiono due caselle di inserimento per la partizione del disco fisso e la directory del disco fisso. Le installazioni da disco fisso richiedono l'utilizzo di immagini ISO (o CD-ROM). Prima di dare inizio all'installazione, assicuratevi di controllare che le immagini ISO siano intatte. Per farlo, utilizzate un programma `md5sum`. Inserite la partizione del disco fisso contenente le immagini ISO (per esempio `/dev/hda1`) nella casella di testo **Partizione del disco fisso** e nella casella **Directory del disco fisso** inserite la directory contenente le immagini ISO.

8.3. Opzioni per il boot loader

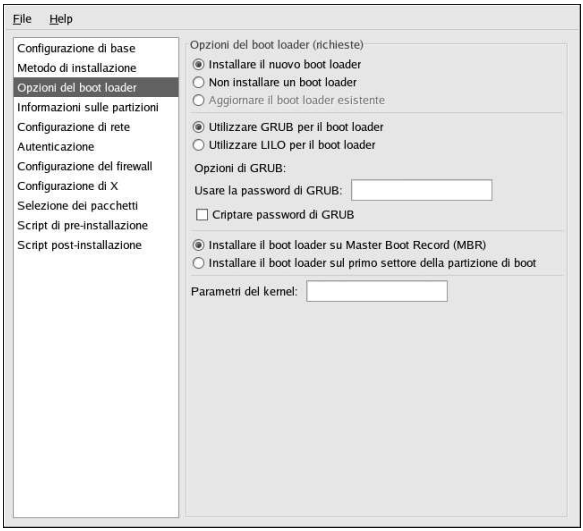

Figura 8-3. Opzioni per il boot loader

Avete la possibilità di scegliere tra GRUB o LILO come boot loader per il sistema. Se non volete installare un boot loader, rimuovete la spunta dal pulsante **Non installa il loader di avvio**. Se scegliete di non installare un boot loader, assicuratevi di creare un dischetto di avvio o di avere a disposizione un altro metodo per avviare il sistema (per esempio un boot loader di terze parti).

Se decidete di installare un boot loader, dovete scegliere quale installare (GRUB o LILO) e dove installarlo (nel Master Boot Record o nel primo settore della partizione `/boot`). Installate il boot loader nell'MBR se pensate di utilizzarlo come boot loader per il vostro sistema. Se state utilizzando un boot loader diverso, installate LILO o GRUB nel primo settore della partizione `/boot` e configurate l'altro boot loader per l'avvio di Red Hat Linux.

Se avete necessità di passare dei parametri speciali al kernel da utilizzare all'avvio del sistema, inseriteli nel campo di testo **Parametri del kernel**. Per esempio, se avete un masterizzatore per CD di tipo IDE, potete indicare al kernel di utilizzare il driver di emulazione SCSI che deve essere caricato prima di utilizzare **cdrecord** digitando **`hdd=ide-scsi`** come parametro del kernel (dove **`hdd`** è il lettore CD-ROM).

Se scegliete GRUB come boot loader, potete configurare una password di protezione impostando una password per GRUB. Inserite tale password nell'apposito campo **Usa la password di GRUB**. Se desiderate salvare la password come password criptata, selezionate **Cripta password di GRUB**. Una volta che il file è stato salvato, la password in formato testo che avete digitato viene criptata e salvata nel file kickstart. Non dovete inserire una password già criptata né tantomeno indicare al sistema di criptarla.

Se scegliete LILO come boot loader, dovete decidere se usarlo in modalità lineare e se volete imporre l'utilizzo della modalità lba32.

Se scegliete di **Aggiornare una installazione giá esistente** sulla pagina **Metodi di installazione**, potete selezionare **Aggiornare una installazione giá esistente** per aggiornare la configurazione del boot loader esistente conservando le vecchie voci in essa presenti.

8.4. Informazioni sulla partizione

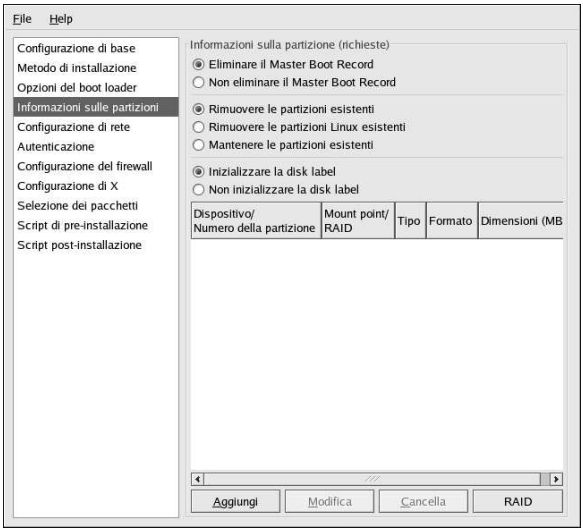

Figura 8-4. Informazioni sulla partizione

Segliete se ripulire o meno il Master Boot Record (MBR). Potete decidere di rimuovere tutte le partizioni esistenti o le sole partizioni Linux oppure di mantenere le partizioni esistenti.

È possibile inizializzare l'etichetta del disco sull'impostazione di default per l'architettura del sistema (`msdos` per x86 e `gpt` per Itanium). Selezionare **Inizializzare l'etichetta del disco** se state effettuando un'installazione su un nuovo disco fisso.

8.4.1. Creazione delle partizioni

Per creare una partizione, fate clic sul pulsante **Aggiungi**. Compare la finestra **Opzioni di partizione** mostrata nella Figura 8-5. Scegliete il mount point, il tipo di filesystem e le dimensioni per la nuova partizione. Potete anche scegliere tra le seguenti opzioni:

- Nella sezione **Opzioni aggiuntive per le dimensioni**, scegliete di attribuire alla partizione delle dimensioni fisse, stabilire che raggiunga una determinata dimensione oppure che occupi lo spazio residuo sul disco fisso. Se avete selezionato il tipo di filesystem "swap", potete decidere di far creare al programma di installazione la partizione di swap con le dimensioni consigliate invece di specificarle da voi.
- Imporre che la partizione sia creata come primaria.
- Creare la partizione su un disco fisso specifico. Per esempio, per creare la partizione sul primo disco fisso IDE (`/dev/hda`), indicate **`hda`** come disco. Non inserite `/dev` nel nome del disco.
- Utilizzare la partizione esistente. Per esempio, per creare la partizione sul primo disco fisso IDE (`/dev/hda1`), indicate **`hda1`** come la partizione. Non inserite `/dev` nel nome della partizione.
- Formattare la partizione come il filesystem prescelto.

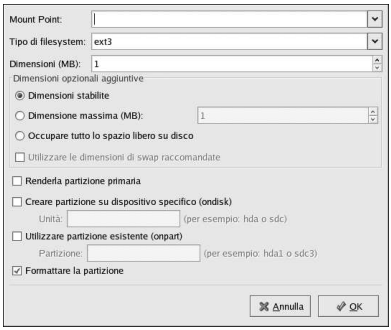

Figura 8-5. Creazione di partizioni

Per modificare una partizione esistente, selezionate la partizione dall'elenco e fate clic sul pulsante **Modifica**. Compare la stessa finestra **Opzioni di partizione** che vi viene presentata quando aggiungete una partizione come mostrato in Figura 8-5, con l'eccezione che questa volta contiene i valori relativi alla partizione selezionata. Modificate le opzioni della partizione e fate clic su **OK**.

Per cancellare una partizione esistente, selezionate la partizione dall'elenco e fate clic sul pulsante **Cancella**.

8.4.1.1. Creare partizioni RAID software

Per saperne di più sul RAID e sui vari livelli RAID, consultate il Capitolo 3. È possibile configurare il RAID sui livelli 0,1 e 5.

Per creare una partizione RAID software, eseguite quanto segue:

1. Fate clic sul pulsante **RAID**.
2. Selezionate **Create a software RAID partition**.
3. Configurate le partizioni come descritto in precedenza, selezionando però il tipo di filesystem **RAID software**. Dovete inoltre specificare su quale disco fisso desiderate creare la partizione oppure quale delle eventuali partizioni esistenti utilizzare.

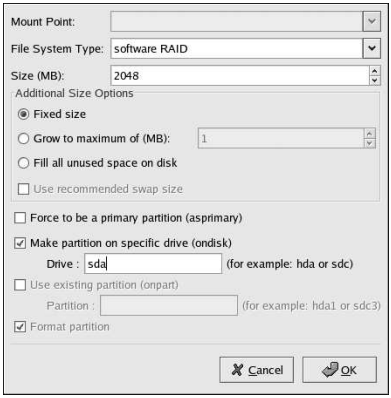

Figura 8-6. Creazione di una partizione RAID software

Ripetete queste operazioni per creare tutte le partizioni che serveno per le vostre impostazioni RAID. Tutte le vostre partizioni non devono essere necessariamente partizioni RAID.

Dopo aver creato le partizioni necessarie alla costruzione di un dispotivo RAID, eseguite quanto segue:

1. Fate clic sul pulsante **RAID**.
2. Selezionate **Crea un dispositivo RAID**.
3. Selezionate un mount point, un tipo di filesystem, un nome per il dispositivo RAID, il livello di RAID, i membri RAID, il numero di spare per il dispositivo RAID software e decidete se formattare la partizione.

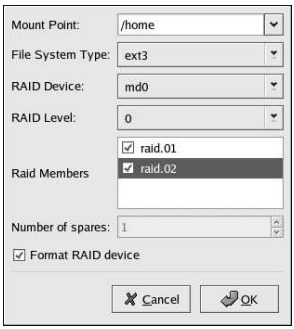

Figura 8-7. Creazione di un dispositivo RAID software

4. Fate clic su **OK** per aggiungere il dispositivo all'elenco.

8.5. Configurazione della rete

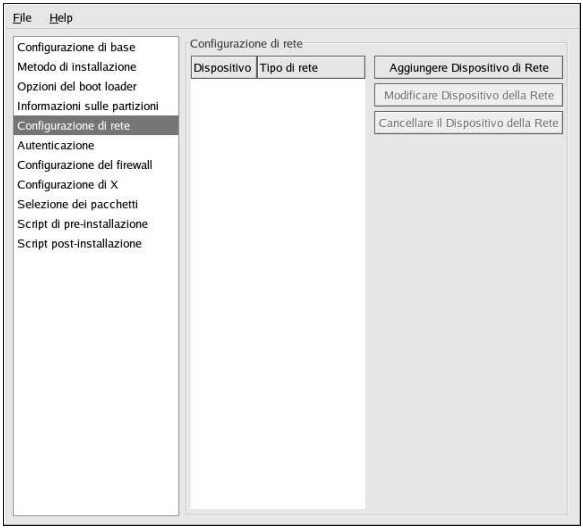

Figura 8-8. Configurazione della rete

Se il sistema che deve essere installato tramite kickstart non ha una scheda Ethernet, non configurarne uno sulla pagina **Configurazione di rete**.

Il networking è richiesto solo se scegliete un metodo di installazione di tipo networking. Networking puó sempre essere configurato dopo l'installazione con il **Strumento di amministrazione di rete** (`redhat-config-network`). Consultare Capitolo 12 per maggiori informazioni.

Per ogni scheda Ethernet sul sistema, fate clic su **Aggiungi un dispositivo di rete** e selezionare il dispositivo e il tipo di rete del dispositivo. Selezionare **eth0** come dispositivo di rete per la prima scheda Ethernet, selezionare **eth1** per la seconda scheda Ethernet e cosí via.

8.6. Autenticazione

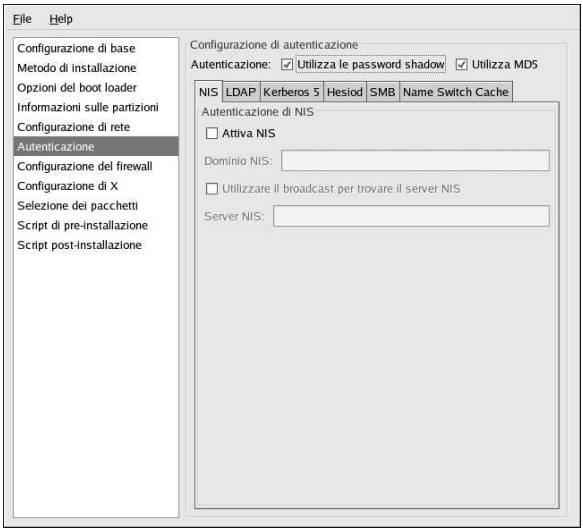

Figura 8-9. Autenticazione

Nella sezione **Autenticazione** indicate se utilizzare password shadow e cifratura MD5 per le password utente. Queste opzioni sono altamente consigliate e scelte come predefinite.

Le opzioni di **Configurazione di autenticazione** vi consentono di configurare i seguenti metodi di autenticazione:

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- Name Switch Cache

Questi metodi non sono abilitati per default. Per attivare uno o più metodi, fate clic sulla tabella corrispondente, quindi sulla casella di spunta accanto ad **Attiva** e infine inserite le informazioni relative al metodo di autenticazione.

8.7. Configurazione del firewall

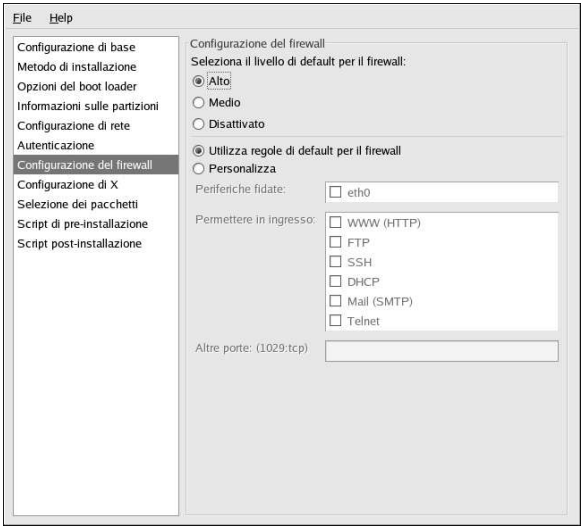

Figura 8-10. Configurazione del firewall

La finestra **Configurazione del firewall** è identica alla schermata corrispondente nel programma di installazione e il **Strumento di configurazione del livello di sicurezza**, con la medesima funzionalità. Scegliete tra i livelli di sicurezza **Alto**, **Medio** e **Disattivato**. Per informazioni dettagliate in merito a questi livelli di sicurezza, consultate la la Sezione 13.1

8.8. Configurazione di X

Se state installando il sistema X Window, potete configurarlo durante l'installazione kickstart, selezionando il relativo pulsante **Configura il sistema X Window** nella finestra **Configurazione di X** riportata nella Figura 8-11. Se non scegliete questa opzione, le opzioni di configurazione di X vengono disattivate e l'opzione `skipx` viene salvata nel file kickstart.

8.8.1. Generale

La prima operazione da svolgere nel configurare X è quella di scegliere la profondità di colore e la risoluzione predefinite, selezionandole dai rispettivi menù a tendina. Assicuratevi di specificare una profondità di colore e una risoluzione che siano compatibili con la scheda video e il monitor del vostro sistema.

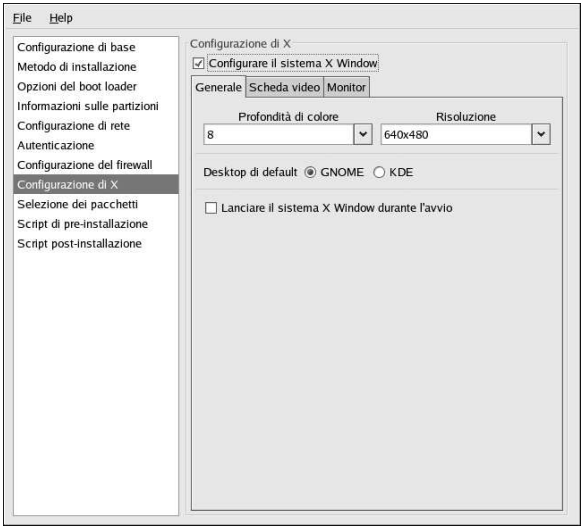

Figura 8-11. Configurazione di X - Generale

Se state installando sia il desktop di GNOME sia quello di KDE, dovete scegliere quale desktop impostare come default. Se state installando un solo desktop, assicuratevi di selezionarlo. Una volta terminata l'installazione del sistema, potete impostare il desktop di default. Per maggiori informazioni su GNOME e KDE, consultate la *Red Hat Linux Installation Guide* e la *Red Hat Linux Getting Started Guide*.

Dovete poi scegliere se far partire X Window all'avvio del sistema. Questa opzione avvia il sistema sul runlevel 5 con schermata grafica di login. Dopo che il sistema è stato installato, si possono ancora apportare cambiamenti, modificando il file di configurazione `/etc/inittab`.

8.8.2. Scheda video

Cerca una scheda video è l'impostazione predefinita. Accettate il valore di default se desiderate che il programma d'installazione esegua una verifica sulla scheda video durante l'installazione. Funziona con la maggior parte delle schede video attuali. Quando quest'opzione è selezionata, nel caso in cui non riesca a trovare la scheda video, il programma d'installazione si ferma alla schermata di configurazione della stessa. Per continuare il processo d'installazione, selezionate la scheda video prescelta dall'elenco e fate clic su **Avanti**.

In alternativa, selezionate la scheda video dall'elenco in corrispondenza di **Scheda video**, come riportato nella Figura 8-12. Dal menu a tendina **RAM della scheda video** selezionate la quantità di RAM per la scheda video prescelta. Questi valori verranno utilizzati dal programma d'installazione per configurare il sistema X Window.

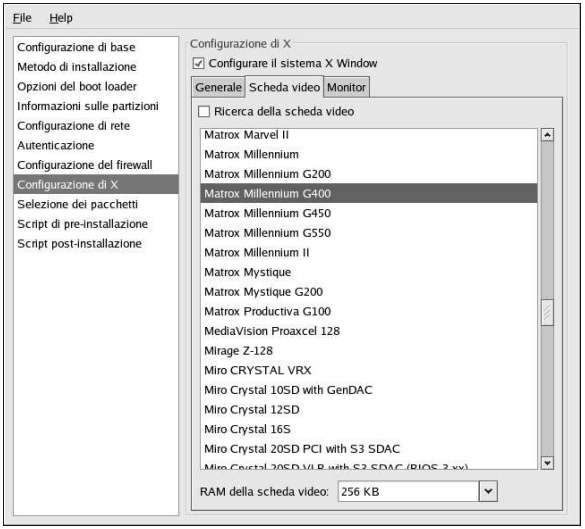

Figura 8-12. Configurazione di X - Scheda video

8.8.3. Monitor

Dopo aver configurato la scheda video, fate clic in corrispondenza di **Monitor** come illustrato nella Figura 8-13.

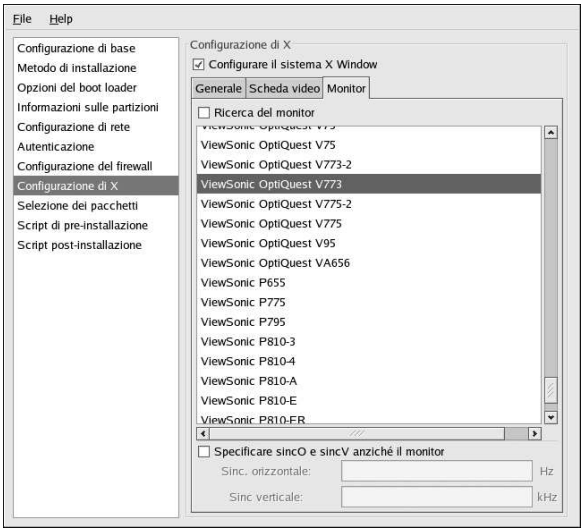

Figura 8-13. Configurazione di X - Monitor

Cerca il monitor è l'impostazione predefinita. Accettate il valore di default se desiderate che il programma d'installazione esegua una verifica sul monitor durante l'installazione. Funziona con la maggior parte dei monitor attuali. Quando quest'opzione è selezionata, nel caso in cui non riesca a verificare il monitor, il programma d'installazione si ferma alla schermata di configurazione dello stesso. Per continuare il processo d'installazione, selezionate il monitor prescelto dall'elenco e fate clic su **Avanti**.

In alternativa, selezionate il monitor dall'elenco. Potete specificare le frequenze di sincronizzazione verticale e orizzontale invece di specificare un monitor, selezionando l'opzione **Specifica hysnc e vsync anziché il monitor**. Ciò si rivela utile quando il monitor non è presente in elenco. Va ricordato che quando questa opzione viene attivata, è disattivato anche l'elenco dei monitor.

8.9. Selezione dei pacchetti

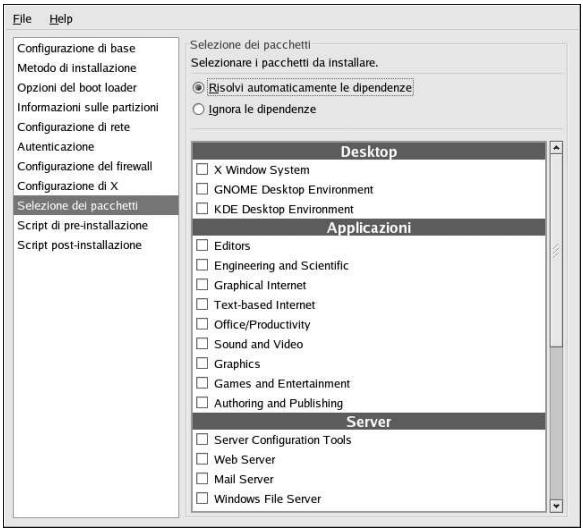

Figura 8-14. Selezione dei pacchetti

La finestra **Selezione dei pacchetti** vi consente di scegliere quali gruppi installare.

Vi sono anche opzioni atte a risolvere oppure ignorare le dipendenze fra pacchetti automaticamente.

Attualmente, **Configurazione Kickstart** non permette la selezione individuale dei pacchetti. Per installare i pacchetti singolarmente, dovete modificare la sezione `%packages` del file kickstart dopo averlo salvato. Consultate la Sezione 7.5 per maggiori informazioni.

8.10. Script di pre-installazione

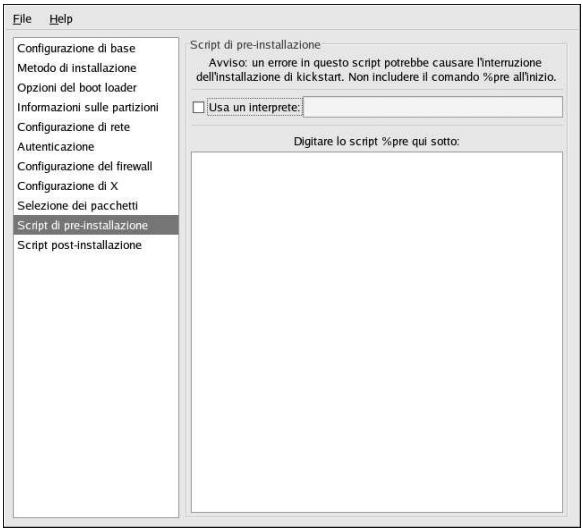

Figura 8-15. Script di pre-installazione

I comandi da eseguire sul sistema possono essere aggiunti immediatamente dopo la lettura del file kickstart e prima che inizi l'installazione. Se avete configurato la rete nel file kickstart, la rete viene attivata prima dell'elaborazione di questa sezione. Se desiderate includere uno script di pre-installazione, digitatelo nel campo di testo.

Se volete specificare un linguaggio di scripting da utilizzar per eseguire lo script, fate clic sul pulsante **Use an interpreter** e inserite l'interprete nella casella di testo posta accanto al pulsante. Per esempio, si può specificare **`/usr/bin/python2.2`** per uno script Python. Questa opzione equivale a utilizzare `%pre --interpreter` *`/usr/bin/python2.2`* nel vostro file kickstart.

Attenzione

Non includete il comando `%pre`, poiché viene aggiunto automaticamente.

8.11. Script di post-installazione

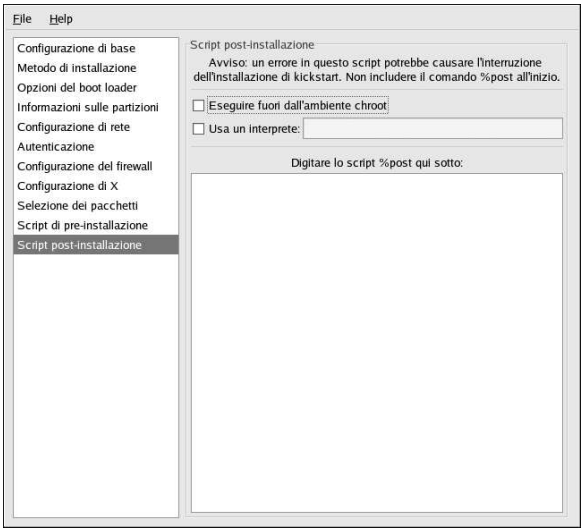

Figura 8-16. Script di post-installazione

I comandi da eseguire sul sistema possono essere aggiunti anche una volta completata l'installazione. Se avete configurato correttamente la rete nel file di kickstart, la rete è attivata. Se desiderate includere uno script di post-installazione, digitatelo nel campo di testo.


Attenzione

Non includete il comando `%post`, poiché viene aggiunto automaticamente.

Per esempio, per cambiare il "messaggio del giorno" per il sistema appena installato, aggiungete il comando seguente alla sezione `%post`:

```
echo "Hackers will be punished!" > /etc/motd
```


Suggerimento

Nella la Sezione 7.7.1 si possono reperire ulteriori esempi.

8.11.1. Ambiente chroot

Se volete che il vostro script di post-installazione sia eseguito al di fuori dell'ambiente chroot, selezionate la casella accanto a questa opzione all'inizio della finestra **Script post-installazione**. Ciò equivale a utilizzare l'opzione `--nochroot` nella sezione `%post`.

Se volete apportare qualche modifica al filesystem appena installato nella sezione di post-installazione fuori dell'ambiente chroot, dovete aggiungere `/mnt/sysimage` al nome della directory.

Per esempio, se selezionate il pulsante **Esegui fuori dall'ambiente chroot**, l'esempio precedente va modificato nel modo che segue:

```
echo "Hackers will be punished!" > /mnt/sysimage/etc/motd
```

8.11.2. Utilizzo di un interprete

Se volete specificare un linguaggio di scripting da utilizzare per eseguire il vostro script, fate clic sul pulsante **Usa un interprete** e inserite l'interprete nella casella di testo posta accanto. Per esempio, per **`/usr/bin/python2.2`** si può specificare uno script Python. Questa opzione corrisponde all'utilizzo di `%post --interpreter /usr/bin/python2.2` nel file kickstart.

8.12. Salvataggio del file

Dopo aver terminato con la selezione delle varie opzioni kickstart, se volete visualizzare in anteprima il contenuto del file kickstart, selezionate **File => Anteprima** dal menu a tendina.

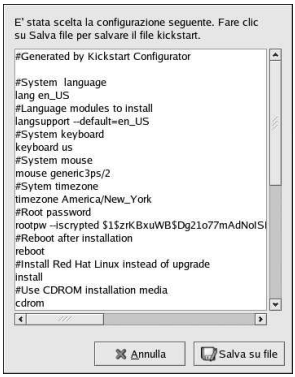

Figura 8-17. Anteprima

Per salvare il file kickstart, fate clic sul pulsante **Salva sul file** selezionate **File => Salva file** oppure premete la combinazione di tasti [Ctrl]-[S]. Comparirà una finestra di dialogo che vi permette di scegliere la posizione in cui salvare il file.

Dopo aver salvato il file, consultate la la Sezione 7.10 per informazioni su come si avvia l'installazione kickstart.

redhat.

Capitolo 9.

Recupero del sistema di base

Quando si verificano degli imprevisti, c'é sempre una via di rimedio, Tuttavia, questi rimedi, richiedono una buona comprensione del sistema. Questo capitolo descrive come effettuare l'avvio in modalitá rescue, modalitá singolo utente, e modalitá di emergenza, dove potete usare la vostra conoscenza per far fronte agli imprevisti del sistema.

9.1. Problemi comuni

Potrebbe essere necessario effettuare l'avvio in uno dei suddetti modi di recupero a causa dei seguenti motivi:

- Siete impossibilitati ad affettuare un avvio normale nel Red Hat Linux (runlevel 3 or 5).
- Avete problemi di hardware o software, e desiderate ottenere alcuni file importanti dal disco fisso del vostro sistema.
- Avete dimenticato la password di root.

9.1.1. Impossibile avviare Red Hat Linux

Questo problema viene spesso riscontrato quando si procede all'installazione di un altro sistema operativo dopo che è stato installato Red Hat Linux. Alcuni sistemi operativi presumono che non abbiate altri sistemi operativi sul vostro computer e sovrascrivono il Master Boot Record (MBR) che in origine conteneva GRUB o LILO. Se il boot loader viene sovrascritto, non potrete più avviare Red Hat Linux a meno che non utilizziate la modalità rescue.

Un altro problema comune si verifica quando modificate l'ordine delle vostre partizioni utilizzando un tool di partizionamento per ridimensionare una partizione o per crearne una nuova sfruttando lo spazio libero una volta terminata l'installazione. Se cambia il numero della vostra partizione `/`, il boot loader non è più in grado di trovarla e di montarla. Per risolvere questo problema, avviate in modalità rescue e modificate `/boot/grub/grub.conf` se state utilizzando GRUB o `/etc/lilo.conf` se state usando LILO. *Dovete* anche eseguire il comando `/sbin/lilo` ogni qualvolta che si modifica il file di configurazione di LILO.

9.1.2. Problemi hardware/software

Questa categoria comprende una grande varietà di situazioni. Alcuni esempi possono includere dischi fissi difettosi, specificazione di un dispositivo o kernel root invalido nel file di configurazione del boot loader. Se si verifica uno dei suddetti problemi, é probabile che non sarete in grado di avviare Red Hat Linux. Tuttavia, se effettuate un avvio in una dei modi di recupero indicati, potreste essere in grado di risolvare il problema oppure di riuscire a ottenere le copie dei file desiderati.

9.1.3. Password di root

Cosa potete fare se dimenticate la vostra password? Per impostare una nuova password eseguite un avvio in modalitá rescue oppure utente singolo e usare il comando `passwd` per resettare la password di root.

9.2. Avvio modalitá rescue

La modalità rescue permette di avviare un piccolo ambiente Linux direttamente da un dischetto, da un CD-ROM oppure utilizzando qualche altro metodo.

Come indica il nome, la modalità rescue vi salva da qualche cosa. Durante il funzionamento normale, il vostro sistema Red Hat Linux utilizza i file contenuti nel vostro disco rigido per eseguire programmi, immagazzinare file e altro ancora.

Tuttavia, a volte Red Hat Linux non riesce ad accedere ai file del vostro disco fisso. Grazie alla modalità rescue potete accedere ai file contenuti nel vostro disco fisso anche se non riuscite a eseguire Red Hat Linux da questo disco.

Per avviare il sistema in modalità, dovete essere in grado di avviare il sistema usando uno dei seguenti metodi:

- Avviando il sistema da un dischetto di avvio creato dall'immagine `bootdisk.img`. [1]
- Avviando il sistema da un CD-ROM di avvio dell'installazione. [2]
- Avviando il sistema dal primo CD-ROM di Red Hat Linux.

Dopo aver effettuato un avvio usando uno dei metodi descritti, inserire il seguente comando al prompt di avvio dell'installazione:

```
linux rescue
```

Vi verrá richiesto di rispondere ad alcune semplici domande, del tipo quale lingua usare. Vi sará richiesto anche di selezionare dov'é posizionata una immagine rescue valida. Selezionare da **CD-ROM locale**, **Disco fisso**, **immagine NFS**, **FTP**, o **HTTP**. La posizione selezionata deve avere un albero d'installazione valido, e il suddetto albero deve essere della stessa versione del Red Hat Linux CD-ROM #1 dal quale é stato effettuato l'avvio. Se usate un CD-ROM o dischetto d'avvio per iniziare la modalitá rescue, l'albero d'installazione deve essere lo stesso albero dal quale é stato creato il media. Per maggiori informazioni su come impostare un albero d'installazione su di un disco fisso, server NFS, server FTP o server HTTP, consultare *Red Hat Linux Installation Guide*.

Se selezionate una immagine rescue che non richiede una connessione di rete, vi sará chiesto se desiderate o meno stabilire tale connessione. Una connessione di rete é utile se avete bisogno di effettuare alcuni file di backup ad un computer diverso o installare alcuni pacchetti RPM da una posizione di rete condivisa.

Visualizzerete il seguente messaggio:

```
The rescue environment will now attempt to find your Red Hat
Linux installation and mount it under the directory
/mnt/sysimage.  You can then make any changes required to your
system.  If you want to proceed with this step choose
'Continue'. You can also choose to mount your file systems
read-only instead of read-write by choosing 'Read-only'.
If for some reason this process fails you can choose 'Skip'
and this step will be skipped and you will go directly to a
command shell.
```

Se selezionate **Continua**, l'ambiente rescue tenterà di montare il vostro file system sotto la directory `/mnt/sysimage`. Qualora non riuscisse a montare una partizione, vi manderà un avviso. Se selezionate **Solo lettura**, tenterà di montare il vostro file system sotto la directory `/mnt/sysimage`, ma in

1. Per creare un dischetto di avvio dell'installazione, inserite un dischetto vuoto e utilizzate il file `images/bootdisk.img` contenuto nel primo CD-ROM di Red Hat Linux con il comando `dd if=bootdisk.img of=/dev/fd0`.
2. Per la creazione del suddetto CD-ROM, seguite le istruzioni nel *Red Hat Linux Installation Guide*.

modalità di sola lettura. Se selezionate **Ignora**, il file system non viene montato. Scegliete **Ignora** se ritenete che il vostro file system possa essere corrotto.

Una volta che siete entrati nella modalità rescue, compare un prompt nella console virtuale (VC) 1 e 2. Per accedere alla VC 1, usate la combinazione di tasti [Ctrl]-[Alt]-[F1] , mentre per accedere alla VC 2, usate [Ctrl]-[Alt]-[F2]):

```
-/bin/sh-2.05b#
```

Se avete selezionato **Continua** per montare automaticamente le partizioni e queste sono state montate correttamente, siete in modalità utente singolo.

Se il vostro file system è montato e volete che la partizione root sia la partizione del vostro sistema invece che dell'ambiente di modalitá rescue, usare il seguente comando:

```
chroot /mnt/sysimage
```

Ciò è utile se avete bisogno di eseguire comandi come `rpm`, per i quali è necessario che la partizione root sia montata come `/`. Per uscire dall'ambiente chroot, digitate `exit` e tornerete al prompt.

Se avete selezionato **Ignora**, potete ancora tentare di montare una partizione manualmente all'interno della modalitá rescue, creando una directory come */foo*, e digitando il seguente comando:

```
mount -t ext3 /dev/hda5 /foo
```

Nel comando riportato sopra, */foo* rappresenta una directory da voi creata e */dev/hda5* è la partizione che volete montare. Se la partizione è di tipo `ext2`, sostituite `ext3` con `ext2`.

Se non conoscete i nomi delle vostre partizioni, utilizzate il seguente comando per ottenere un elenco:

```
fdisk -l
```

Dal prompt potete avviare molti comandi utili, quali:

- `list-harddrives` per ottenere una lista dei dischi fissi nel sistema
- `ssh`,`scp`, e `ping` se é avviata la rete.
- `dump` e `restore` per utenti con ---------- tape drive
- `parted` e `fdisk` per la gestione delle partizioni
- `rpm` per l'installazione o il miglioramento del software
- `joe` per la modifica dei file di configurazione (Se digitate `joe`, `emacs`, `pico`, o `vi`, sará avviato l'editor `joe`.)

9.3. Avvio della modalità utente singolo

Uno dei vantaggi della modalitá utente singolo é quella di non aver bisogno di un dischetto o un CD-ROM di avvio, tuttavia, non vi dá l'opzione di montare i file system come solo lettura o non li monta affatto.

In modalitá utente singolo, il vostro computer avvia il runlevel 1. I vostri file system locali sono montati, ma la vostra rete non é attivata. Avete a disposizione una shell di manutenzione del sistema. La modalitá ad utente singolo, automaticamente cerca di montare il vostro file system; *non* usate questa modalitá se il vostro file system non puó essere montato con successo. Inoltre non potete usare tale modalitá se la configurazione del runlevel 1 é corrotta.

Se il vostro sistema effettua un avvio, ma non vi permette di registrarvi quando ha completato tale procedura, provate allora la modalitá a utente singolo.

Se state usando GRUB, per effettuare l'avvio in modalità utente singolo dovete attenervi alle procedure seguenti:

1. Se avete configurato una password per GRUB, digitate `p` e inseritela.
2. Selezionate **Red Hat Linux** con la versione del kernel che desiderate avviare e digitate `e` per le modifiche. Vi viene presentato un elenco di oggetti nel file di configurazione relativo alla vostra selezione.
3. Selezionate la linea che comincia con `kernel` e digitate `e` per modificarla.
4. Andate in fondo alla linea e digitate **`single`**, come parola separata (premete la [Barra spaziatrice] e digitate **`single`**). Quindi premete [Invio] per uscire dalla modalità di modifica.
5. Una volta tornati alla schermata di GRUB, digitate `b` per avviare in modalità utente singolo.

Se state usando LILO, specificate una di queste opzioni al prompt di avvio di LILO (se state usando LILO in modalità grafica, dovete premere [Ctrl]-[x] per uscire dalla schermata grafica e andare al prompt `boot:`):

```
linux single
```

9.4. Avvio della modalitá di emergenza

Nella modalità di emergenza il sistema si avvia in un ambiente estremamente semplice. Il file system root viene montato in modalità di sola lettura e non viene configurato quasi niente. Il principale vantaggio della modalità di emergenza rispetto a quella a utente singolo è che i file **init** non vengono caricati. Se **init** è danneggiato o non funziona, potete sempre montare dei file system per recuperare i dati che rischiano di andare persi durante una reinstallazione.

Per avviare la modalitá di emergenza, usare lo stesso metodo descritto per la modalitá a utente singolo in la Sezione 9.3 con una sola eccezione, sostituire la parola chiave **`singolo`** con la parola **`emergenza`**.

Capitolo 10.

Configurazione del software RAID

Leggete anzitutto il Capitolo 3 per conoscere la tecnologia RAID e le differenze tra software e hardware RAID, nonché le differenze tra RAID 0, 1 e 5.

Il software RAID può essere configurato durante l'installazione grafica di Red Hat Linux oppure durante un'installazione kickstart. Questo capitolo mostra come configurare il software RAID durante l'installazione, usando l'interfaccia **Disk Druid**.

Prima di creare un dispositivo RAID, è necessario creare innanzitutto delle partizioni RAID. Per farlo seguite le istruzioni dettagliate fornite di seguito.

1. Nella schermata **Configurazione del partizionamento del disco** selezionate **Partizionamento manuale con Disk Druid**.
2. In **Disk Druid** scegliete **Nuovo** per creare una nuova partizione.
3. Non potrete immettere un mount point, ma sarà possibile farlo dopo avere creato il dispositivo RAID.
4. Scegliete **software RAID** dal menu a tendina **Tipo di filesystem** come illustrato nella Figura 10-1.

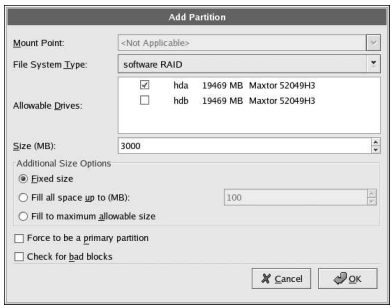

Figura 10-1. Creare una nuova partizione RAID

5. Per **Unità disponibili**, selezionate le unità sui cui creare il RAID. Se disponete di diverse unità, verranno selezionate tutte e dovrete dunque deselezionare quelle che *non* avranno alcun array RAID.
6. Inserite la dimensione desiderata per la partizione.
7. Selezionate **Dimensioni stabilite** per impostare la dimensione desiderata per la partizione, quindi **Occupa tutto lo spazio fino a (MB)** e digitate una dimensione in MB per fornire un range per la dimensione della partizione oppure selezionate **Occupa fino alle dimensioni massime consentite** per fare in modo che la partizione utilizzi tutto lo spazio residuo sul disco fisso. Se applicate questa funzione a più partizioni, lo spazio libero disponibile sul disco verrà condiviso.
8. Selezionate **Rendi la partizione primaria** se volete che la partizione sia primaria.
9. Selezionate **Controllo dei blocchi difettosi** se volete che il programma di installazione effettui un controllo per rilevare eventuali blocchi difettosi sul disco fisso prima di formattarlo.

10. Fate clic su **OK** per tornare alla schermata principale.

Ripetete questi passi per creare tutte le partizioni necessarie per configurare il vostro RAID. Non tutte le partizioni devono essere RAID. Per esempio, potete configurare la partizione `/home` come unico dispositivo software RAID.

Dopo avere creato tutte le vostre partizioni **software RAID** attenetevi alle istruzioni riportate di seguito:

1. Selezionate il pulsante **RAID** nella schermata di partizionamento principale di **Disk Druid** (vedere la Figura 10-3).
2. Verrà visualizzata la Figura 10-2, dove potete creare un dispositivo RAID.

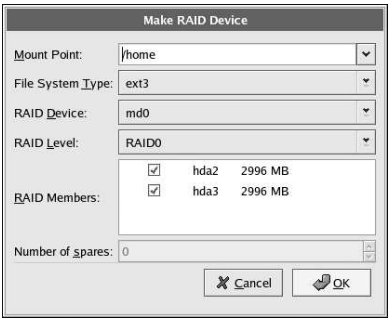

Figura 10-2. Creazione di un dispositivo RAID

3. Inserite un mount point.
4. Scegliere il tipo di filesystem per la partizione.
5. Selezionate un nome del dispositivo come **md0** per il dispositivo RAID.
6. Selezionate il vostro livello di RAID. Potete scegliere tra **RAID 0**, **RAID 1** e **RAID 5**.

Nota Bene

Se state creando una partizione RAID di `/boot`, occorre selezionare il livello 1 di RAID e utilizzare uno dei primi due dischi (prima IDE, poi SCSI). Se non state creando una partizione RAID di `/boot` ma una partizione di `/`, occorre selezionare il livello 1 di RAID e utilizzare uno dei primi due dischi (prima IDE e poi SCSI).

7. Le partizioni RAID appena create, appariranno nella lista **Membri RAID**. Selezionate quali partizioni devono essere usate per creare il dispositivo RAID.
8. Si può specificare una partizione di riserva (spare) per RAID 1 e RAID 5. Se una partizione software RAID si blocca, quella di riserva entra automaticamente in funzione per sostituirla. Per ogni partizione di riserva che volete specificare, dovete creare una partizione software RAID aggiuntiva (oltre alle partizioni per il dispositivo RAID). Nel passo precedente, selezionate le partizioni per il dispositivo RAID e le partizioni per le riserve.
9. Dopo aver cliccato su **OK** il dispositivo RAID apparirá nella lista **Drive Summary** come mostrato su Figura 10-3. A questo punto, potete continuare con il vostro processo d'installazione. Per maggiori informazioni consultate *Red Hat Linux Installation Guide*

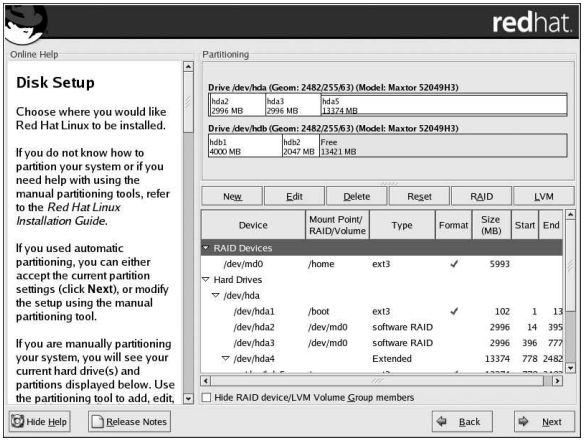

Figura 10-3. Creazione di un array RAID

Capitolo 11.

Configurazione dell'LVM

L'LVM può essere configurato durante l'installazione grafica di Red Hat Linux oppure durante l'installazione di kickstart. Potete utilizzare le utilità del pacchetto `lvm` per configurare il vostro LVM, ma queste istruzioni si concentrano sull'utilizzo di **Disk Druid** durante l'installazione di Red Hat Linux per effettuare questa operazione.

Leggete innanzitutto Capitolo 4 per maggiori informazioni sull'LVM. Di seguito è riportata una descrizione generale delle istruzioni necessarie per configurare l'LVM:

- Create *volumi fisici* dai dischi fissi.
- Create *gruppi di volumi* dai volumi fisici.
- Create *volumi logici* dai gruppi di volumi e assegnate a tali volumi i mount point.

Nota Bene

Potete modificare i gruppi di volumi LVM solo in modalità di installazione dell'interfaccia utente. Nell'installazione in modalità di testo potete assegnare i mount point a volumi logici esistenti.

Per creare un gruppo di volumi logici con i volumi logici durante l'installazione di Red Hat Linux:

1. Nella schermata **Configurazione del partizionamento del disco** selezionate **Partizionamento manuale con Disk Druid**.
2. Selezionate **Nuovo**.
3. Anche se ora non è possibile immettere un mount point, lo sarà dopo avere creato il gruppo di volumi.
4. Selezionare **volume fisico (LVM)** dal menu a tendina **Tipo di filesystem** come illustrato nella Figura 11-1.

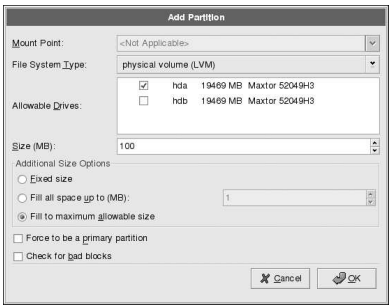

Figura 11-1. Creazione di un volume fisico

5. Un volume fisico deve essere limitato a un'unità. Per **Unità disponibili** selezionare l'unità in cui creare il volume fisico. Se disponete di più unità, in questo contesto appariranno tutte selezionate e sarete voi a decidere quale unità scegliere.
6. Immettete la dimensione desiderata per il volume fisico.
7. Selezionate **Dimensioni stabilite** per impostare la dimensione specificata del volume fisico, selezionate **Occupa tutto lo spazio fino a (MB)** e digitate una dimensione in MB per fornire il range per la dimensione del volume fisico oppure selezionate **Occupa fino alle dimensioni massime consentite** per fare in modo che aumenti fino a occupare lo spazio disponibile sul disco fisso. Più volumi di questo tipo condivideranno lo spazio libero disponibile sul disco.
8. Selezionate **Rendi la partizione primaria** se desiderate che la partizione sia primaria.
9. Selezionate **Controllo dei blocchi difettosi** se desiderate che il programma di installazione verifichi la presenza di blocchi corrotti sul disco fisso prima della formattazione.
10. Fate clic su **OK** per tornare alla schermata principale.

Ripetete queste istruzioni per creare il numero di volumi fisici desiderato per l'impostazione di LVM. Se, per esempio, desiderate che il gruppo di volumi sia disponibile su più unità, create un volume fisico su ciascuna delle unità.

Avvertenza

La partizione `/boot` può non essere su un gruppo di volumi perché il boot loader non è in grado di leggerlo. Se desiderate che la partizione root si trovi su un volume logico, sarà necessario creare una partizione `/boot` separata che non sia parte di un gruppo di volumi.

Dopo avere creato tutti i volumi fisici, attenetevi alle seguenti istruzioni:

1. Fate clic sul pulsante **LVM** per unire i volumi fisici in gruppi di volumi. Un gruppo di volumi è principalmente un insieme di volumi fisici. Potete disporre di più gruppi di volumi logici, ma un volume fisico può trovarsi solo in un gruppo di volumi.

Nota Bene

Nel gruppo di volumi logici è presente dello spazio in eccesso riservato. La somma dei volumi fisici potrebbe non essere uguale alla dimensione del gruppo di volumi. Tuttavia, la dimensione dei volumi logici visualizzata è corretta.

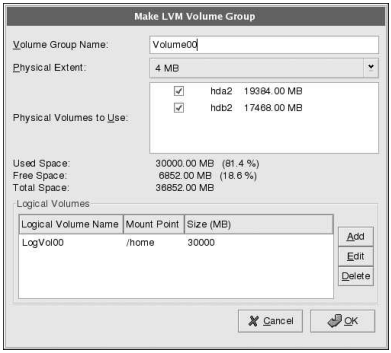

Figura 11-2. Creazione di un dispositivo LVM

2. Modificate il **Nome gruppo di volumi** se lo desiderate.
3. Tutti i volumi logici all'interno del gruppo di volumi devono essere allocati nelle unità delle *dimensioni fisiche*. Per default, le dimensioni fisiche sono impostate a 4 MB. In questo modo le dimensioni dei volumi logici devono essere divisibili per 4 MB. Se immettete una dimensione che non sia un multiplo di 4 MB, il programma di installazione selezionerà automaticamente la dimensione più prossima a un multiplo di 4 MB. Non è consigliabile modificare questa impostazione.
4. Selezionate i volumi fisici da utilizzare per il gruppo di volumi.
5. Create volumi logici con mount point come `/home`. Ricordate che `/boot` non può essere un volume logico. Per aggiungere un volume logico, fate clic sul pulsante **Aggiungi** nella sezione **Volumi logici**. Verrà visualizzata la finestra di dialogo illustrata nella Figura 11-3.

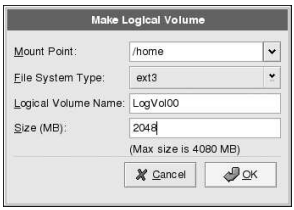

Figura 11-3. Creazione di un volume logico

Ripetete le istruzioni per ciascun gruppo di volumi che desiderate creare.

Suggerimento

Potete lasciare dello spazio libero nel gruppo di volumi logici per poter espandere i volumi in un secondo tempo.

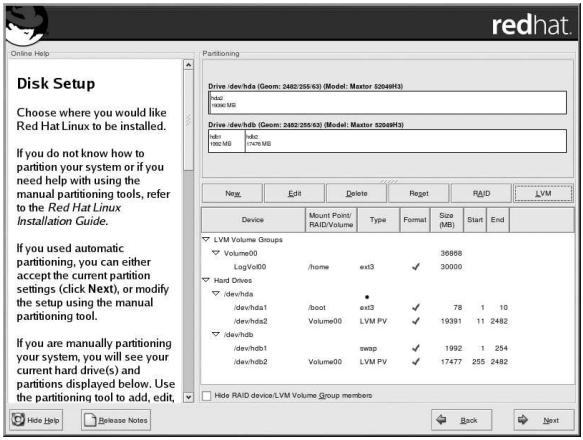

Figura 11-4. Volumi logici creati

III. Configurazione relativa alla rete

Dopo aver spiegato come configurare la rete, questo capitolo discute gli argomenti inerenti la rete, ad esempio come abilitare i login remoti, condivisioni dei file e directory attraverso la rete, ed impostazione di un server Web.

Sommario

Capitolo 12.

Configurazione di rete

Computer diversi comunicano tra di loro attraverso una connessione di rete che consente al sistema operativo di riconoscere una scheda di interfaccia (Ethernet, modem ISDN, o token ring) e di configurarla per connettersi alla rete.

Il **Strumento di amministrazione di rete** permette di configurare i tipi di interfacce di rete riportati di seguito:

- Ethernet
- ISDN
- modem
- xDSL
- token ring
- CIPE
- dispositivi wireless

Per utilizzare il **Strumento di amministrazione di rete**, dovete avere i privilegi root. Per avviare l'applicazione selezionate **Pulsante del menu principale** (sul pannello) **=> Impostazioni di sistema => Rete** oppure digitate il comando `redhat-config-network` al prompt della shell (per esempio, in un **terminale XTerm** o in un **terminale GNOME**). Se digitate il comando, viene mostrata la versione grafica se X é stato eseguito, altrimenti verrá visualizzata la versione di testo. Per forzare l'esecuzione della versione testo, usare il comando `redhat-config-network-tui`.

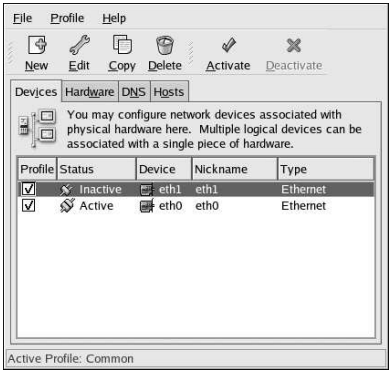

Figura 12-1. Strumento di amministrazione di rete

Se preferite modificare direttamente i file di configurazione, fate riferimento alla *Red Hat Linux Reference Guide* per informazioni sulla loro posizione e i contenuti.

Suggerimento

Consultate l'elenco dei componenti hardware compatibili di Red Hat sul sito http://hardware.redhat.com/hcl/ per verificare che Red Hat Linux supporti il vostro dispositivo hardware.

12.1. Panoramica

Per configurare una connessione di rete con il **Strumento di amministrazione di rete**, seguite le procedure qui riportate:

1. Aggiungete l'hardware fisico all'elenco degli hardware.
2. Aggiungete un dispositivo di rete associato all'hardware fisico.
3. Configurate gli hostname e le impostazioni DNS.
4. Configurate gli hostname e le impostazioni DNS.

Questo capitolo illustra le procedure per ciascun tipo di connessione di rete.

12.2. Stabilire una connessione Ethernet

Per stabilire una connessione Ethernet, sono necessari una scheda di interfaccia (NIC), un cavo di rete (in genere un cavo CAT5) e una rete cui connettersi. Poiché esistono diverse velocità di connessione, assicuratevi la vostra NIC sia compatibile con la rete cui desiderate connettervi.

Per aggiungere una connessione Ethernet, eseguite le seguenti procedure:

1. Fate clic sulla scheda **Dispositivi**.
2. Fate clic sul pulsante **Nuovo** sulla barra degli strumenti.
3. Selezionate la voce **Ethernet connection** dall'elenco **Tipo di dispositivo**, e fate clic su **Forward**.
4. Se avete già aggiunto la scheda di interfaccia di rete all'elenco hardware, selezionate la voce corrispondente dall'elenco **Ethernet card**. In caso contrario, selezionate **Other Ethernet Card** per aggiungere il dispositivo hardware.

   

   Nota Bene

   Normalmente, il programma di installazione individua automaticamente i dispositivi Ethernet supportati e vi chiede di configurarli. Se durante l'installazione avete configurato dei dispositivi Ethernet, questi verranno visualizzati nell'elenco hardware all'interno della scheda **Hardware**.

5. Se avete selezionato **Other Ethernet Card**, comparirà la finestra **Select Ethernet Adapter**. Selezionate il produttore e il modello della scheda Ethernet, quindi il nome del dispositivo. Se si tratta della prima scheda Ethernet del sistema, selezionate **eth0** come nome, se invece è la seconda selezionate **eth1**, e così via. Il **Strumento di amministrazione di rete** vi consente anche di configurare le risorse per la NIC. Fate clic su **Forward** per continuare.
6. Dalla pagina **Configurare le impostazioni di rete**, scegliete DHCP o un indirizzo IP statico, come illustrato in Figura 12-2. Non specificate un hostname se il dispositivo riceve un indirizzo IP ogni volta che viene stabilita la connessione di rete. Fate clic su **Forward** per continuare.
7. Fate clic su **Applica** nella pagina **Create Ethernet Device**.

Figura 12-2. Impostazioni Ethernet

Una volta terminata la sua configurazione, il dispositivo Ethernet verrà visualizzato nell'elenco dispositivi come mostra la Figura 12-3.

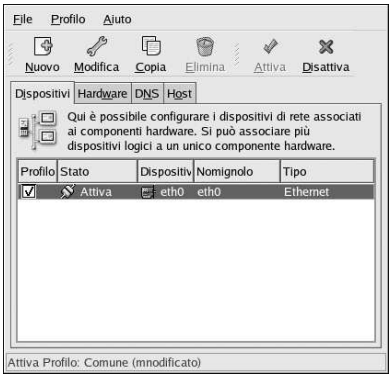

Figura 12-3. Dispositivo Ethernet

Assicurarsi di selezionare **File => Salva** per cambiare i cambiamenti.

Dopo aver aggiunto il dispositivo Ethernet, è possibile modificarne le impostazioni selezionando la voce relativa dall'elenco dispositivi e cliccando su **Modifica**. Per esempio, quando aggiungete il dispositivo, questo verrà lanciato di default all'avvio del sistema. Per cambiare questa impostazione, scegliere di modificare il dispositivo, modificare il valore **Attivare il dispositivo quando si avvia il computer**, e salvare i cambiamenti.

Quando viene aggiunto un dispositivo, esso non viene attivato immediatamente, come mostrato dal proprio stato **Inattivo**. Per attivarlo, selezionarlo dall'elenco e fate clic sul pulsante **Attivare**. Se il sistema é configurato per attivare il dispositivo al momento dell'avvio del computer (di default), questa fase non deve essere eseguita.

Associando più di un dispositivo alla stessa scheda Ethernet, i dispositivi successivi sono *alias dispositivo*. Gli alias vi permettono di impostare dispositivi virtuali multipli per un singolo dispositivo

fisico, dando cosí piú di un indirizzo IP. Potete, ad esempio, configurare un dispositivo eth1 e un dispositivo eth1:1. Per maggiori informazioni, consultate la Sezione 12.13.

12.3. Stabilire una connessione ISDN

La connessione ISDN è una connessione Internet stabilita mediante una scheda modem ISDN attraverso una speciale linea telefonica installata dalla società dei telefoni. Questo tipo di connessione è diffuso in Europa.

Per aggiungere una connessione ISDN eseguite le seguenti procedure:

1. Fate clic sulla scheda **Dispositivi**.
2. Fate clic sul pulsante **Nuovo**sulla barra degli strumenti.
3. Nell'elenco **Tipo di dispositivo**, selezionate **ISDN connection** e fate clic su **Forward**.
4. Selezionate l'adattatore ISDN dal menu a tendina. Configurate poi le risorse di sistema e il Protocollo Canale D. Fate clic su **Forward** per continuare.

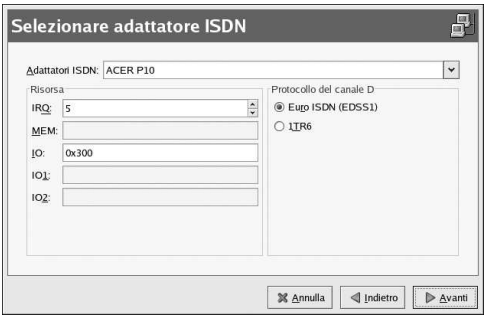

Figura 12-4. Impostazioni ISDN

5. Selezionate l'ISP, se presente nell'elenco preconfigurato. In caso contrario, inserite le informazioni richieste relative al vostro account con il provider. Se non conoscete i valori richiesti, contattate direttamente l'ISP. Fate clic su **Forward**.
6. Nella finestra **Impostazioni IP**, selezionare **Modalitá Encapsulation** e ottenere un indirizzo IP tramite DHCP o impostarne uno in modo statico. Fate clic su **Forward** quando avete terminato.
7. Nella pagina **Create Dialup Connection**, fate clic su **Applica**.

Dopo aver terminato la configurazione del dispositivo ISDN, nell'elenco dispositivi compare la voce **ISDN** come mostra la Figura 12-5.

Assicurarsi di selezionare **File => Salva** per cambiare i cambiamenti.

Una volta aggiunto il dispositivo ISDN, è possibile modificarne le impostazioni selezionando la voce relativa dall'elenco dispositivi e facendo clic su **Modifica**. Per esempio, quando aggiungete il dispositivo, questo verrà lanciato di default all'avvio del sistema, ma cambiando la sua configurazione potete modificarne l'impostazione. Potete intervenire anche in merito a compressione, opzioni PPP, nome di login, password e altro ancora.

Quando viene aggiunto un dispositivo, esso non viene attivato immediatamente, come mostrato dal proprio stato **Inattivo**. Per attivarlo, selezionarlo dall'elenco e fate clic sul pulsante **Attivare**. Se

il sistema é configurato per attivare il dispositivo al momento dell'avvio del computer (di default), questa fase non deve essere eseguita.

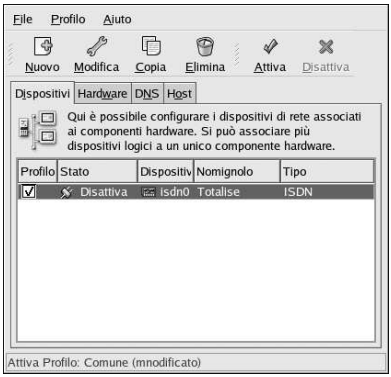

Figura 12-5. Dispositivo ISDN

12.4. Stabilire una connessione via modem

Il modem consente di configurare la connessione Internet attraverso una linea telefonica attiva. È necessario disporre di un account con un provider di servizi Internet (ISP) (definito anche account dial-up).

Per aggiungere una connessione via modem, eseguite la seguente procedura:

1. Fate clic sulla scheda **Dispositivi**.
2. Fate clic sul pulsante **Nuovo**sulla barra degli strumenti.
3. Nell'elenco **Tipo di dispositivo**, selezionate **Modem connection** e fate clic su **Forward**.
4. Se nell'elenco modem (alla voce **Hardware**) è presente un modem già configurato, il **Strumento di amministrazione di rete** presume vogliate utilizzarlo per stabilire una connessione via modem. In caso contrario, ricerca qualsiasi modem installato sul sistema. Questa operazione potrebbe richiedere del tempo. Se il modem non viene trovato, viene visualizzato un messaggio avvisandovi che le impostazioni mostrate non sono valori trovati dalla ricerca.
5. In seguito, compare la finestra in Figura 12-6.

Figura 12-6. Impostazioni modem

6. Configurate la frequenza baud, il controllo di flusso e il volume del modem. Se non conoscete questi valori, accettate quelli predefiniti. Se non usate la composizione a toni, deselezionate la casella di spunta corrispondente. Fate clic su **Forward**.
7. Selezionate l'ISP, se presente nell'elenco preconfigurato. In caso contrario, inserite le informazioni richieste relative al vostro account con il provider. Se non conoscete i valori richiesti, contattate direttamente l'ISP. Fate clic su **Forward**.
8. Nella pagina **Impostazioni IP**, selezionate se ottenere un indirizzo IP tramite DHCP oppure impostarne uno in modo statico. Fate clic su **Forward** quando terminato.
9. Nella pagina **Create Dialup Connection**, fate clic su **Applica**.

Terminata la configurazione del dispositivo modem, questo comparirà nell'elenco dispositivi con la tipologia `Modem` come mostrato nella Figura 12-7.

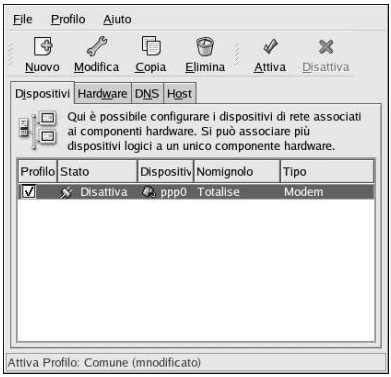

Figura 12-7. Dispositivo modem

Assicurarsi di selezionare **File => Salva** per cambiare i cambiamenti.

Una volta aggiunto il dispositivo modem, è possibile modificarne le impostazioni selezionando la voce relativa dall'elenco dispositivi e facendo clic su **Modifica**. Per esempio, quando aggiungete il dispositivo, questo verrà lanciato di default all'avvio del sistema, ma cambiando la sua configurazione

potete modificarne l'impostazione. Potete intervenire anche in merito a compressione, opzioni PPP, nome di login, password e altro ancora.

Quando viene aggiunto un dispositivo, esso non viene attivato immediatamente, come mostrato dal proprio stato **Inattivo**. Per attivarlo, selezionarlo dall'elenco e fate clic sul pulsante **Attivare**. Se il sistema é configurato per attivare il dispositivo al momento dell'avvio del computer (di default), questa fase non deve essere eseguita.

12.5. Stabilire una connessione xDSL

DSL è l'acronimo di Digital Subscriber Lines. Esistono diversi tipi di DSL: ADSL, IDSL e SDSL. Il **Strumento di amministrazione di rete** utilizza il termine xDSL con riferimento a tutti i tipi di connessione DSL.

Alcuni provider DSL richiedono di configurare il sistema per ottenere un indirizzo IP mediante DHCP con una scheda Ethernet, mentre altri necessitano una connessione PPPoE (Point-to-Point Protocol su Ethernet) con una scheda Ethernet. Chiedete al vostro provider DSL quale metodo usare.

Se è richiesto l'uso del DHCP, consultate la Sezione 12.2 per configurare la scheda Ethernet.

Se è richiesto l'uso del PPPoE, seguite le istruzioni riportate:

1. Fate clic sulla scheda **Dispositivi**.
2. Fate clic sul pulsante **Aggiungi**.
3. Nell'elenco **Tipo di dispositivo**, selezionate **xDSL connection** e fate clic su **Forward**.
4. Selezionate la voce **Ethernet Device** dal menu a tendina dalla pagina mostrata nella Figura 12-8 qualora l'elenco hardware presenti già la vostra scheda Ethernet. Altrimenti, apparirà la finestra **Select Ethernet Adapter**.

Nota Bene

Generalmente, il programma di installazione individua i dispositivi Ethernet supportati e ne richiede la configurazione. Eventuali dispositivi Ethernet configurati durante l'installazione saranno visualizzati nell'elenco hardware alla voce **Hardware**.

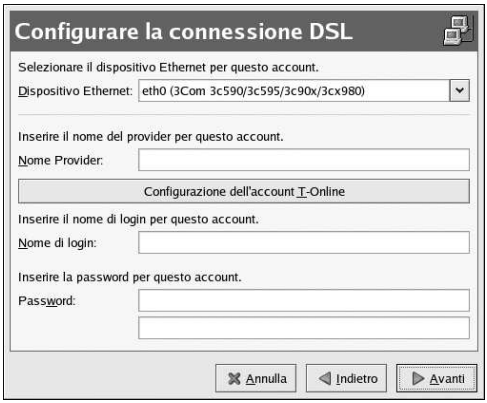

Figura 12-8. Impostazioni xDSL

5. Nella finestra **Select Ethernet Adapter**, selezionate il produttore e il modello della scheda Ethernet, quindi il nome del dispositivo. Se si tratta della prima scheda Ethernet del sistema, selezionate **eth0** come nome, se invece è la seconda selezionate **eth1**, e così via. Il **Strumento di amministrazione di rete** vi consente anche di configurare le risorse per la NIC. Fate clic su **Forward** per continuare.
6. Inserite le informazioni necessarie nei campi **Provider Name**, **Login Name**, e **Password**. Se avete un account T-Online, invece di inserire un **Login Name** e **Password** nella finestra di default, fate clic sul pulsante **T-Online Account Setup** e inserire le informazioni necessarie. Fate clic su **Forward** per continuare.
7. Nella pagina **Create DSL Connection**, fate clic su **Applica**.

La connessione DSL impostata comparirà nell'elenco dispositivi, come mostrato nella Figura 12-7.

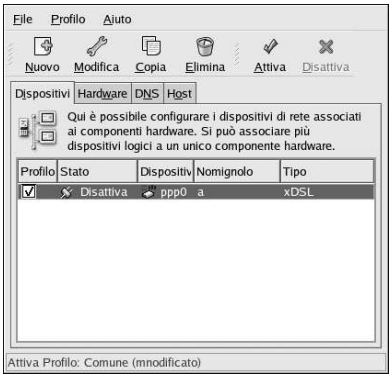

Figura 12-9. Dispositivo xDSL

Assicurarsi di selezionare **File => Salva** per cambiare i cambiamenti.

Una volta aggiunta la connessione xDSL, è possibile modificarne le impostazioni selezionando la voce relativa dall'elenco dispositivi e facendo clic su **Modifica**. Per esempio, quando aggiungete il dispositivo, questo verrà lanciato di default all'avvio del sistema, ma potete modificarne l'impostazione cambiando la sua configurazione.

Quando viene aggiunto un dispositivo, esso non viene attivato immediatamente, come mostrato dal proprio stato **Inattivo**. Per attivarlo, selezionarlo dall'elenco e fate clic sul pulsante **Attivare**. Se il sistema é configurato per attivare il dispositivo al momento dell'avvio del computer (di default), questa fase non deve essere eseguita.

12.6. Stabilire una connessione Token Ring

In una rete token ring tutti i computer sono connessi tramite un unico cavo circolare. I computer possono scambiare le informazioni tramite il *token*, uno speciale pacchetto di rete, che circola sulla token ring.

Suggerimento

Per ulteriori informazioni sull'impiego di token ring con Linux, consultate il sito Web *Linux Token Ring Project* all'indirizzo http://www.linuxtr.net.

Per aggiungere una connessione token ring, eseguite le seguenti procedure:

1. Fate clic sulla scheda **Dispositivi**.
2. Fate clic sul pulsante **Nuovo** sulla barra degli strumenti.
3. Nell'elenco **Tipo di dispositivo**, selezionate **Token Ring connection** e fate clic su **Forward**.
4. Se avete già aggiunto la scheda token ring all'elenco hardware, selezionate la voce relativa dall'elenco **Ethernet card**. Altrimenti, selezionate la voce **Other Tokenring Card** per aggiungere il dispositivo hardware.
5. Se avete selezionato **Other Tokenring Card**, apparirà la finestra **Select Token Ring Adapter**, come mostrato nella Figura 12-10. Selezionate il produttore e il modello dell'adattatore, quindi il nome del dispositivo. Se si tratta della prima scheda token ring del sistema, selezionate **tr0**, se invece è la seconda selezionate **tr1**, e così via. Il **Strumento di amministrazione di rete** vi consente anche di configurare le risorse di sistema per l'adattatore. Fate clic su **Forward** per continuare.

Figura 12-10. Impostazioni token ring

6. Nella pagina **Configure Network Settings**, specificate il DHCP, l'indirizzo IP statico, ed eventualmente l'hostname. Se il dispositivo riceve un indirizzo IP dinamico ogni volta che viene attivata la connessione di rete, non specificate l'hostname. Fate clic su **Forward** per continuare.
7. Fate clic su **Applica** nella pagina **Create Ethernet Device**.

Il dispositivo token ring configurato comparirà nell'elenco dispositivi, come mostra la Figura 12-11.

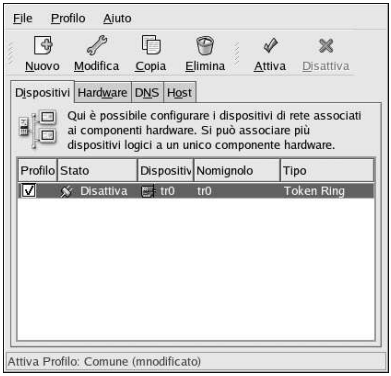

Figura 12-11. Dispositivo token ring

Assicurarsi di selezionare **File => Salva** per cambiare i cambiamenti.

Una volta aggiunto il dispositivo, è possibile modificarne le impostazioni selezionando la voce relativa dall'elenco dispositivi e facendo clic su **Modifica**. Per esempio, potete stabilire se lanciarlo all'avvio del sistema.

Quando viene aggiunto un dispositivo, esso non viene attivato immediatamente, come mostrato dal proprio stato **Inattivo**. Per attivarlo, selezionarlo dall'elenco e fate clic sul pulsante **Attivare**. Se il sistema é configurato per attivare il dispositivo al momento dell'avvio del computer (di default), questa fase non deve essere eseguita.

12.7. Stabilire una connessione CIPE

CIPE è l'acronimo di Crypto IP Encapsulation. Viene utilizzato per configurare il dispositivo IP per il tunneling. Il CIPE può, per esempio, essere utilizzato per assicurare l'accesso dall'esterno in un Virtual Private Network (VPN). Se avete l'esigenza di impostare un dispositivo CIPE, contattate il vostro amministratore di sistema per i valori corretti.

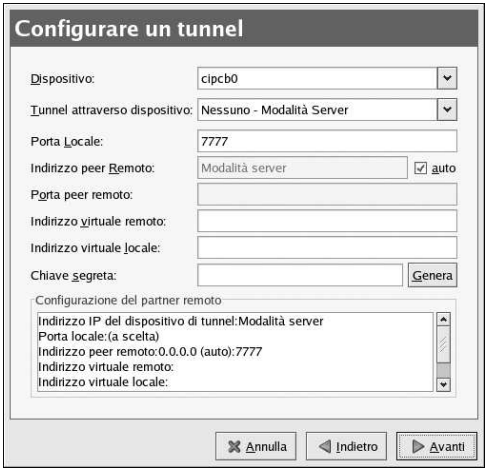

Figura 12-12. Impostazioni CIPE

Suggerimento

Per maggiori informazioni su CIPE e su come impostare CIPE, consultate *Red Hat Linux Security Guide*.

12.8. stabilire una connessione wireless

I dispositivi wireless sono sempre più utilizzati. La loro configurazione è simile a quella di un dispositivo Ethernet, ma offre anche la possibilità di impostare l'SSID, e il tasto per il dispositivo wireless.

Per aggiungere una connessione Ethernet wireless, eseguite la seguente procedura:

1. Fate clic sulla scheda **Dispositivi**.
2. Fate clic sul pulsante **Nuovo** sulla barra degli strumenti.
3. Nell'elenco **Tipo di dispositivo**, selezionate **Wireless connection** e fate clic su **Avanti**.
4. Se avete già aggiunto la scheda di interfaccia di rete wireless all'elenco hardware, selezionate la voce relativa dall'elenco **Ethernet card**. Altrimenti, selezionate **Other Ethernet Card** per aggiungere il dispositivo hardware.

   Nota Bene

   Generalmente, il programma di installazione individua i dispositivi Ethernet wireless supportati e ne richiede la configurazione. Eventuali dispositivi configurati durante l'installazione saranno visualizzati nell'elenco hardware alla voce **Hardware**.

5. Se avete selezionato **Other Wireless Card**, apparirà la finestra **Select Ethernet Adapter**. Selezionate il produttore e il modello della scheda Ethernet, quindi il dispositivo. Se si tratta della

prima scheda Ethernet del sistema, selezionate **eth0**, se invece è la seconda selezionate **eth1**, e così via. Il **Strumento di amministrazione di rete** vi consente anche di configurare le risorse di sistema per la scheda di interfaccia di rete wireless. Fate clic su **Forward** per continuare.

6. Nella pagina **Configure Wireless Connection** come mostrato in Figura 12-13, configurate le impostazioni per il dispositivo wireless.

Figura 12-13. Impostazioni wireless

7. Nella pagina **Configure Network Settings**, specificate il DHCP, l'indirizzo IP statico, ed eventualmente l'hostname. Se il dispositivo riceve un indirizzo IP dinamico ogni volta che viene attivata la connessione di rete, non specificate l'hostname. Fate clic su **Forward** per continuare.
8. Fate clic su **Applica** nella pagina **Create Wireless Device**.

Il dispositivo wireless configurato apparirà nell'elenco dispositivi come mostrato nella Figura 12-14.

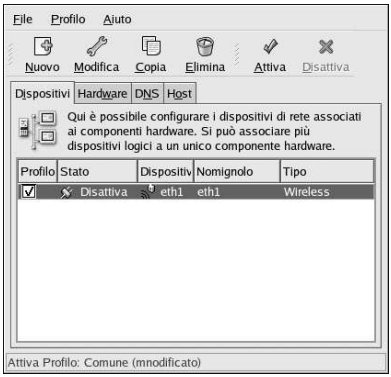

Figura 12-14. Dispositivo wireless

Assicurarsi di selezionare **File => Salva** per cambiare i cambiamenti.

Una volta aggiunto il dispositivo wireless, è possibile modificarne le impostazioni selezionando la voce relativa dall'elenco dispositivi e facendo clic su **Modifica**. Per esempio, potete configurarlo affinché si attivi all'avvio del sistema.

Quando viene aggiunto un dispositivo, esso non viene attivato immediatamente, come mostrato dal proprio stato **Inattivo**. Per attivarlo, selezionarlo dall'elenco e fate clic sul pulsante **Attivare**. Se il sistema é configurato per attivare il dispositivo al momento dell'avvio del computer (di default), questa fase non deve essere eseguita.

12.9. Gestione impostazioni DNS

La scheda **DNS** consente di configurare l'hostname di sistema, il dominio, i name server e il dominio di ricerca. I name server sono utilizzati per consultare altri host sulla rete.

Se i nomi del server DNS vengono ripresi da DHCP o PPPoE (oppure da ISP), non aggiungere server DNS primari, secondari e terziari.

Se l'hostname viene ripreso in modo dinamico da DHCP o PPPoE (oppure ISP), non cambiatelo.

Figura 12-15. Configurazione DNS

Nota Bene

La sezione dei server del nome non configura il sistema per essere un server del nome. Invece, configura i suddetti server all'uso nel risolvere l'indirizzo IP in hostname e viceversa.

12.10. Gestione host

La scheda **Host** consente di aggiungere, modificare o rimuovere gli host dal file `/etc/hosts`. Questo contiene gli indirizzi IP e gli hostname relativi.

Quando il vostro sistema cerca di risolvere un hostname verso un indirizzo IP oppure di determinare l'hostname per un indirizzo IP, fa riferimento al file `/etc/hosts`, utilizzando dapprima i name server (se usate la configurazione di default di Red Hat Linux). Se l'indirizzo IP si trova nell'elenco del file `/etc/hosts`, i name server non vengono utilizzati. Se gli indirizzi IP dei computer della vostra rete non si trovano nell'elenco DNS, è consigliabile aggiungerli nel file `/etc/hosts`.

Per aggiungere una voce al file `/etc/hosts`, fate clic su **Aggiungi** nella scheda **Host**, fornite le informazioni richieste, quindi fate clic su **OK**. Selezionate **File => Salva** o premere [Ctrl]-[S]per salvare i cambiamenti sul file `/etc/hosts`. La rete o i servizi di rete non necessitano di essere riavviati dato che la versione attuale viene riferita ogni qualvolta che viene risolto un indirizzo.

Attenzione!

Non rimuovere la voce `localhost`. Anche se il sistema non possiede una connessione di rete o una connessione eseguita costantemente, alcuni programmi necessitano di collegarsi al sistema tramite l'interfaccia loopback del localhost.

Figura 12-16. Configurazione host

Suggerimento

Per modificare l'ordine di consultazione, intervenite sul file `/etc/host.conf`. La riga `order hosts, bind` specifica che `/etc/hosts` ha precedenza sui name server. Modificando la riga in `order bind, hosts`, il sistema sarà configurato per risolvere gli hostname e gli indirizzi IP usando dapprima i name server. Se l'indirizzo IP non può essere risolto mediante i name server, il sistema cerca gli indirizzi IP nel file `/etc/hosts`.

12.11. Attivazione dei dispositivi

I dispositivi di rete possono essere configurati per essere attivi o inattivi al momento dell'avvio. Per esempio, un dispositivo di rete per una connessione modem non é generalmente configurato ad avviarsi al momento dell'inizio; considerando che una connessione Ethernet viene generalmente configurata al momento dell'avvio. Se il vostro dispositivo di rete non é configurato per avviarsi al momento dell'inizio, potete usare il programma **Red Hat Control Network** per attivarlo dopo l'avvio. Per iniziarlo, selezionate **Pulsante menu principale** (sul pannello) **=> Tool del sistema => Network Device Control** o digitare il comando `redhat-control-network`.

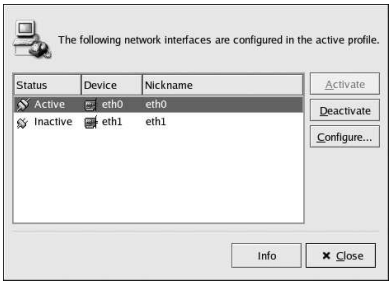

Figura 12-17. Attivazione dei dispositivi

Per attivare un dispositivo, selezionatelo dall'elenco e fate clic sul pulsante **Attiva**. Per fermarlo, procedete allo stesso modo facendo, però clic su **Disattiva**.

Se viene configurato piú di un profilo di rete, essi sono elencati nelle interfaccie e possono essere attivati. Consultate la Sezione 12.12 per maggiori informazioni.

12.12. Lavorare con i profili

È possibile creare molteplici dispositivi logici di rete per ciascun dispositivo hardware fisico. Per esempio, se avete una scheda Ethernet sul vostro sistema (eth0), potete creare vari dispositivi logici di rete associati a eth0 con nickname diversi e opzioni di configurazione diverse.

I dispositivi logici di rete sono diversi dagli alias. I dispositivi logici di rete associati allo stesso dispositivo fisico devono esistere all'interno di profili diversi e non possono essere attivati simultaneamente. Gli alias sono anch'essi associati allo stesso dispositivo hardware fisico, ma possono essere attivati in simultanea. Per conoscere i dettagli relativi alla creazione di alias per i dispositivi, consultate la la Sezione 12.13.

I *profili* possono servire a creare diversi set di configurazione per diverse reti. Un set di configurazione può comprendere dispositivi logici, host e impostazioni DNS. Dopo aver configurato i profili, potete usare **Strumento di amministrazione di rete** per passare da un profilo all'altro.

Per default, esiste un profilo chiamato **Common**. Per creare un nuovo profilo, fate clic sul pulsante **Nuovo** nella cornice **Profile**. Inserite un nome unico per il profilo.

State modificando ora il nuovo profilo come indicato dalla barra dello stato nella parte inferiore della finestra principale.

Fate clic su di un dispositivo giá esistente nell'elenco, e premete il pulsante **Copia** per copiare il dispositivo esistente. Se utilizzate il pulsante **Nuovo**, viene creato un alias di rete e questa procedura non è corretta. Per cambiare le proprietá del dispositivo logico, selezionarlo dall'elenco e fate clic su **Modifica**. Per esempio, il nickname puó essere cambiato in un nome piú descrittivo, come ad esempio **`eth0_office`**, in modo tale da poter essere riconosciuto piú facilmente.

Nell'elenco dei dispositivi, vi è una colonna di caselline etichettata come **Profile**. Per ciascun profilo, potete togliere o mettere una spunta accanto ai vari dispositivi. Solo i dispositivi spuntati vengono inclusi nel profilo attualmente selezionato. Per esempio, se create un dispositivo logico chiamato **`eth0_office`** in un profilo chiamato **`Office`** e volete attivare il dispositivo logico se il profilo é selezionato, non selezionate il dispositivo `eth0` e selezionate il dispositivo `eth0_office`.

Per esempio, la Figura 12-18 mostra un profilo chiamato **Office** con il dispositivo logico **eth0_office**. La configurazione prevede che sia attivata la prima scheda Ethernet tramite DHCP.

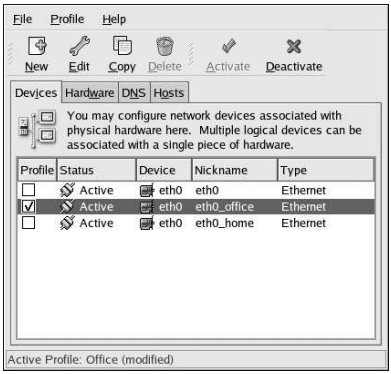

Figura 12-18. Profilo Office

Il profilo **Home** mostrato nella Figura 12-19 attiva il dispositivo logico **eth0_home**, che è associato con `eth0`.

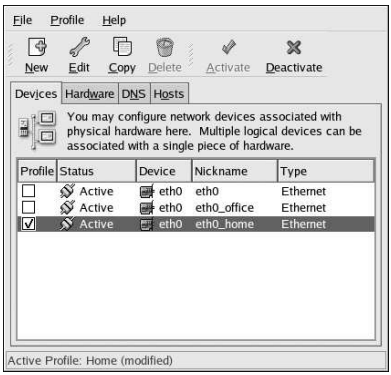

Figura 12-19. Profilo Home

Potete anche configurare `eth0` in modo che si attivi solo nel profilo **Office** e che attivi solo un dispositivo ppp (modem) nel profilo **Home**. Oppure è possibile fare in modo che il profilo **Common** attivi `eth0` e che un profilo **Away** attivi un dispositivo ppp da usare in viaggio.

Un profilo non può essere attivato all'avvio. Solo i dispositivi associati al profilo **Common**, sono impostati in modo da attivarsi all'avvio. Dopo che il sistema è stato attivato, andate su **Menu principale** (sul pannello) => **Tool del sistema** => **Network Device Control** (oppure digitare il comando `redhat-control-network`) per selezionare e attivare un profilo. La sezione del profilo attivato appare solo nell'interfaccia **Network Device Control** se esistono altre interfaccie **Common**.

Alternativamente, eseguire il seguente comando per abilitare un profilo (sostituire *<profilename>* con il nome del profilo):

```
redhat-config-network-cmd --profile <profilename> --activate
```

12.13. Alias per dispositivi

Gli *alias per dispositivi* sono dispositivi virtuali associati allo stesso hardware fisico, ma possono essere attivati simultaneamente in modo da possedere diversi indirizzi IP. Vengono spesso rappresentati con il nome del dispositivo seguito dai due punti e da un numero (per esempio, eth0:1). Sono utili se desiderate avere più di un indirizzo IP per un singolo sistema che abbia una sola scheda di rete.

Dopo aver configurato il dispositivo Ethernet, per esempio `eth0`, per poter usare un indirizzo IP statico (DHCP non funziona con gli alias), andate sulla scheda **Dispositivi** e selezionate **Nuovo**. Selezionate la scheda Ethernet per effettuare una configurazione con un alias, impostare l'indirizzo IP per l'alias, e fate clic su **Applica** per crearlo. Dato che é giá esistente un dispositivo per la scheda Ethernet, quello appena creato é l'alias, esempio `eth0:1`.

Attenzione!

Se state configurando l'alias di un dispositivo Ethernet, sappiate che non potete impostare né il dispositivo né l'alias in modo che utilizzino DHCP. Dovete configurare l'indirizzo IP manualmente.

Figura 12-20 mostra un esempio di un alias per il dispositivo `eth0`. Osservate il dispositivo `eth0:1` — il primo alias per `eth0`. Il secondo alias per `eth0` avrá il nome del dispositivo `eth0:2`, e cosí via. Per modificare le impostazioni relative all'alias del dispositivo (per esempio, il numero di alias o l'eventuale attivazione all'avvio), selezionatelo dall'elenco e fate clic sul pulsante **Modifica**.

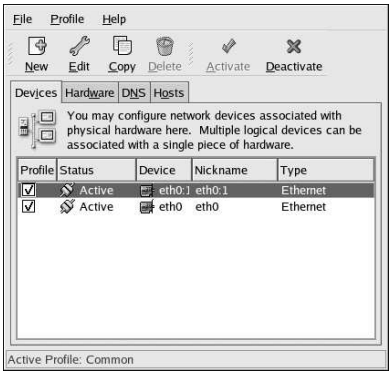

Figura 12-20. Esempio di alias per dispositivi di rete

Selezionate l'alias e fate clic sul pulsante **Activate** per attivarlo. Se avete configurato molteplici profili, scegliete in quali profili includere l'alias.

Per verificare che l'attivazione sia avvenuta correttamente, servitevi del comando `/sbin/ifconfig`. L'output fornito dal comando dovrebbe mostrare il dispositivo e il relativo alias con indirizzo IP diverso:

```
eth0      Link encap:Ethernet  HWaddr 00:A0:CC:60:B7:G4
          inet addr:192.168.100.5  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:161930 errors:1 dropped:0 overruns:0 frame:0
          TX packets:244570 errors:0 dropped:0 overruns:0 carrier:0
          collisions:475 txqueuelen:100
          RX bytes:55075551 (52.5 Mb)  TX bytes:178108895 (169.8 Mb)
```

```
          Interrupt:10 Base address:0x9000

eth0:1    Link encap:Ethernet  HWaddr 00:A0:CC:60:B7:G4
          inet addr:192.168.100.42  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:10 Base address:0x9000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5998 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5998 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1627579 (1.5 Mb)  TX bytes:1627579 (1.5 Mb)
```

Capitolo 13.

Configurazione di base del firewall

Proprio come un muro che cerca di impedire che il fuoco si propaghi ad altre aree di un edificio in fiamme, il firewall del computer cerca di impedire a virus pericolosi e utenti non autorizzati di accedere al vostro computer. Il firewall si colloca tra il computer e la rete e determina i servizi del computer ai quali gli utenti remoti possono accedere tramite la rete. Un firewall configurato correttamente può potenziare la sicurezza del vostro sistema. Si consiglia di configurare un firewall per ogni sistema Red Hat Linux dotato di connessione a Internet.

13.1. Strumento di configurazione del livello di sicurezza

Nella schermata di **Configurazione del firewall** dell'installazione di Red Hat Linux, avete la possibilità di scegliere il livello di sicurezza (alto, medio, basso), nonché di abilitare dispositivi specifici, servizi in entrata e porte.

A installazione avvenuta, potete cambiare il livello di sicurezza del vostro sistema utilizzando **Strumento di configurazione del livello di sicurezza**. Se preferite un'applicazione basata su procedure guidate, consultate la Sezione 13.2.

Per avviare l'applicazione, selezionate **Pulsante del menu principale** (sul Pannello) **=> Impostazioni del sistema => Livello di sicurezza** o digitate il comando `redhat-config-securitylevel` al prompt della shell, per esempio in un terminale XTerm o GNOME.

Figura 13-1. Strumento di configurazione del livello di sicurezza

Selezionate il livello di sicurezza desiderato dal menu a tendina.

Alto

Se scegliete **Alto**, il vostro sistema non accetterà le connessioni, diverse dalle impostazioni predefinite, che non siano state definite in modo esplicito. Per default, sono consentite solo le seguenti connessioni:

- Risposte DNS
- DHCP — per fare in modo che le interfacce di rete che utilizzano il protocollo DHCP possano essere configurate in modo appropriato

Se scegliete **Alto**, il vostro firewall non consentirà quanto segue:

- FTP in modalità attiva (FTP in modalità passiva, utilizzato per default nella maggior parte dei client, dovrebbe comunque funzionare
- Trasferimenti di file IRC DCC
- RealAudio™
- Client del sistema X Window remoto

La scelta più sicura è la connessione del sistema a Internet, quando non si stabilisce di installare un server. Se sono necessari servizi aggiuntivi, potete scegliere **Personalizza** per consentire servizi specifici attraverso il firewall.

Nota Bene

Se selezionate un firewall medio o alto da configurare durante l'installazione, i metodi di autenticazione di rete (NIS e LDAP) non funzioneranno.

Medio

Se scegliete **Medio**, il vostro firewall non consentirà ai computer remoti di avere l'accesso a determinate risorse del vostro sistema. Per default, non è consentito l'accesso alle seguenti risorse:

- Porte inferiori alla 1023 — le porte standard riservate, utilizzate dalla maggior parte di servizi di sistema, come **FTP**, **SSH**, **telnet**, **HTTP** e **NIS**.
- La porta del server NFS (2049) — NFS è disabilitato per i server remoti e i client locali.
- La visualizzazione del sistema X Window locale per i client X remoti.
- La porta del server dei font X (per default **xfs** non ascolta la rete ed è disabilitato nel server dei font).

Se desiderate consentire l'accesso a risorse come **RealAudio™** pur continuando a bloccare l'accesso a servizi di sistema comuni, scegliete **Medio**. Selezionate **Personalizza** per consentire l'accesso a servizi specifici attraverso il firewall.

Nota Bene

Se selezionate un firewall medio o alto da configurare durante l'installazione, i metodi di autenticazione di rete (NIS e LDAP) non funzioneranno.

Nessun firewall

Questa opzione fornisce l'accesso completo al vostro sistema e non esegue alcun controllo sulla sicurezza. Tale controllo disabilita l'accesso a determinate risorse. L'opzione deve essere selezionata solo se è installata una rete fidata (non Internet) o se pianificate di eseguire la configurazione di più firewall in seguito.

Scegliete **Personalizza** per aggiungere dispositivi fidati o consentire altri servizi in ingresso.

Periferiche fidate

La selezione di una delle **Periferiche fidate** consente l'accesso al vostro sistema di tutto il traffico proveniente da tale dispositivo. Non fa parte delle regole del firewall. Se, per esempio, è installata una rete locale, ma la connessione a Internet avviene tramite un protocollo PPP, potete selezionare **eth0** e tutto il traffico proveniente dalla rete locale sarà consentito. La selezione di **eth0** come dispositivo fidato indica che è consentito tutto il traffico attraverso le reti Ethernet, purché l'interfaccia ppp0 sia ancora dotata di firewall. Se desiderate limitare il traffico relativo a un'interfaccia, lasciate l'opzione deselezionata.

Non è consigliabile rendere **Periferiche fidate** tutti i dispositivi connessi alle reti pubbliche, come Internet.

Permetti in ingresso

L'abilitazione di queste opzioni consente ai servizi specificati di passare attraverso il firewall. Durante l'installazione di una workstation la maggior parte di questi servizi *non* è installata nel sistema.

DHCP

Se consentite le query e le risposte DHCP in entrata, fate in modo che tutte le interfacce di rete che utilizzano il protocollo DHCP possano determinare il proprio indirizzo IP. DHCP è in genere abilitato. In caso contrario, il vostro computer non può più ottenere un indirizzo IP.

SSH

*S*ecure *SH*ell (SSH) è una serie di strumenti per l'accesso e l'esecuzione di comandi in un computer remoto. Se stabilite di utilizzare gli strumenti SSH per accedere al vostro computer attraverso un firewall, abilitate questa opzione. È necessario che sia installato il pacchetto `openssh-server` per poter accedere al computer da remoto mediante gli strumenti SSH.

Telnet

Telnet è un protocollo per l'accesso a computer remoti. Le comunicazioni Telnet non sono criptate e non forniscono alcuna sicurezza. L'abilitazione dell'accesso a Telnet in entrata non è consigliato. Se desiderate consentire l'accesso Telnet in entrata, sarà necessario installare il pacchetto `telnet-server`.

WWW (HTTP)

Il protocollo HTTP è utilizzato da Apache e da altri server Web per le pagine Web. Se pensate di rendere il vostro server Web disponibile pubblicamente, abilitate questa opzione, che non è necessaria per visualizzare le pagine localmente o per sviluppare le pagine Web. Sarà necessario installare il pacchetto `apache` perché sia utile alle pagine Web.

La selezione di **WWW (HTTP)** non aprirà una porta per HTTPS. Per abilitare HTTPS, specificatelo nel campo **Altre porte**.

Mail (SMTP)

Se desiderate consentire la ricezione della posta in entrata attraverso il vostro firewall, per fare in modo che gli host remoti possano connettersi direttamente al computer per inviare la posta, abilitate questa opzione. Non è necessario abilitarla se la posta vi arriva dal server del vostro provider di servizi Internet che utilizza POP3 o IMAP oppure se utilizzate uno strumento come **fetchmail**. Un server SMTP non configurato in modo appropriato può fare in modo che i computer remoti utilizzino il vostro server per inviare spam.

FTP

Il protocollo FTP è utilizzato per trasferire i file tra i computer di una rete. Se stabilite di rendere il vostro server FTP disponibile pubblicamente, abilitate questa opzione. È necessario installare il pacchetto `wu-ftpd` e possibilmente `anonftp` perché questa opzione sia utile.

Cliccare **OK** per attivare il firewall. Dopo aver cliccato **OK**, le opzioni selezionate vengono trasmesse sui comandi `iptables` e scritte sul file `/etc/sysconfig/iptables`. Il servizio `iptables` viene avviato in modo tale che il firewall viene attivato immediatamente dopo aver salvato le opzioni selezionate.

Attenzione

Se avete configurato un firewall o qualsiasi altre regole inerenti il firewall, nel file `/etc/sysconfig/iptables`, il suddetto file sará cancellato, se viene selezionato **No Firewall** e se cliccate **OK** per salvare i cambiamenti.

Le opzioni selezionate sono anche scritte sul file `/etc/sysconfig/redhat-config-securitylevel` cosí l'impostazione puó essere ripristinata la prossima volta che l'applicazione viene avviata. Non modificate manualmente questo file.

Per attivare il servizio `iptables` ad un avvio automatico al momento dell'avvio, consultate la Sezione 13.3 per maggiori informazioni.

13.2. GNOME Lokkit

GNOME Lokkit vi consente di configurare le impostazioni di un firewall per l'utente medio creando delle regole di base `iptables` per la rete. Anziché scrivere subito le regole, questo programma vi pone una serie di domande relative al modo in cui utilizzate il vostro sistema e scrive per voi le regole nel file `/etc/sysconfig/iptables`.

Si consiglia di non utilizzare **GNOME Lokkit** per generare regole del firewall complesse. Questo programma è infatti ideato per l'utente medio che desidera proteggere il proprio sistema durante una connessione a Internet via modem, cavo o DSL. Per configurare delle regole del firewall specifiche, consultate il capitolo *Creare firewall con `iptables`* nella *Red Hat Linux Reference Guide*.

Per disabilitare dei servizi specifici e rifiutare determinati host e utenti, consultate il Capitolo 14.

Per avviare la versione grafica di **GNOME Lokkit**, selezionare **Pulsante menu principale => Strumenti del sistema => piú strumenti del sistema => Lokkit**, o inserire il comando `gnome-lokkit` al prompt della shell, come un utente root. Se non avete installato il sistema X di Window o se preferite un programma di testo, inserire il comando `lokkit` al prompt della shell, per avviare la versione in modalitá di testo.

13.2.1. Configurazione di base

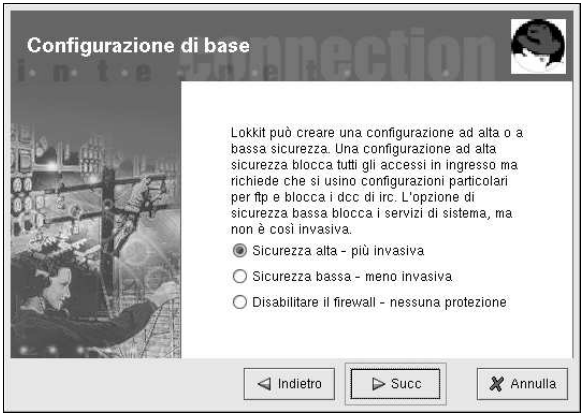

Figura 13-2. Configurazione di base

Dopo aver avviato il programma, selezionate il livello di sicurezza idoneo per il vostro sistema:

- **Sicurezza alta** — questa opzione disabilita quasi tutte le connessioni di rete salvo le risposte del DNS e il protocollo DHCP affinché le interfacce di rete possano essere attivate. IRC, ICQ e gli altri servizi di messaggi immediati, nonché RealAudio™ non funzioneranno senza un proxy.
- **Sicurezza bassa** — questa opzione non abilita le connessioni remote al sistema, comprese le connessioni NFS e le sessioni remote del sistema X Window. Tutti i servizi eseguiti sotto la porta 1023 non accettano connessioni (tra cui FTP, SSH, Telnet e HTTP).
- **Disabilitare il firewall** — questa opzione non genera alcuna regola di sicurezza. Si consiglia di abilitarla solo se il sistema si trova in una rete fidata (non Internet), se possedete un sistema di firewall più avanzato o se preferite scrivere delle regole personalizzate. Se selezionate questa opzione e fate clic su **Succ**, proseguite con la Sezione 13.3. Il livello di sicurezza del sistema non verrà modificato.

13.2.2. Host locali

Se nel sistema sono presenti dispositivi Ethernet, la pagina **Host locali** vi consente di impostare se le regole del firewall devono essere applicate alle richieste di connessione inviate a ogni dispositivo. Se il dispositivo connette il sistema a una LAN utilizzando un firewall e non si connette direttamente a Internet, selezionate **Sì**. Se la scheda Ethernet connette il sistema a un modem DSL o via cavo, si consiglia di selezionare **No**.

Figura 13-3. Host locali

13.2.3. DHCP

Se utilizzate un protocollo DHCP per attivare qualsiasi interfaccia Ethernet nel sistema, rispondete **Sì** alla domanda DHCP. Se impostate 'No', non riuscirete a stabilire una connessione usando l'interfaccia Ethernet. Molti provider Internet (via cavo o DSL) richiedono l'uso del protocollo DHCP per stabilire una connessione a Internet.

Figura 13-4. DHCP

13.2.4. Configurazione dei servizi

GNOME Lokkit vi consente, inoltre, di attivare o disattivare servizi comuni. Se rispondete **Sì** ai servizi di configurazione, vi viene richiesto di abilitare o disabilitare i servizi seguenti:

- **Server Web** — selezionate questa opzione se desiderate connettervi a un server Web (come Apache) in esecuzione sul vostro sistema. Non occorre selezionare questa opzione se desiderate visualizzare delle pagine Web sul vostro sistema o su altri server in rete.
- **Posta in arrivo** — selezionate questa opzione per far accettare al vostro sistema la posta in arrivo. Se invece ricevete la posta tramite IMAP, POP3 o fetchmail, non è necessario abilitarla.
- **Secure Shell** — Secure Shell o SSH è una raccolta di strumenti per collegarsi ed eseguire comandi su una macchina remota tramite una connessione criptata. Attivate questa opzione per accedere alla macchina in modo remoto tramite ssh.
- **Telnet** — Telnet vi consente di collegarvi al vostro computer in modo remoto; tuttavia questo metodo non è sicuro, poiché invia le informazioni (comprese le password) in chiaro nella rete. Si consiglia di utilizzare SSH per connessioni remote alla propria macchina. Se vi occorre un accesso telnet al vostro sistema, selezionate questa opzione.

Per disabilitare altri servizi che non vi occorrono, potete utilizzare **Serviceconf** (vedere la Sezione 14.3) o **ntsysv** (vedere la Sezione 14.4) o `chkconfig` (vedere la Sezione 14.5).

13.2.5. Attivazione del firewall

Selezionando **Fine**, le regole del firewall verranno scritte nel file `/etc/sysconfig/iptables` e il firewall si attiverà all'avvio del servizio `iptables`.

Attenzione

Se avete configurato un firewall o qualsiasi altre regole inerenti il firewall, nel file `/etc/sysconfig/iptables`, il suddetto file sará cancellato, se viene selezionato **Disabilita Firewall** e se cliccate **Fine** per salvare i cambiamenti.

Si consiglia vivamente di eseguire **GNOME Lokkit** dal proprio computer e non da una sessione X remota. Se disattivate l'accesso remoto al vostro sistema, non sarete più in grado di accedervi o di disabilitare le regole del firewall.

Se non desiderate scrivere le regole del firewall, fate clic sul pulsante **Annulla**.

13.2.5.1. Trasmissione di posta

Il sistema di trasmissione di posta consente ad altri sistemi di inviare posta elettronica. Se il vostro sistema dispone del sistema di trasmissione di posta, chiunque potrebbe utilizzarlo per inviare spam dalla vostra macchina.

Se abilitate i servizi di posta, dopo aver selezionato **Termina** nella pagina **Attivazione del firewall**, vi viene richiesto di controllare il sistema di trasmissione di posta. Se selezionate **Sì**, **GNOME Lokkit** cerca di connettersi al sito Web *Mail Abuse Prevention System* all'indirizzo http://www.mail-abuse.org/ e di eseguire un programma di verifica, al termine del quale vengono visualizzati i risultati. Se il vostro computer dispone di tale sistema, vi consigliamo di configurare Sendmail per bloccarlo.

13.3. Attivazione del servizio `iptables`

Le regole del firewall sono attive solo se il servizio `iptables` è in esecuzione. Per attivare manualmente il servizio, usate il comando:

```
/sbin/service iptables restart
```

Per assicurarvi che venga eseguito all'avvio del sistema, digitate il comando:

```
/sbin/chkconfig --level 345 iptables on
```

Il servizio `ipchains` non puó essere eseguito con il servizio `iptables`. Per assicurarsi che il servizio `ipchains` é disabilitato, eseguire il comando:

```
/sbin/chkconfig --level 345 ipchains off
```

Il **Strumento di configurazione dei servizi** puó essere usato per configurare i servizi `iptables` e `ipchains`. Consultare la Sezione 14.3 per maggiori informazioni.

redhat.

Capitolo 14.

Controllo dell'accesso ai servizi

Garantire la sicurezza del vostro sistema Red Hat Linux è estremamente importante. Una gestione consapevole dell'accesso ai servizi di sistema è il metodo migliore per assicurarsi tale punto. Il sistema potrebbe avere la necessità di fornire accesso aperto a servizi specifici (per esempio, all'`httpd` per un server Web). Tuttavia, se non avete l'esigenza di disporre di un servizio, si consiglia di disattivarlo e; ciò ridurrà la vostra esposizione a possibili bug.

Vi sono diversi metodi per la gestione dell'accesso ai servizi di sistema. Dovete decidere quale preferite utilizzare in base al servizio, alla configurazione del sistema e alla vostra conoscenza di Linux.

Il modo più semplice per negare l'accesso a un servizio è, chiaramente, quello di disattivarlo. I servizi gestiti mediante `xinetd` (che saranno affrontati in dettaglio successivamente in questa sezione) e quelli della gerarchia `/etc/rc.d` possono essere configurati per essere avviati o arrestati utilizzando tre diverse applicazioni:

- **Strumento di configurazione dei servizi** — un'applicazione grafica che visualizza la descrizione di ciascun servizio, indica se questo è stato eseguito durante l'avvio (per i runlevel 3, 4 e 5) e vi consente di avviare, arrestare e riavviare ogni singolo servizio.
- **ntsysv** — un'applicazione basata su testo che vi permette di configurare i servizi lanciati all'avvio per ciascun runlevel. Le modifiche apportate non diventano immediatamente effettive. Questo programma non vi consente di avviare, arrestare o riavviare tali servizi.
- `chkconfig` — una utility da linea di comando che vi permette di attivare o disattivare i servizi per i diversi runlevel. Le modifiche apportate non diventano immediatamente effettive per i servizi non xinetd. Questa utility non vi consente di avviare, arrestare o riavviare i servizi.

Scoprirete che questi tool sono più facili da utilizzare rispetto ad altri — che richiedono la modifica manuale di numerosi link simbolici nelle directory sotto `/etc/rc.d` o la modifica dei file di configurazione `xinetd` contenuti in `/etc/xinetd.d`.

Un'alternativa per la gestione dell'accesso ai servizi di sistema è l'uso di `iptables` per configurare un firewall IP. Se non siete utenti esperti di Linux, considerate che `iptables` potrebbe non essere la soluzione più adatta per voi. Impostare `iptables` può essere complicato ed è meglio lasciare questo compito ad amministratori di sistema UNIX/Linux esperti.

D'altro canto, `iptables` offre il vantaggio della flessibilità. Se avete, per esempio, l'esigenza di una soluzione personalizzata che consenta l'accesso di host specifici a servizi altrettanto specifici, `iptables` fa al caso vostro. Consultate la *Red Hat Linux Reference Guide* per ulteriori informazioni su `iptables`.

Se, invece, state cercando una utility per impostare le regole generali d'accesso per il vostro personal computer, e/o se siete nuovi utenti Linux, potete provare la utility **Strumento di configurazione del livello di sicurezza**. (`redhat-config-securitylevel`), che consente di selezionare il livello di sicurezza per il vostro sistema, in modo simile alla schermata **Configurazione del firewall** del programma di installazione di Red Hat Linux. Potete anche usare **GNOME Lokkit** una applicazione GUI che vi porrà delle domande relative all'utilizzo della vostra macchina. Basandosi sulle risposte fornite, configurerà per voi un semplice firewall. Fate riferimento al Capitolo 13 per maggiori informazioni. Se avete bisogno di maggiori informazioni su specifiche regole sui firewall, consultate il capitolo `iptables` in *Red Hat Linux Reference Guide*.

14.1. Runlevel

Prima di configurare l'accesso ai servizi, è necessario comprendere i runlevel di Linux. Un runlevel è uno stato, o *modalità*, definita dai servizi elencati nella directory `/etc/rc.d/rc<x>.d`, dove `<x>` indica il numero del runlevel.

Red Hat Linux utilizza i seguenti runlevel:

- 0 — arresto
- 1 — modalità utente singolo
- 2 — non utilizzato (definibile dall'utente)
- 3 — modalità multi-utente completa
- 4 — non utilizzato (definibile dall'utente)
- 5 — modalità multi-utente completa (con una finestra di registrazione basata su X)
- 6 — riavvio

Se avete configurato il sistema X Window durante il processo d'installazione di Red Hat Linux, avrete facoltà di scegliere una finestra di registrazione grafica o testuale. In quest'ultimo caso, state operando nel runlevel 3. Nel caso in cui scegliate una schermata grafica per il login, invece, opererete nel runlevel 5.

Il runlevel di default può essere cambiato modificando il file `/etc/inittab`, il quale presenta, nella parte iniziale, una riga del file simile alla seguente:

```
id:5:initdefault:
```

Cambiate il numero di questa linea in base al runlevel desiderato. Tale modifica sarà effettiva solo dopo aver riavviato il sistema.

Per modificare il runlevel con effetto immediato, usate il comando `telinit` seguito dal numero di runlevel. Per eseguire questo comando, dovete collegarvi come root.

14.2. Wrapper TCP

Molti amministratori di sistemi UNIX sono ormai abituati a utilizzare i wrapper TCP per gestire l'accesso a certi servizi di rete. Infatti, qualsiasi servizio di rete gestito da `xinetd` (come del resto tutti i programmi dotati di supporto integrato per libwrap) è in grado di utilizzare i wrapper TCP per gestire l'accesso. `xinetd` utilizza i file `/etc/hosts.allow` e `/etc/hosts.deny` per configurare l'accesso ai servizi di sistema. Come è intuibile dal nome, `hosts.allow` contiene un elenco di regole per consentire l'accesso dei client ai servizi di rete controllati da `xinetd`, mentre `hosts.deny` contiene le regole per negarlo. Il file `hosts.allow` ha la precedenza su `hosts.deny`. I permessi per garantire o negare l'accesso possono basarsi su indirizzi IP individuali (o nomi di host) oppure su una tipologia di client. Per dettagli, consultate le relative pagine man di `hosts_access` nella *Red Hat Linux Reference Guide* .

14.2.1. `xinetd`

Per controllare l'accesso ai servizi Internet, utilizzate `xinetd`, un valido sostituto di `inetd`. Il demone `xinetd` preserva le risorse di sistema, assicura il controllo sull'accesso e la registrazione e può essere utilizzato per avviare i server con scopi particolari. `xinetd` può anche essere usato per disporre dell'accesso di host particolari, per consentire l'accesso a un servizio in un momento specifico, per negarlo a host specifici, per limitare la frequenza di connessioni in entrata e/o il carico determinato dalle connessioni stesse e altro ancora.

`xinetd` è in costante esecuzione e si pone in ascolto su tutte le porte per i servizi che controlla. Quando arriva una richiesta di connessione per uno dei servizi che gestisce, `xinetd` avvia il server appropriato per quel servizio.

Il file di configurazione per `xinetd` è `/etc/xinetd.conf`, ma, esaminando il file, noterete che contiene solo un numero limitato di valori di default e un'istruzione per inserire la directory `/etc/xinetd.d`. Per abilitare o disabilitare un servizio `xinetd`, modificate il file di configurazione nella directory `/etc/xinetd.d`. Se l'attributo `disable` è impostato su **`yes`**, allora il servizio non è attivato. Se, invece, `disable` è impostato su **`no`**, il servizio è attivato. Potete modificate uno qualsiasi dei file di configurazione `xinetd`, o ne modificate lo stato di attivazione mediante **Strumento di configurazione dei servizi**, **ntsysv**, oppure `chkconfig`, dovrete riavviare `xinetd` con il comando `service xinetd restart`, prima che i cambiamenti diventino effettivi. Usate `ls /etc/xinetd.d` per ottenere un elenco dei servizi di rete controllati dall'elenco dei contenuti `xinetd` della directory `/etc/xinetd.d`.

14.3. Strumento di configurazione dei servizi

Strumento di configurazione dei servizi è un'applicazione grafica sviluppata da Red Hat per impostare i servizi SysV contenuti in `/etc/rc.d/init.d` che devono essere eseguiti durante l'avvio del sistema (per i runlevel 3, 4 e 5) e per stabilire quali servizi `xinetd` devono essere attivati. Quest'applicazione vi consente, inoltre, di avviare, arrestare e riavviare i servizi SysV e di riavviare `xinetd`.

Per avviare **Strumento di configurazione dei servizi** dal desktop, selezionate **Pulsante del menu principale** (sul Pannello) => **Impostazioni del sistema** => **Servizi** oppure digitate il comando `redhat-config-services` al prompt della shell (per esempio in un terminale **XTerm** o **GNOME**).

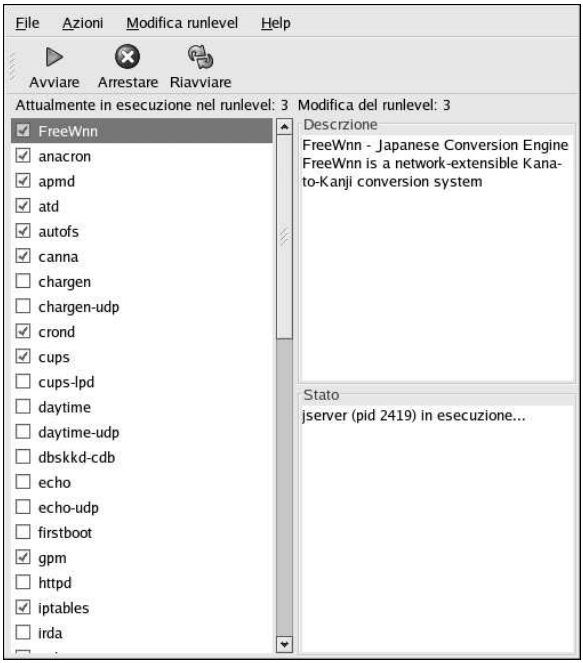

Figura 14-1. Strumento di configurazione dei servizi

Strumento di configurazione dei servizi visualizza il runlevel corrente e il runlevel sottoposto a modifica. Per modificare un runlevel differente, selezionare **Modifica runlevel** dal menù a tendina, quindi il runlevel 3, 4 o 5. Consultate la Sezione 14.1 per una descrizione dei runlevel.

Strumento di configurazione dei servizi elenca i servizi forniti da `/etc/rc.d/init.d` e quelli controllati da `xinetd`. Fate clic su un servizio per visualizzarne una breve descrizione nella parte inferiore della finestra.

Per avviare, arrestare o riavviare un servizio in modo immediato, selezionate il servizio e l'azione del caso dal menu a tendina **Azioni**. Avete anche la facoltà di selezionare il servizio e fare clic sui tasti di avvio, arresto o riavvio sulla barra degli strumenti.

Se selezionate un servizio `xinetd` come telnet, i tasti **Avviare**, **Arrestare**, e **Riavviare** non saranno disponibili. Modificando, invece, il valore **Fare partire all'avvio** di un servizio `xinetd`, dovrete fare clic sul pulsante **Salvare modifiche** per riavviare `xinetd` e disattivare/attivare i servizi `xinetd` modificati.

Per attivare un servizio durante l'avvio per il runlevel correntemente prescelto, selezionate la casella di controllo relativa al nome del servizio sotto la colonna **Fare partire all'avvio**. Dopo la configurazione del runlevel, applicate le modifiche selezionando **File => Salvare modifiche** dal menu a tendina oppure facendo clic sul pulsante **Salvare modifiche**.

Avvertenza

Quando salvate le modifiche apportate ai servizi `xinetd`, viene riavviato `xinetd`. Per gli altri servizi, viene invece riconfigurato il runlevel, ma le modifiche non sono effettive all'istante.

Se selezionate o deselezionate il valore **Fare partire all'avvio** per un servizio di `/etc/rc.d/init.d`, si attiverà il pulsante **Salvare modifiche**. Fate clic sul pulsante per riconfigurare il runlevel correntemente selezionato. Le modifiche non saranno applicate immediatamente al sistema. Supponete, per esempio, di configurare il runlevel 3. Se modificate il valore **Fare partire all'avvio** per il servizio `anacron`, deselezionandolo e facendo clic sul pulsante **Salvare modifiche**, la configurazione del runlevel 3 cambia in modo tale che `anacron` non venga lanciato all'avvio. Tuttavia, il runlevel 3 non è nuovamente inizializzato, e `anacron` resta in esecuzione. A questo punto, selezionate una delle seguenti opzioni:

1. Arresta il servizio `anacron` — interrompete il servizio selezionandolo dall'elenco e facendo clic sul tasto **Arresta servizio selezionato**. Verrà visualizzato un messaggio che vi informa che l'operazione di arresto ha avuto successo.
2. Inizializza nuovamente il runlevel — inizializzate di nuovo il runlevel passando al prompt della shell (come un terminale **XTerm** oppure **GNOME**) e digitando il comando `telinit 3` (dove 3 è il numero del runlevel). Si raccomanda di utilizzare quest'opzione qualora modifichiate il valore **Fare partire all'avvio** di più servizi e desideriate attivare immediatamente i cambiamenti apportati.
3. Rimanda — non è necessario arrestare il servizio `anacron`. È possibile attendere finché il sistema non viene riavviato perché il servizio si arresti. All'avvio successivo del sistema, il runlevel sarà inizializzato senza l'esecuzione del servizio `anacron`.

14.4. ntsysv

La utility **ntsysv** fornisce un'interfaccia dall'uso semplice per attivare o disattivare i servizi. Potete utilizzare **ntsysv** per attivare o disattivare i servizi gestiti mediante `xinetd`. **ntsysv** vi consente anche di avviare o arrestare un servizio della gerarchia `/etc/rc.d`. In questo caso, il comando `ntsysv` (privo di opzioni) viene utilizzato per configurare il runlevel corrente. Se desiderate configurare un runlevel diverso, potete usare qualcosa di simile a `ntsysv --levels 016`. (Nell'esempio fornito, saranno impostati i servizi per i runlevel 0, 1 e 6).

L'interfaccia **ntsysv** funziona come il programma di installazione di modalità testo. Usate le frecce direzionali per spostarvi all'interno dell'elenco. La barra spaziatrice seleziona/deseleziona i servizi e vi consente anche di "premere" i pulsanti **Ok** e **Annulla**. Usate il tasto [Tab] per spostarvi dall'elenco dei servizi e i pulsanti **Ok** e **Annulla**. Il carattere jolly ***** indica che il servizio cui si riferisce è attivato. Il tasto [F1] visualizzerà una breve descrizione di ciascun servizio.

Avvertenza

Le modifiche apportate usando **ntsysv** non sono immediatamente effettive; per renderle tali, arrestate o avviate il singolo servizio con il comando `service` *`demone`* `stop`. Nel precedente esempio sostituite *`demone`* con il nome del servizio che desiderate arrestare, per esempio, `httpd`. Sostituite `stop` con `start` oppure `restart` per avviare o riavviare il servizio. Per lanciare o arrestare un servizio gestito da `xinetd`, utilizzate il comando `service xinetd restart`.

14.5. `chkconfig`

Anche il comando `chkconfig` consente di attivare e disattivare i servizi. Se usate il comando `chkconfig --list`, comparirà un elenco dei servizi di sistema che visualizzerà il loro stato di avvio (`on`) oppure di arresto (`off`) nei runlevel da 0 a 6 (alla fine dell'elenco vi è una sezione dedicata ai servizi gestiti da `xinetd`).

Se utilizzate `chkconfig --list` per una query al servizio gestito mediante `xinetd`, sarà possibile vedere se il servizio `xinetd` è attivato (on) o disattivato (off). I seguenti comandi mostrano, per esempio, che `finger` è attivato in un servizio xinetd:

```
finger          on
```

Come mostra l'esempio, se `xinetd` è in esecuzione, `finger` è attivato.

Se utilizzate `chkconfig --list` per una query in un servizio in `/etc/rc.d`, visualizzerete le impostazioni di quel servizio per ciascun runlevel, come mostra l'esempio:

```
anacron         0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Cosa ancora più importante, `chkconfig` può essere utilizzato per impostare un servizio in modo che venga o meno avviato su un runlevel specifico. Per esempio, se voleste disattivare `nscd` sui runlevel 3, 4 e 5, dovreste usare il comando:

```
chkconfig --level 345 nscd off
```

Consultate la pagina man `chkconfig` per ulteriori informazioni sul suo utilizzo.

Avvertenza

Le modifiche apportate mediante `chkconfig` hanno effetto immediato sui servizi gestiti con `xinetd`. Per esempio, se `xinetd` è in esecuzione, `finger` è disattivato e il comando `chkconfig finger on` viene eseguito, `finger` si attiva automaticamente senza dover riavviare manualmente `xinetd`. Dopo l'utilizzo di `chkconfig`, le modifiche agli altri servizi non hanno effetto immediato. È necessario arrestare oppure avviare il singolo servizio con il comando `service` *`demone`* `stop`. Nell'esempio precedente sostituite *`demone`* con il nome del servizio che desiderate sospendere, per esempio `httpd`. Sostituite `stop` con `start` oppure `restart` per lanciare o riavviare il servizio.

14.6. Risorse aggiuntive

Per maggiori informazioni su `xinetd`, fate riferimento alle seguenti risorse.

14.6.1. Documentazione installata

- `man ntsysv` — La pagina man **ntsysv**.
- `man chkconfig` — La pagina man `chkconfig`.
- `man xinetd` — La pagina man `xinetd`.
- `man xinetd.conf` — La pagina man per il file di configurazione `xinetd.conf`.
- `man 5 hosts_access` — La pagina man per il formato di file di controllo di accesso degli host (sezione 5 delle pagine man).

14.6.2. Siti Web utili

- http://www.xinetd.org — La pagina Web di `xinetd`. Contiene un elenco dettagliato delle caratteristiche e dei file di configurazione di esempio.

Capitolo 15.

OpenSSH

OpenSSH è una implementazione gratuita e open source del protocollo SSH (*S*ecure *SH*ell). Sostituisce i comandi `telnet`, `ftp`, `rlogin`, `rsh` e `rcp` con tool di connettività sicuri e criptati per il traffico di rete. OpenSSH supporta le versioni 1.3, 1.5 e 2 del protocollo SSH. Dalla versione 2.9 di OpenSSH, il protocollo predefinito è la versione 2, che utilizza, per default, chiavi RSA.

15.1. Perché utilizzare OpenSSH?

Utilizzando i tool OpenSSH, si migliora notevolmente la sicurezza del computer. Tutte le comunicazioni generate con i tool OpenSSH, incluse le password, sono cifrate. I comandi `Telnet` e `ftp` utilizzano le password "in chiaro" e inviano informazioni non cifrate. Perciò le informazioni possono essere intercettate, le password registrate e il sistema potrebbe essere compromesso da una persona che senza autorizzazione accede al sistema usando una delle password intercettate. Per limitare i problemi di sicurezza, si consiglia l'uso delle utility OpenSSH.

Un'altra ragione per utilizzare il sistema OpenSSH è che invia automaticamente al computer client la variabile `DISPLAY`. In altre parole, se sul vostro computer locale eseguite il sistema X Window e vi collegate a un computer remoto usando il comando `ssh`, quando eseguite un programma sul computer remoto che richiede X Window, questo viene visualizzato direttamente sulla vostra macchina locale. È utile se preferite usare strumenti grafici ma non avete l'accesso fisico al server.

15.2. Configurazione di un server OpenSSH

Prima di eseguire un server OpenSSH, è necessario verificare che siano installati i pacchetti RPM appropriati. Il pacchetto `openssh-server` è richiesto e si basa sul pacchetto `openssh`.

Il demone OpenSSH utilizza il file di configurazione `/etc/ssh/sshd_config`. Il file di configurazione di default installato con Red Hat Linux è adatto alla maggior parte degli scopi. Se volete configurare il demone in modo diverso dalla configurazione di default di `sshd_config`, consultate la pagina man del comando `sshd` per ottenere un elenco delle parole chiave che è possibile includere nel file di configurazione.

Per avviare il servizio OpenSSH, digitate il comando `/sbin/service sshd start`. Per interrompere l'esecuzione del server OpenSSH, usate il comando `/sbin/service sshd stop`. Se volete che il demone venga attivato automaticamente all'avvio, consultate il Capitolo 14 per informazioni su come gestire i servizi.

Se reinstallate un sistema Red Hat Linux e i client relativi prima della reinstallazione con qualsiasi tool OpenSSH, al termine della reinstallazione gli utenti dei client visualizzeranno il seguente messaggio:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
```

Il sistema reinstallato crea una nuova serie di chiavi di identificazione per il sistema. Da questo deriva l'avviso relativo alla modifica delle chiavi dell'host RSA. Se desiderate conservare le chiavi host generate per il sistema, eseguite un backup dei file `/etc/ssh/ssh_host*key*` e ripristinali dopo la reinstallazione. Questo processo conserva l'identità del sistema e quando i client tenteranno di connettersi dopo la reinstallazione, non riceveranno il messaggio di avviso.

15.3. Configurazione del client OpenSSH

Per collegarvi a un server OpenSSH tramite un computer client, è necessario che siano installati i pacchetti `openssh-clients` e `openssh`.

15.3.1. Uso del comando `ssh`

Il comando `ssh` può essere considerato una valida alternativa ai comandi `rlogin`, `rsh` e `telnet`. Questo comando permette di collegarsi e di eseguire comandi su una macchina remota.

L'uso del comando `ssh` per collegarsi a un computer remoto è simile al comando `telnet`. Per collegarvi a un computer remoto penguin.example.net, digitate il comando seguente al prompt della shell:

```
ssh penguin.example.net
```

La prima volta che vi collegate a una macchina remota tramite il comando `ssh`, compare un messaggio simile al seguente:

```
The authenticity of host 'penguin.example.net' can't be established.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

Digitate **`yes`** per continuare. In questo modo aggiungete il server all'elenco degli host:

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list of known hosts.
```

Successivamente compare il prompt per l'inserimento della password di accesso al server remoto. Una volta inserita la password, compare il prompt della shell. Se non specificate un nome utente, viene passato alla macchina remota il nome utente usato per l'accesso alla macchina client locale. Per specificare un nome utente differente, usate il seguente comando:

```
ssh nomeutente@penguin.example.net
```

Potete anche usare la sintassi `ssh -l nomeutente penguin.example.net`.

Il comando `ssh` può essere utilizzato per eseguire direttamente un comando su una macchina remota senza collegarsi al prompt della shell. La sintassi è `ssh nomehost comando`. Per esempio, se volete eseguire il comando `ls /usr/share/doc` sulla macchina remota penguin.example.net, digitate il seguente comando al prompt della shell:

```
ssh penguin.example.net ls /usr/share/doc
```

Dopo aver inserito la password corretta, viene visualizzato il contenuto della directory `/usr/share/doc`. Quindi ritornerete al prompt della shell.

15.3.2. Uso del comando `scp`

Il comando `scp` viene usato per trasferire file tra computer tramite una connessione sicura e criptata. E` simile al comando `rcp`.

La sintassi generale per trasferire file locali su un sistema remoto è la seguente:

```
scp filelocale nomeutente@nomehost:/nomenuovofile
```

Il file *`filelocale`* specifica la sorgente e *`nomeutente@nomehost:/nomenuovofile`* specifica la destinazione.

Per trasferire il file locale `shadowman` su penguin.example.net tramite il proprio account, digitate il comando seguente al prompt della shell (sostituendo *`nomeutente`* con il vostro nome utente):

```
scp shadowman nomeutente@penguin.example.net:/home/nomeutente
```

Questo comando trasferisce il file locale `shadowman` in `/home/`*`nomeutente`*`/shadowman` su penguin.example.net.

La sintassi per trasferire un file da una macchina remota al sistema locale è la seguente:

```
scp nomeutente@nomehost:/fileremoto
/nuovofilelocale
```

`fileremoto` specifica il file sorgente e *`nuovofilelocale`* specifica la destinazione.

Piu` file possono essere specificati come file sorgenti. Per esempio per trasferire il contenuto della directory `/downloads` nella directory `uploads` già esistente sulla macchina remota penguin.example.net, digitate al prompt della shell il comando seguente:

```
scp /downloads/* nomeutente@penguin.example.net:/uploads/
```

15.3.3. Utilizzo del comando `sftp`

L'utility `sftp` è utilizzata per sessioni FTP interattive e sicure. È simile al comando `ftp` tranne per il fatto che utilizza una connessione sicura e criptata. La sintassi è *`sftp nomeutente@nomehost.com`*. Completata la fase di autenticazione, potete utilizzare il set di comandi simile all'FTP. Consultate la pagina man del comando `sftp` per ottenere un elenco di questi comandi. Per leggere la pagina man, eseguite il comando `man sftp` al prompt della shell. L'utility `sftp` è disponibile a partire dalla versione 2.5.0p1 e successiva di OpenSSH.

15.3.4. Generazione delle coppie di chiavi

Se non volete inserire la vostra password ogni volta che usate i comandi `ssh`, `scp` o `sftp` per collegarvi a una macchina remota, potete generare una coppia di chiavi di autorizzazione.

Le chiavi devono essere generate per ogni utente. Per generare le chiavi per un utente, eseguite la procedura seguente collegandovi con il vostro nome utente. Se vi collegate come root, solo l'utente root potrà utilizzare le chiavi.

Se eseguite l'avvio con la versione 3.0 di OpenSSH, `~/.ssh/authorized_keys2`, `~/.ssh/known_hosts2` e `/etc/ssh_known_hosts2` risultano obsoleti. I protocolli 1 e 2 di SSH condividono i file `~/.ssh/authorized_keys`, `~/.ssh/known_hosts` e `/etc/ssh/ssh_known_hosts`.

Red Hat Linux 9 utilizza le chiavi SSH Protocol 2 e RSA di default.

Suggerimento

Se reinstallate Red Hat Linux ma desiderate salvare la coppia di chiavi generata, eseguite il backup della directory `.ssh` nella vostra directory home. Dopo la reinstallazione copiate di nuovo la directory nella directory home. Questo processo può essere eseguito per tutti gli utenti del sistema, inclusi gli utenti root.

15.3.4.1. Generazione di una coppia di chiavi RSA per la versione 2

Per generare una coppia di chiavi RSA per la versione 2 del protocollo SSH, utilizzate la seguente procedura, che rappresenta il punto di partenza di default relativo a OpenSSH 2.9.

1. Per generare una coppia di chiavi RSA da utilizzare con la versione 2 del protocollo, digitate il seguente comando al prompt della shell:
   ```
   ssh-keygen -t rsa
   ```
   Accettate il percorso predefinito del file `~/.ssh/id_rsa`. Immettete una frase di accesso diversa dalla password del vostro account e confermatela digitandola una seconda volta.

   La chiave pubblica verrà scritta in `~/.ssh/id_rsa.pub`, mentre la chiave privata verrà scritta in `~/.ssh/id_rsa`. Non comunicate mai la vostra chiave privata a nessuno.
2. Modificate i permessi per la directory `.ssh` mediante il comando `chmod 755 ~/.ssh`.
3. Copiate il contenuto di `~/.ssh/id_rsa.pub` in `~/.ssh/authorized_keys` nel computer a cui desiderate connettervi. Se il file `~/.ssh/authorized_keys` non esiste, potete copiare il file `~/.ssh/id_rsa.pub` nel file `~/.ssh/authorized_keys` dell'altro computer.
4. Se è installato GNOME, consultate la Sezione 15.3.4.4. Se non è installato il sistema X Window, consultate la Sezione 15.3.4.5.

15.3.4.2. Generazione di una coppia di chiavi DSA per la versione 2

Per generare una coppia di chiavi DSA per la versione 2 del protocollo SSH, eseguite la procedura qui descritta.

1. Per generare una coppia di chiavi DSA per la versione 2 del protocollo, digitate il seguente comando al prompt della shell:
   ```
   ssh-keygen -t dsa
   ```
   Accettate il percorso predefinito del file `~/.ssh/id_dsa`. Immettete una frase di accesso diversa dalla password del vostro account e confermatela inserendola una seconda volta.

   

   Suggerimento

   Una frase di accesso è una sequenza di parole e caratteri utilizzata per autenticare l'utente. Al contrario delle password, le frasi di accesso possono contenere anche spazi e tabulazioni. Inoltre le frasi di accesso sono generalmente più lunghe delle password poiché possono contenere più parole.

   La chiave pubblica verrà scritta in `~/.ssh/id_dsa.pub`, mentre la chiave privata verrà scritta in `~/.ssh/id_dsa`. Non comunicate mai la vostra chiave privata a nessuno.
2. Modificate i permessi della directory `.ssh` usando il comando `chmod 755 ~/.ssh`.
3. Copiate il contenuto della directory `~/.ssh/id_dsa.pub` in `~/.ssh/authorized_keys` sulla macchina a cui volete collegarvi. Se il file `~/.ssh/authorized_keys` non esiste, potete copiare il file `~/.ssh/id_dsa.pub` nel file `~/.ssh/authorized_keys` sull'altra macchina.
4. Se state utilizzando GNOME, consultate la Sezione 15.3.4.4. Se non state utilizzando il sistema X Window, consultate la Sezione 15.3.4.5.

15.3.4.3. Generazione di una coppia di chiavi RSA per le versioni 1.3 e 1.5

Eseguite la procedura seguente per generare una coppia di chiavi RSA per la versione 1 del protocollo SSH. Se effettuate solo connessioni tra sistemi Red Hat Linux 9, non dovete generare una coppia di chiavi RSA versione 1.3 o RSA versione 1.5.

1. Per generare une coppia di chiavi RSA (per le versioni 1.3 e 1.5), digitate il comando seguente al prompt della shell:
   ```
   ssh-keygen -t rsa1
   ```
   Accettate il percorso predefinito del file (`~/.ssh/identity`). Immettete una frase di accesso diversa dalla vostra password di account e confermatela digitandola una seconda volta.

   La chiave pubblica verrà scritta in `~/.ssh/identity.pub`, mentre la chiave privata verrà scritta in `~/.ssh/identity`. Non comunicate mai la vostra chiave privata a nessuno.
2. Modificate i permessi della directory `.ssh` e le vostre chiavi tramite i comandi `chmod 755 ~/.ssh` e `chmod 644 ~/.ssh/identity.pub`.
3. Copiate il contenuto di `~/.ssh/identity.pub` nel file `~/.ssh/authorized_keys` della macchina remota alla quale volete collegarvi. Se il file `~/.ssh/authorized_keys` non esiste, copiate il file `~/.ssh/identity.pub` nel file `~/.ssh/authorized_keys` sulla macchina remota.
4. Se state eseguendo GNOME, consultate la Sezione 15.3.4.4. Se non state eseguendo GNOME, consultate la Sezione 15.3.4.5.

15.3.4.4. Configurazione di ssh-agent con GNOME

L'utility `ssh-agent` può essere usata per salvare la frase di accesso ed evitare di ridigitarla ogni volta che attivate una connessione `ssh` o `scp`. In GNOME l'utility `openssh-askpass-gnome` può essere usata per richiedere la frase di accesso al momento della connessione a GNOME e per conservarla fino alla disconnessione. Non dovrete inserire la vostra password o frase di accesso per le connessioni `ssh` o `scp` effettuate durante la sessione di GNOME. Se non state usando GNOME, consultate la Sezione 15.3.4.5.

Per salvare la frase di accesso durante la sessione GNOME, eseguite questa procedura:

1. Il vostro sistema deve contenere il pacchetto `openssh-askpass-gnome`; per sapere se disponete di tale pacchetto, digitate il comando `rpm -q openssh-askpass-gnome`. Il pacchetto può essere installato da uno dei CD Red Hat, da un sito mirror FTP Red Hat o usando Red Hat Network.
2. Se non avete il file `~/.Xclients`, potete eseguire `switchdesk` per crearlo. Nel file `~/.Xclients`, modificate la riga seguente:
   ```
   exec $HOME/.Xclients-default
   ```
   Cambiate la riga in modo che risulti:
   `exec /usr/bin/ssh-agent $HOME/.Xclients-default`
3. Selezionate il **pulsante del menu principale** => (sul Pannello) =>**Preferenze** => **Piú preferenze** => **Sessioni** => e fate clic sulla scheda **Programmi di startup**. Fate clic su **Aggiungi** e digitate **`/usr/bin/ssh-add`** nell'area **Comando di startup**. Attribuitegli un livello di priorità superiore a qualsiasi altro comando in modo che venga eseguito per ultimo. Vi consigliamo di attribuire a `ssh-add` un numero uguale o superiore a 70. Più alto è il numero, più bassa è la priorità. Se avete altri programmi in elenco, questo deve avere la priorità più bassa. Selezionate **Close** per uscire dal programma.
4. Scollegatevi e ricollegatevi a GNOME; in altre parole, riavviate X. Una volta avviato GNOME, si apre una finestra di dialogo che richiede l'inserimento della frase di accesso. Inserite la frase

di accesso richiesta. Se sono state configurate sia le chiavi DSA che RSA, il sistema richiede entrambe le coppie. D'ora in poi, i comandi `ssh`, `scp` o `sftp` non richiedono alcuna password.

15.3.4.5. Configurazione di ssh-agent

Il comando `ssh-agent` permette di registrare la frase di accesso per non doverla digitare ogni volta che viene stabilita una connessione `ssh` o `scp`. Se non usate il sistema X Window, eseguite la procedura di seguito riportata dal prompt della shell. Se siete in GNOME, ma non volete configurarlo in modo che vi chieda la vostra frase di accesso al momento del login (consultate la Sezione 15.3.4.4), la procedura funziona in una finestra di terminale, come xterm. Se state eseguendo X, ma non GNOME, la procedura funziona in una finestra di terminale. Tuttavia, la vostra frase di accesso viene memorizzata solo per quella finestra. Non si tratta di un'impostazione valida a livello globale.

1. Al prompt della shell digitate il comando:
   ```
   exec /usr/bin/ssh-agent $SHELL
   ```
   Quindi digitate il comando:
   ```
   ssh-add
   ```
   e inserite la vostra frase di accesso. Se sono configurate più coppie di chiavi, vi vengono richieste tutte le coppie.
2. Quando vi scollegate, la vostra frase di accesso viene cancellata. Ogni volta che vi collegate a una console virtuale o aprite una finestra di terminale, dovete eseguire questi due comandi.

15.4. Risorse aggiuntive

I progetti OpenSSH e OpenSSL sono in continuo sviluppo. Per informazioni più aggiornate, vi consigliamo di collegarvi direttamente al sito Web relativo. Anche le pagine man dei tool OpenSSH e OpenSSL contengono informazioni dettagliate.

15.4.1. Documentazione installata

- Pagine man dei comandi `ssh`, `scp`, `sftp`, `sshd` e `ssh-keygen` — riportano informazioni sull'utilizzo di tali comandi e tutti i parametri a essi associati.

15.4.2. Siti Web utili

- http://www.openssh.com — il sito contiene la pagina delle FAQ di OpenSSH, i report sui bug, le mailing list, gli obiettivi del progetto e una spiegazione più tecnica delle funzioni di sicurezza.
- http://www.openssl.org — il sito contiene la pagina delle FAQ di OpenSSL, le mailing list e una descrizione degli obiettivi del progetto.
- http://www.freessh.org — software client SSH per altre piattaforme.

Capitolo 16.

NFS (Network File System)

L'NFS permette di condividere file tra computer in rete come se fossero sul disco fisso locale del client. Red Hat Linux può essere sia un server che un client NFS, il che significa che può esportare filesystem verso altri sistemi nonché montare filesystem esportati da altri computer.

16.1. Perché usare NFS?

NFS è utile per la condivisione di directory di file fra più utenti su una stessa rete. Per esempio un gruppo che lavora su uno stesso progetto può accedere ai file di questo progetto usando una parte condivisa del filesystem di NFS (solitamente chiamata condivisione NFS) montata nella directory `/myproject`. Per accedere ai file condivisi, l'utente entra nella directory `/myproject` dal suo computer. Per accedervi non è richiesta alcuna password né alcun comando particolare. L'utente lavora come se la directory si trovasse sul suo computer locale.

16.2. Montaggio di un filesystem NFS

Per montare una directory condivisa NFS da un altro computer, digitate il comando `mount`:

```
mount shadowman.example.com:/misc/export /misc/local
```

Avvertenza

Nel computer locale deve esistere la directory mount point (`/misc/local` nell'esempio sopra citato).

In questo comando `shadowman.example.com` corrisponde al nome dell'host del fileserver NFS, `/misc/export` è la directory che `shadowman` sta esportando e `/misc/local` è la directory del computer locale dove si vuole montare il filesystem. Una volta eseguito il comando `mount` (e se avete le autorizzazioni appropriate dal server NFS `shadowman.example.com`), potete digitare `ls /misc/local` per ottenere un elenco di file in `/misc/export` su `shadowman.example.com`.

16.2.1. Montaggio di filesystem NFS con `/etc/fstab`

Per montare una condivisione NFS da un altro computer potete anche aggiungere una linea al file `/etc/fstab`. La linea deve riportare il nome dell'host del server NFS, la directory che viene esportata e la directory che deve contenere la condivisione NFS sul computer locale. Per modificare il file `/etc/fstab` dovete essere collegati come root.

Di seguito è riportata la sintassi generale per la linea in `/etc/fstab`:

```
server:/usr/local/pub    /pub    nfs    rsize=8192,wsize=8192,timeo=14,intr
```

Il vostro computer client deve contenere il mount point `/pub`. Una volta aggiunta la linea a `/etc/fstab` sul sistema client, digitate il comando `mount /pub` al prompt della shell e il mount point `/pub` sarà montato dal server.

16.2.2. Montaggio di filesystem NFS con autofs

Il terzo metodo di montaggio di una condivisione NFS prevede l'utilizzo di Autofs, che impiega il demone automount per gestire i mount point montandoli in modo dinamico.

Autofs consulta il file di configurazione della mappa master `/etc/auto.master` per determinare quali mount point sono definiti. Avvia quindi un processo di automontaggio con i parametri appropriati per ogni mount point. Ogni linea della mappa master definisce un mount point e un file di mappa separato che definisce i filesystem da montare sotto questo mount point. Per esempio, il file `/etc/auto.misc` definisce i mount point nella directory `/misc`; ciò viene definito nel file `/etc/auto.master`.

Ogni voce in `auto.master` ha tre campi. Il primo campo è il mount point. Il secondo campo indica la posizione del file di mappa e il terzo campo, opzionale, può contenere informazioni quali il valore di timeout.

Per esempio, per montare la directory `/proj52` della macchina remota penguin.example.net sul mount point `/misc/myproject` della vostra macchina, aggiungete la riga seguente ad `auto.master`:

```
/misc   /etc/auto.misc --timeout 60
```

Aggiungete questa riga al file `/etc/auto.misc`:

```
myproject  -rw,soft,intr,rsize=8192,wsize=8192 penguin.example.net:/proj52
```

Il primo campo contenuto in `/etc/auto.misc` indica il nome della sottodirectory `/misc`, che viene creata in modo dinamico da automount. In realtà la directory non dovrebbe esistere sul computer client. Il secondo campo contiene opzioni di montaggio quali `rw` per accesso in lettura e scrittura. Il terzo campo è la posizione dell'NFS di esportazione e contiene il nome dell'host e la directory.

Nota Bene

La directory `/misc` deve esistere nel filesystem locale, che non deve contenere sottodirectory di `/misc`.

Il servizio Autofs può essere avviato dal prompt della shell digitando i comandi seguenti:

```
/sbin/service autofs restart
```

Per visualizzare i mount point attivi, digitate il comando seguente al prompt della shell:

```
/sbin/service autofs status
```

Se modificate il file di configurazione `/etc/auto.master` mentre autofs è in esecuzione, dovete dire ai demoni automount di ricaricare autofs digitando al prompt della shell il comando seguente:

```
/sbin/service autofs reload
```

Per imparare a configurare autofs in modo che venga eseguito all'avvio, consultate le informazioni sulla gestione dei servizi contenute nel Capitolo 14.

16.3. Esportazione di filesystem NFS

La condivisione di file da un server NFS è conosciuta come esportazione di directory. Il **Strumento di configurazione del server NFS** può essere utilizzato per configurare un sistema come server NFS.

Per utilizzare il **Strumento di configurazione del server NFS**, dovete eseguire sul vostro computer il sistema X Window, avere privilegi root e avere installato il pacchetto RPM `redhat-config-nfs`. Per lanciare l'applicazione, selezionate **Pulsante menu principale** (sul pannello) => **Impostazioni del sistema** => **Server NFS** oppure digitate il comando `redhat-config-nfs`.

Figura 16-1. Strumento di configurazione del server NFS

Per aggiungere una condivisione NFS, fate clic sul pulsante **Aggiungi**. Compare la casella di dialogo mostrata nella Figura 16-2.

La linguetta **Basico** richiede le informazioni seguenti:

- **Directory** — specificare la directory da condividere, come per esempio `/tmp`.
- **Host** — specificare l'host (o gli host) per i quali condividere la directory. Per informazioni sui formati possibili consultate la la Sezione 16.3.2.
- **Permessi di base** — specificare se alla directory vanno attribuiti permessi di sola lettura o di lettura/scrittura.

Figura 16-2. Aggiunta di una condivisione

La linguetta **Opzioni generali** consente di configurare le opzioni seguenti:

- **Allow connections from port 1024 and higher** — i servizi da eseguirsi su numeri di porta inferiori alla 1024 possono essere avviati solo da root. Selezionate questa opzione se volete che il servizio NFS possa esseree avviato da un utente non root. Questa opzione corrisponde a `insecure`.
- **Consenti blocco dei file non sicuri** — non necessita di una richiesta di blocco. Questa opzione corrisponde a `insecure_locks`.

- **Disabilita verifica del subtree** — se viene esportata una sottodirectory di un dato filesystem ma non l'intero filesystem, il server esegue un controllo per verificare se il file richiesto si trova nella sottodirectory esportata. Questa ricerca viene chiamato *subtree checking*. Selezionate questa opzione se volete disabilitare il controllo. Se viene esportato l'intero filesystem, scegliendo di disabilitare questo controllo si può contribuire ad aumentare la velocità di trasferimento. Questa opzione corrisponde a `no_subtree_check`.
- **Sync write operations on request** — attivata per default, questa opzione impedisce al server di rispondere alle richieste prima che le modifiche apportate dalle richieste siano state salvate sul disco. Questa opzione corrisponde a `sync`. Se non è selezionata, viene utilizzata l'opzione`async`.
  - **Sincronizzazione forzata di operazioni in scrittura immediately** — non ritarda la scrittura su disco. Questa opzione corrisponde a `no_wdelay`.

La linguetta **Accesso utente** consente di configurare le seguenti opzioni:

- **Considera utente root remoto come root locale** — per default, le ID utente e le ID gruppo dell'utente root sono entrambe impostate su 0. Lo "schiacciamento" di root imposta l'ID utente 0 e l'ID gruppo 0 come ID utente e gruppo anonime in modo che il root sul client non possegga privilegi di root sul server NFS. Se questa opzione è stata selezionata, l'utente root non è impostato come anonimo e il root su un client possiede priviliegi di root per le directory esportate. Selezionare questa opzione significa ridurre notevolmente la sicurezza del sistema, dunque non fatelo a meno che non lo riteniate strettamente necessario. Questa opzione corrisponde a `no_root_squash`.
- **Considera tutti gli utenti client come utenti anonimi** — se questa opzione è stata selezionata, tutte le ID utente e gruppo vengono impostate come utente anonimo. Questa opzione corrisponde a `all_squash`.
  - **Specifica l'ID dell'utente locale per gli utenti anonimi** — Se l'opzione **Considera tutti gli utenti client come utenti anonimi** è selezionata, questa opzione vi consente di specificare una ID utente per l'utente anonimo. Questa opzione corrisponde a `anonuid`.
  - **Specifica l'ID dell'utente locale per gli utenti anonimi** — Se l'opzione **Considera tutti gli utenti client come utenti anonimi** è in funzione, questa opzione consente di specificare una ID gruppo per l'utente anonimo. Questa opzione corrisponde a `anongid`.

Per modificare una condivisione NFS esistente, selezionatela dall'elenco e fate clic sul pulsante **Proprietà**. Per cancellarla, fate lo stesso e poi fate clic sul pulsante **Cancella**.

Dopo aver cliccato su **OK** per aggiungere, modificare o cancellare uno share NFS dalla lista, il cambiamento viene confermato immediatamente — il demone del server viene riavviato, e il vecchio file di configurazione viene salvato come `/etc/exports.bak`. La nuova configurazione viene iscritta su `/etc/exports`.

Strumento di configurazione del server NFS legge e scrive direttamente da e sul file di configurazione `/etc/exports`; pertanto, il file può essere modificato manualmente dopo aver utilizzato il tool e il tool può essere utilizzato dopo aver modificato manualmente il file (se questo è stato modificato con la sintassi corretta).

16.3.1. Configurazione a linea di comando

Se preferite servirvi di un editor di testo o non avete installato il sistema X Window, potete modificare il file di configurazione direttamente.

Il file `/etc/exports` controlla le directory che il server NFS esporta. Il suo formato è il seguente:

```
directory hostname(options)
```

L'unica opzione che necessita di essere specificata é una tra `sync` o `async` (si raccomanda `sync`). Se si specifica `sync`, il server non replica alle richieste prima che i cambiamenti vengano iscritti sul disco.

Per esempio:

```
/misc/export      speedy.example.com(sync)
```

autorizza gli utenti di `speedy.example.com` a montare `/misc/export` con i permessi di sola lettura di default, ma:

```
/misc/export      speedy.example.com(rw,sync)
```

autorizza gli utenti di `speedy.example.com` a montare `/misc/export` con privilegi di lettura-scrittura.

Per informazioni sui possibili formati dei nomi di host, consultate la la Sezione 16.3.2.

Per reperire un elenco delle opzioni che possono essere specificate, consultate la *Red Hat Linux Reference Guide*.

Attenzione

Prestate attenzione agli spazi, all'interno del file `/etc/exports`. Se non ci sono spazi tra il nome dell'host e le opzioni tra parentesi, le opzioni si riferiscono unicamente al nome dell'host. Se invece i due elementi sono separati da uno spazio, le opzioni si riferiscono al resto del mondo. Osservate per esempio le righe seguenti:

```
/misc/export speedy.example.com(rw,sync)
/misc/export speedy.example.com (rw,sync)
```

La prima linea assicura agli utenti di `speedy.example.com` l'accesso in lettura-scrittura, mentre lo nega a tutti gli altri utenti. La seconda riga, invece, assicura agli utenti di `speedy.example.com` l'accesso di sola lettura (default) e consente al resto del mondo l'accesso in lettura-scrittura.

Ogni volta che modificate `/etc/exports`, dovete informare il demone NFS del cambiamento oppure ricare il file di configurazione tramite il comando seguente:

```
/sbin/service nfs reload
```

16.3.2. Formati dei nomi di host

Gli host possono avere i formati seguenti:

- Macchina singola — un nome di dominio completo (che può essere risolto dal server), nome di host (che può essere risolto dal server) o un indirizzo IP
- Serie di macchine specificate con caratteri jolly — Usate i caratteri * o ? per specificare la corrispondenza di una stringa. Per esempio, `192.168.100.*` specifica un indirizzo IP che comincia con 192.168.100. Quando si aggiungono caratteri jolly a nomi di dominio completi, non si devono inserire punti (.) Per esempio, `*.example.com` comprende one.example.com ma non one.two.example.com.
- Reti IP — Utilizzate *`a.b.c.d/z`*, dove *`a.b.c.d`* è la rete e *`z`* il numero di bit nella maschera di rete (per esempio 192.168.0.0/24). Un altro formato accettabile è *`a.b.c.d/netmask`*, dove *`a.b.c.d`* è la rete e *`netmask`* è la maschera di rete (per esempio, 192.168.100.8/255.255.255.0).

- Gruppi di rete — nel formato `@nome-gruppo`, dove `nome-gruppo` è il nome di gruppo di rete NIS.

16.3.3. Avvio e arresto del server

Sul server che esporta i filesystem NFS deve essere in esecuzione il servizio `nfs`.

Visualizzate lo stato del demone NFS con il comando seguente:

```
/sbin/service nfs status
```

Avviate il demone NFS con il comando seguente:

```
/sbin/service nfs start
```

Arrestate il demone NFS con il comando seguente:

```
/sbin/service nfs stop
```

Per avviare il servizio `nfs` all'avvio, utilizzate il comando:

```
/sbin/chkconfig --level 345 nfs on
```

Potete anche utilizzare `chkconfig`, **ntsysv** o il **Strumento di configurazione dei servizi** per configurare i servizi da lanciare all'avvio del sistema. Per maggiori dettagli, consultate il Capitolo 14.

16.4. Risorse aggiuntive

Il capitolo spiega le basi dell'utilizzo di NFS. Per maggiori informazioni, consultate le risorse di seguito riportate.

16.4.1. Documentazione installata

- Pagine man per `nfsd`, `mountd`, `exports`, `auto.master` e `autofs` (nelle sezioni 5 e 8 del manuale) — queste pagine man mostrano la sintassi corretta dei file di configurazione di autofs e NFS.

16.4.2. Siti Web utili

- http://www.tldp.org/HOWTO/NFS-HOWTO/index.html — Il manuale *Linux NFS-HOWTO* dal progetto di documentazione di Linux.

16.4.3. Libri correlati

- *Managing NFS and NIS Services* di Hal Stern; edizioni O'Reilly & Associates, Inc.

Capitolo 17.

Samba

Samba utilizza il protocollo SMB per la condivisione di file e di stampanti tramite una connessione di rete. I sistemi operativi che supportano questo protocollo sono Microsoft Windows (tramite il suo **Network Neighborhood**), OS/2 e Linux.

17.1. Perché usare Samba?

Samba è utile se alla vostra rete sono collegate sia macchine Windows sia Linux. Samba consente la condivisione di file e stampanti da parte di tutti i vari sistemi in rete. Se desiderate condividere file solo tra macchine Red Hat Linux, usare NFS come accennato su Capitolo 16. Se desiderate condividere stampanti solo tra macchine Red Hat Linux, non avrete bisogno di usare Samba; consultate allora Capitolo 27.

17.2. Configurazione di un server di Samba

Il file di configurazione di default (`/etc/samba/smb.conf`) consente agli utenti di visualizzare le proprie home directory di Red Hat Linux come una condivisione di Samba. Inoltre, condivide tutte le stampanti configurate per il sistema Red Hat Linux come stampanti condivise di Samba. In altre parole, potete collegare una stampante al vostro sistema e usarla per stampare da altre macchine Windows sulla vostra rete.

17.2.1. Configurazione grafica

Per configurare Samba usando una interfaccia grafica, usare il **Strumento di configurazione del server Samba**. Per la configurazione della linea di comando andare su la Sezione 17.2.2.

Il **Strumento di configurazione del server Samba** é una interfaccia grafica per la gestione delle condivisioni di Samba, utenti, ed impostazioni basiche del server. Esso modifica i file di configurazione nella directory `/etc/samba/`. Qualsiasi cambiamento apportato ai suddetti file non effettuato usando la suddetta applicazione, non sará confermato.

Per poter usare questa applicazione, dovete eseguire il Sistema X di Window, avere i privilegi di un utente root, e avere il pacchetto RPM `redhat-config-samba`, installato. Per avviare il **Strumento di configurazione del server Samba** dal desktop, andate su **Pulsante menu principale** (sul pannello) **=> Impostazioni del sistema => Impostazioni del Server => Server di Samba** o inserite il comando `redhat-config-samba` ad un prompt della shell (per esempio, in un terminale XTerm o GNOME).

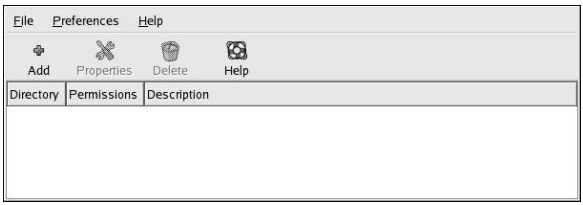

Figura 17-1. Strumento di configurazione del server Samba

Nota Bene

Il **Strumento di configurazione del server Samba** non mostra le stampanti condivise o la stanza di default che permette agli utenti di visualizzare le proprie home directory sul server di Samba.

17.2.1.1. Configurazione delle impostazioni del server

Il primo passo nella configurazione di un server di Samba, é quello di configurare le impostazioni di base per il server e qualche opzione di sicurezza. Dopo aver iniziato l'applicazione, selezionare, **Preferenze => Impostazioni del server** dal menu a tendina. Il tab **Basico** viene visualizzato come mostrato su Figura 17-2.

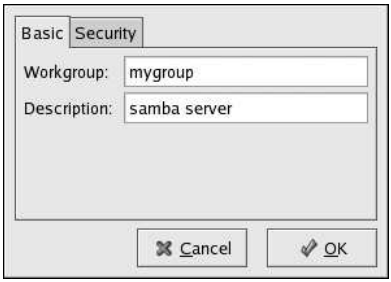

Figura 17-2. Configurazione delle impostazioni di base del server

Sulla scheda **Basica**, specificare in quale gruppo di lavoro il computer si dovrebbe trovare fornendo anche una breve descrizione del computer stesso. Essi corrispondono alle opzioni `workgroup` e `server string` in `smb.conf`.

Figura 17-3. Configurazione impostazioni del server di sicurezza

La tabella **Securezza** contiene le opzioni seguenti:

- **Modalità di autenticazione** — Ció corrisponde alla opzione `security`. Selezionare uno dei seguenti tipi di autenticazione.
  - **Dominio** — Il server di Samba, si affida ad un Controllore del dominio NT primario o di backup per verificare l'utente. L'utente invia il nome utente e la password al Controllore, aspettando la risposta. Specificare il nome del NetBIOS del Controllore del dominio primario o di backup nel campo **Server di autenticazione**.

L'opzione **Password cifrate** deve essere impostato su **Si** se selezionata.

- **Server** — Il server di Samba cerca di verificare la combinazione tra il nome dell'utente e la password, inviandoli ad un altro server. Altrimenti, il server cerca di effettuare la verifica, usando il modo di autenticazione dell'utente. Specificare il nome del NetBIOS dell'altro server del Samba, nel campo **Server di autenticazione**
- **Condivisione** — Gli utenti di Samba, non devono inserire alcun nome utente e password ad ogni singolo server. Essi non sono richiesti a specificare un nome utente e password, fino a quando non provano a connettersi ad una directory di condivisione specifica da un server di Samba.
- **Utente** — gli utenti (Default) di Samba, devono fornire un valido nome utente e password ad ogni server di Samba. Selezionare questa opzione se desiderate che l'opzione **Utente Windows** funzioni. Consultate la Sezione 17.2.1.2 per maggiori dettagli.

- **Cifrare le password** — (il valore di default é **Si**). Questa opzione deve essere abilitata se i clienti sono collegati da Windows 98, Windows NT 4.0 con Service Pack 3, o versioni piú recenti di Microsoft Windows. Le password vengono trasferite tra il server e il client in un formato cifrato invece di un testo in chiaro che puó essere intercettato. Ció corrisponde in una opzione `password cifrate`. Consultare la Sezione 17.2.3 per maggiori informazioni.
- **Account guest** — Quando gli utenti o utenti ospiti effettuano una registrazione ad un server Samba, essi devono essere collocati su di un utente valido nel server. Selezionare uno dei nomi utenti esistenti sul sistema, per ottenere un account Samba guest. Quando gli utenti ospiti effettuano una registrazione nel server di Samba, essi hanno gli stessi privilegi degli utenti Samba. Ció corrisponde all'opzione `guest account`.

Dopo aver fatto clic su **OK**, i cambiamenti vengono scritti sul file di configurazione ed il demone viene riavviato; in modo tale da confermare immediatamente i cambiamenti.

17.2.1.2. Gestione utenti Samba

Il **Strumento di configurazione del server Samba** richiede che un account di un utente giá esistente sia attivo sul sistema Red Hat Linux funzionando come un server di Samba prima che l'utente venga aggiunto. L'utente di Samba é associato con un account di un utente Red Hat Linux esistente.

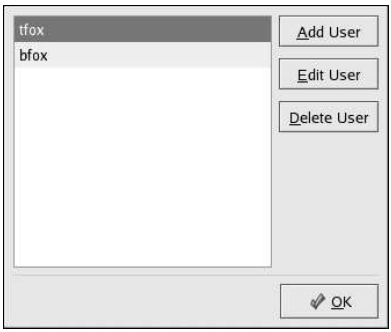

Figura 17-4. Gestione utenti Samba

Per aggiungere un utente Samba, selezionate **Preferenze => Utenti Samba** dal menu a tendina, e fate clic sul pulsante **Aggiungi utente**. Sulla finestra **Creare un nuovo utente Samba** selezionare un **Nome utente Unix** dalla lista di utenti esistenti sul sistema locale.

Se l'utente ha un nome utente diverso su di una macchina Windows e sará registrato in un server Samba da una macchina Windows, specificare il nome utente di Windows nel campo **Nome utente di Windows**. Il **Modo di autenticazione** sulla tabella **Sicurezza** delle preferenze **Impostazioni del Server** deve essere impostato su **Utente** per poter funzionare.

Configurare una **Password di Samba** per l'utente Samba e confermarla digitandola ancora. Anche se decidete di usare password cifrate per Samba, é consigliato che la stessa password sia diversa per ogni utente dalle password del loro sistema Red Hat Linux

Per modificare un utente giá esistente, selezionare l'utente stesso dalla lista e fare clic su **Modifica utente**. Per cancellare un utente Samba esistente, selezionarlo e fare clic sul pulsante **Cancella utente**. Cancellando l'utente di Samba, non si cancella l'associato account utente di Red Hat Linux.

Gli utenti vengono modificati immediatamente dopo aver fatto clic sul pulsante **OK**.

17.2.1.3. Aggiungere una condivisione

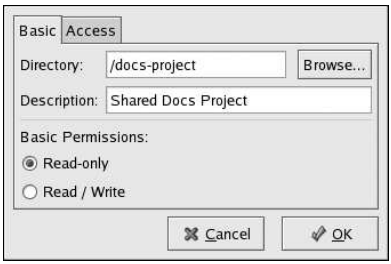

Figura 17-5. Aggiungere una condivisione

Per aggiungere una condivisione, fare clicc sul pulsante **Aggiungi**. La scheda **Basica** configura le seguenti opzioni:

- **Directory** — La directory per la condivisione tramite Samba. La directory deve esistere.
- **Descrizioni** — Una breve descrizione della condivisione.
- **Permessi di base** — Se gli utenti devono solo essere in grado leggere i file nelle directory condivise o se essi devono essere in grado di leggere e scrivere sulla directory condivisa.

Sulla tabella **Accesso**, selezionare se permettere solo utenti specifici all'accesso della condivisione oppure se permettere a tutti gli utenti Samba di accedere alla stessa. Se si seleziona la prima opzione, selezionare gli utenti dalla lista di utenti Samba disponibili.

La condivisione viene aggiunta immediatamente dopo aver fatto clic su **OK**.

17.2.2. Configurazione della linea di comando

Samba usa `/etc/samba/smb.conf` come proprio file di configurazione. Se cambiate questo file, i cambiamenti non saranno confermati fino a quando non riavviate il demone Samba con il comando `service smb restart`.

Per specificare il gruppo di lavoro di Windows con una breve descrizione del server di Samba, modificate le seguenti linee nel vostro file `smb.conf`:

```
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
```

Sostituite il *NOMEGRUPPODILAVORO* con il nome del gruppo di lavoro di Windows a cui questa macchina appartiene. Il *BREVE COMMENTO SUL SERVER* è opzionale e contiene un commento Windows sul sistema Samba.

Per creare una directory di condivisione Samba sul sistema Linux, aggiungete la seguente sezione al vostro file `smb.conf` (dopo averlo modificato in base alle vostre esigenze e a quelle del sistema):

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
writable = yes
printable = no
create mask = 0765
```

L'esempio illustrato sopra consente agli utenti tfox e carole di leggere e scrivere nella directory `/home/share`, sul server Samba da un client Samba.

17.2.3. Password cifrate

In Red Hat Linux 9 le password cifrate sono abilitate di default per una maggiore sicurezza. Se queste non vengono utilizzate, si usano le password in chiaro, che possono essere intercettate da chiunque usi un packet sniffer. È caldamente consigliato preferire le password cifrate.

Il protocollo SMB di Microsoft era usato in origine con le password in "chiaro". Tuttavia, Windows 2000 e Windows NT 4.0 con Service Pack 3 o versioni superiori richiedono password cifrate. Per utilizzare Samba tra un sistema Red Hat Linux e un sistema Windows 2000 o Windows NT 4.0 con Service Pack 3 o superiore, potete modificare il registro di Windows per usare password in chiaro oppure potete configurare Samba sul sistema Linux per usare le password cifrate. Se decidete di modificare la vostra registrazione, dovete farlo per tutte le macchine con Windows NT o 2000: questa operazione è piuttosto rischiosa e può causare ulteriori conflitti.

Per configurare Samba sul sistema Red Hat Linux per utilizzare password cifrate, seguite le istruzioni illustrate qui di seguito:

1. Create un file di password diverso per Samba. Per crearne uno basato sul vostro file esistente `/etc/passwd`, digitate al prompt il comando seguente:
   ```
   cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   Se il sistema utilizza NIS, digitate il seguente comando:
   ```
   ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   Lo script `mksmbpasswd.sh` è installato nella directory `/usr/bin` con il pacchetto `samba`.
2. Cambiate i permessi del file delle password di Samba, in modo che solo root abbia i permessi di lettura e scrittura:
   ```
   chmod 600 /etc/samba/smbpasswd
   ```
3. Lo script non copia le password utente nel nuovo file, e un account utente Samba non é attivo fino a quando una password é impostata. Per maggiore sicurezza, é consigliato che la password di Samba dell'utente sia diversa dalla password di Red Hat Linux. Per impostare ogni password dell'utente di Samba, usare il seguente comando (sostituire *nome utente* con ogni nome utente dell'utente):
   ```
   smbpasswd username
   ```

4. È ora necessario abilitare le password cifrate nel file di configurazione di Samba. Per farlo, eliminate il commento dalle righe seguenti nel file `smb.conf`:
   ```
   encrypt passwords = yes
   smb passwd file = /etc/samba/smbpasswd
   ```
5. Assicuratevi che il servizio `smb` venga lanciato digitando il comando `service smb restart` al prompt della shell.
6. Se desiderate che il servizio `smb` si avvii automaticamente, utilizzate **ntsysv**, `chkconfig`, o **Strumento di configurazione dei servizi** per attivarlo al runtime. Per informazioni dettagliate consultate il Capitolo 14.

Suggerimento

Per saperne di più sulle password cifrate, leggete `/usr/share/doc/samba-`<*versione*>`/docs/htmldocs/ENCRYPTION.html` (sostituite <*versione*> con il numero della versione di Samba che avete installato).

Il modulo PAM `pam_smbpass` consente di sincronizzare le password Samba degli utenti con le loro password di sistema quando usano il comando `passwd`. Se un utente richiama il comando `passwd`, la password per la connessione al sistema Red Hat Linux e quella per la partizione Samba vengono entrambe modificate.

Per attivare questa caratteristica, aggiungete la seguente riga a `/etc/pam.d/system-auth` sotto `pam_cracklib.so`:

```
password required /lib/security/pam_smbpass.so nullok use_authtok try_first_pass
```

17.2.4. Come avviare e fermare il server

Sul server che stá condividendo le directory tramite Samba, deve essere eseguito il servizio `smb`.

Visualizzate la condizione del demone di Samba con il seguente comando:

```
/sbin/service smb status
```

Avviare il server con il seguente comando:

```
/sbin/service smb start
```

Fermare il demone con il seguente comando:

```
/sbin/service smb stop
```

Per avviare il servizio `smb` al momento dell'avvio, usare il comando:

```
/sbin/chkconfig --level 345 smb on
```

Potete usare anche `chkconfig`, **ntsysv** o **Strumento di configurazione dei servizi** per configurare quale servizio deve essere avviato al momento della partenza. Consultare Capitolo 14 per maggiori informazioni.

17.3. Connettersi alla condivisione Samba

Per connettersi ad una condivisione Samba da una macchina Microsoft Windows, usare **Network Neighborhood** o il file grafico manager.

Per connettervi da un sistema Linux, digitate quanto segue al prompt della shell:

```
smbclient //hostname/sharename -U username
```

È necessario sostituire *nome dell'host* con il nome dell'host o l'indirizzo IP del server Samba a cui volete connettervi, *nome di condivisione* con il nome della directory che volete visitare e *nome utente* con il nome utente Samba per il sistema. Inserite la password corretta oppure premete [Invio], nel caso non sia richiesta alcuna password per l'utente.

Se al prompt compare la stringa `smb:\>`, il login è avvenuto correttamente. Una volta collegati, digitate **`help`** per ottenere la lista di comandi. Se desiderate visualizzare i contenuti della vostra directory home, sostituite *nomecondivisione* con il vostro nome utente. Se non utilizzate `-U`, il nome utente attuale viene inviato al server Samba.

Per uscire da `smbclient`, digitate **`exit`** al prompt `smb:\>`.

Potete anche utilizzare **Nautilus** per visualizzare le condivisioni Samba disponibili sulla vostra rete. Selezionate **Pulsante menu principale** (sul pannello) => **Server di rete** per visualizzare una lista di gruppi di lavoro di Samba. Potete anche inserire **`smb:`** nella barra **Posizione:** di Nautilus per visualizzare i gruppi di lavoro.

Come mostrato nella Figura 17-6, vedrete un'icona per ogni gruppo di lavoro SMB disponibile sulla vostra rete.

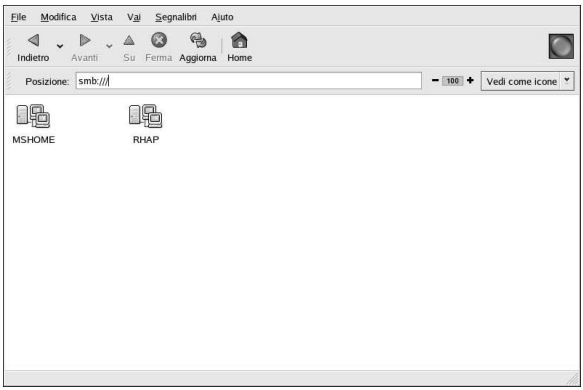

Figura 17-6. Gruppi di lavoro SMB in Nautilus

Effettuate un doppio clic su una delle icone del gruppo di lavoro, per visualizzare una lista di computer all'interno del gruppo di lavoro.

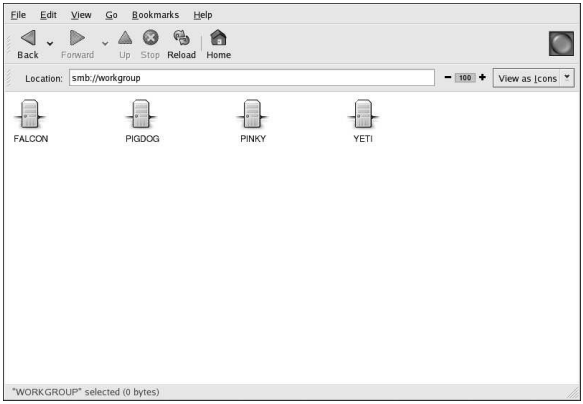

Figura 17-7. Macchine SMB in Nautilus

Come é possibile vedere su Figura 17-7, c'é una icona per ogni macchina all'interno del gruppo di lavoro. Fate un doppio clic sull'icona per visualizzare le condivisioni Samba sulla macchina. Se é necessaria una combinazione tra nome utente e password, esse vi verranno richieste.

Alternativamente, potete specificare un nome utente e password nella barra **Posizione:** utilizzando la seguente sintassi (sostituite *utente*, *password*, *nome server*, e *nome condivisione* con i valori corretti):

```
smb://user:password@servername/sharename/
```

17.4. Risorse aggiuntive

Per informazioni sulle opzioni di configurazione che non sono state trattate in questo capitolo, consultate le risorse seguenti:

17.4.1. Documentazione installata

- Pagina man di `smb.conf` — illustra come impostare il file di configurazione di Samba.
- Pagina man di `smbd` — descrive il funzionamento del demone di Samba.
- `/usr/share/doc/samba-<version-number>/docs/` — si tratta di file help txt o HTML e sono compresi nel pacchetto `samba`.

17.4.2. Siti Web utili

- http://www.samba.org — la pagina Web di Samba contiene una documentazione utile relativa alle mailing list e alla lista delle interfacce grafiche.

Capitolo 18.

Dynamic Host Configuration Protocol (DHCP)

Il Dynamic Host Configuration Protocol (DHCP) è un protocollo di rete per l'assegnazione automatica di informazioni TCP/IP alle macchine client. Ciascun client DHCP si connette al server DHCP collocato centralmente, il quale restituisce la configurazione di rete del client includendo indirizzo IP, gateway e server DNS.

18.1. Perché usare il DHCP?

Il DHCP è utile per l'allocazione dinamica della configurazione di rete del client. Durante la configurazione del sistema client, l'amministratore può scegliere il DHCP e decidere di non dover inserire un indirizzo IP, la maschera di rete, il gateway o i server DNS. Il client recupera queste informazioni dal server DHCP. Il DHCP si rivela utile anche quando l'amministratore desidera cambiare l'indirizzo IP di un ampio numero di sistemi. Invece di riconfigurare tutti i sistemi, l'amministratore può modificare un solo file di configurazione DHCP sul server per il nuovo set di indirizzi IP. Se i server DNS di un'organizzazione cambiano, le modifiche vengono applicate al server DHCP, non a tutti i client DHCP. Una volta riavviata la rete sui client (o riavviati i client), le modifiche diventeranno effettive.

Inoltre, se si configura un laptop o qualsiasi altro tipo di computer portatile per il DHCP, è possibile spostarlo da un ufficio all'altro senza doverlo riconfigurare, purché l'ufficio disponga di un server DHCP che ne consenta la connessione in rete.

18.2. Configurazione di un server DHCP

È possibile configurare un server DHCP usando il file di configurazione `/etc/dhcpd.conf`.

Il DHCP utilizza anche il file `/var/lib/dhcp/dhcpd.leases` per archiviare il database in 'affitto' (lease) del client. Per ulteriori informazioni, fate riferimento alla la Sezione 18.2.2.

18.2.1. File di configurazione

La prima fase della configurazione di un server DHCP è la creazione del file di configurazione contenente le informazioni di rete per i client. Le opzioni globali possono essere inserite per tutti i client oppure per ciascun sistema client.

Il file di configurazione può contenere schede e linee vuote aggiuntive per facilitare la formattazione. Le parole chiave non distinguono tra lettere maiuscole e lettere minuscole e le linee che iniziano con un cancelletto (#) sono considerate commenti.

Due sono gli schemi di aggiornamento DNS correntemente implementati, la modalità di aggiornamento DNS ad-hoc e quella della bozza di interazione DHCP-DNS temporanea. Se e quando queste due modalità verranno accettate come parte del processo degli standard IETF, sarà disponibile una terza modalità— il metodo di aggiornamento DNS standard. Il server DHCP deve essere configurato per l'utilizzo di uno dei due schemi correnti. La versione 3.0b2pl11 e la versione precedente utilizzavano la modalità ad-hoc, che ora non è più così utilizzata. Se desiderate che venga mantenuto lo stesso comportamento, aggiungete la riga riportata di seguito nella parte superiore del file di configurazione:

```
ddns-update-style ad-hoc;
```

Per utilizzare la modalità consigliata, aggiungete la riga riportata di seguito nella parte superiore del file di configurazione:

```
ddns-update-style interim;
```

Per ulteriori informazioni sulle diverse modalità, consultate la pagina man `dhcpd.conf`.

Esistono due tipi di dichiarazioni nei file di configurazione:

- Parametri — indicano come eseguire un'operazione, se eseguire un'operazione oppure quali opzioni di configurazione di rete inviare al client.
- Dichiarazioni — descrivono la topologia della rete, i client, forniscono indirizzi per i client o applicano un gruppo di parametri a un gruppo di dichiarazioni.

Alcuni parametri richiedono di essere avviati con la parola chiave `option` e sono indicati come opzioni che configurano le opzioni DHCP, mentre i parametri configurano i valori non opzionali oppure controllano l'attività del server DHCP.

I parametri (incluse le opzioni) dichiarati prima di una sezione inclusa tra parentesi graffe ({ }) sono considerati parametri globali, ovvero si applicano a tutte le sezioni che li seguono.

Importante

Se modificate il file di configurazione, le modifiche avranno effetto solo al riavvio del demone DHCP con il comando `service dhcpd restart`.

Nell'Esempio 18-1 le opzioni `routers`, `subnet-mask`, `domain-name`, `domain-name-servers` e `time-offset` sono utilizzate per le dichiarazioni `host` dichiarate sotto di esse.

Come mostra l'Esempio 18-1, è possibile indicare una `subnet`. È necessario includere una dichiarazione `subnet` per ogni sottorete della rete. In caso contrario, il server DHCP non si avvierà.

Quest'esempio riporta delle opzioni globali per ogni client DHCP nella sottorete e un `range` dichiarato. Ai client viene assegnato un indirizzo IP compreso nel `range`.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
        option routers                  192.168.1.254;
        option subnet-mask              255.255.255.0;

        option domain-name              "example.com";
        option domain-name-servers       192.168.1.1;

        option time-offset              -18000;     # Eastern Standard Time

 range 192.168.1.10 192.168.1.100;
}
```

Esempio 18-1. Dichiarazione di sottorete

Tutte le sottoreti che condividono la stessa rete fisica dovrebbero essere inserite in una dichiarazione `shared-network`, come mostra l'Esempio 18-2. I parametri contenuti nella `shared-network` e non nelle dichiarazioni `subnet` sono considerati parametri globali. Il nome della `shared-network` dovrebbe essere un titolo descrittivo per la rete, come per esempio test-lab per descrivere tutte le sottoreti in un ambiente di laboratorio per i test.

```
shared-network name {
    option domain-name              "test.redhat.com";
    option domain-name-servers      ns1.redhat.com, ns2.redhat.com;
    option routers                  192.168.1.254;
    more parameters for EXAMPLE shared-network
    subnet 192.168.1.0 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.1 192.168.1.31;
    }
    subnet 192.168.1.32 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.33 192.168.1.63;
    }
}
```

Esempio 18-2. Dichiarazione di rete condivisa

Come mostra l'Esempio 18-3, la dichiarazione `group` può essere utilizzata per applicare i parametri globali a un gruppo di dichiarazioni. È possibile raggruppare reti condivise, sottoreti, host o altri gruppi.

```
group {
   option routers                  192.168.1.254;
   option subnet-mask              255.255.255.0;

   option domain-name              "example.com";
   option domain-name-servers       192.168.1.1;

   option time-offset              -18000;     # Eastern Standard Time

   host apex {
      option host-name "apex.example.com";
      hardware ethernet 00:A0:78:8E:9E:AA;
      fixed-address 192.168.1.4;
   }

   host raleigh {
      option host-name "raleigh.example.com";
      hardware ethernet 00:A1:DD:74:C3:F2;
      fixed-address 192.168.1.6;
   }
}
```

Esempio 18-3. Dichiarazione di gruppo

Per configurare un server DHCP che affitta indirizzi IP dinamici al sistema inserito in una sottorete, modificate l'Esempio 18-4 inserendo i vostri valori. Questo dichiara un tempo di affitto di default, il tempo massimo e i valori della configurazione di rete per i client. L'esempio riportato qui di seguito assegna gli indirizzi IP ai sistemi client nel `range` 192.168.1.10 e 192.168.1.100.

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";

subnet 192.168.1.0 netmask 255.255.255.0 {
   range 192.168.1.10 192.168.1.100;
}
```

Esempio 18-4. Parametro del range

Per assegnare un indirizzo IP a un client che si basa sull'indirizzo MAC della scheda di rete, utilizzare il parametro `hardware ethernet` contenuto nella dichiarazione `host`. Come dimostra l'Esempio 18-5, la dichiarazione `host apex` specifica che la scheda di rete con l'indirizzo MAC 00:A0:78:8E:9E:AA dovrebbe sempre corrispondere all'indirizzo IP 192.168.1.4.

Si ricorda che è anche possibile utilizzare il parametro opzionale `host-name` per assegnare un nome di host al client.

```
host apex {
   option host-name "apex.example.com";
   hardware ethernet 00:A0:78:8E:9E:AA;
   fixed-address 192.168.1.4;
}
```

Esempio 18-5. Indirizzo IP statico con DHCP

Suggerimento

Potete usare il file campione di configurazione in Red Hat Linux 9 come il punto iniziale a cui aggiungere le opzioni di configurazione personalizzata. Copiatelo nella posizione appropriata con il comando

```
cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf
```

(dove <*numero-versione*> è la versione DHCP in uso).

Per un elenco completo di dichiarazioni per le opzioni e delle loro funzioni, fate riferimento alla pagina man dhcp-options.

18.2.2. Database degli affitti

Sul server DHCP, il file `/var/lib/dhcp/dhcpd.leases` archivia la database degli affitti del client DHCP. Si consiglia di non modificare il file manualmente. Le informazioni sull'affitto DHCP per ogni indirizzo IP assegnato di recente sono archiviate automaticamente nel database degli affitti. Le informazioni includono la lunghezza dell'affitto, a chi è stato assegnato l'indirizzo IP, l'inizio e la chiusura delle date di affitto e l'indirizzo MAC della scheda di interfaccia di rete usata per reperire l'affitto.

Tutti gli orari della database degli affitti fanno riferimento al Greenwich Mean Time (GMT), non all'ora locale.

La database degli affitti viene ricreata ogni tanto cosichè no diventa troppo lungo. Prima, tutti gli affitti esistenti vengono salvati in una databasetemporanea degli affitti. Il file `dhcpd.leases` viene rinominato `dhcpd.leases~` e la database temporanea degli affitti viene scritta nel file `dhcpd.leases`.

Quando la database degli affitti viene rinominata come file di backup, questo potrebbe causare il demone DHCP ad essere eliminato o potrebbe bloccare il sistema, se il nuovo file non viene creato prima. In questo caso, non vi è il file `dhcpd.leases`, che è richiesto per avviare il servizio. Se ciò si verifica, non create un nuovo file degli affitti, altrimenti tutti gli affitti precedenti andranno persi causando molti problemi. La soluzione corretta è rinominare il file di backup `dhcpd.leases~` come `dhcpd.leases`, quindi avviare il demone.

18.2.3. Avvio e arresto del server

Importante

Prima di avviare il server DHCP per la prima volta, assicuratevi dell'esistenza del file `dhcpd.leases`, in mancanza del quale l'operazione fallirà. Utilizzate il comando `touch /var/lib/dhcp/dhcpd.leases` per creare il file prima di avviare il servizio.

Per avviare il servizio DHCP, utilizzate il comando `/sbin/service dhcpd start`. Per arrestarlo, utilizzate invece il comando `/sbin/service dhcpd stop`. Se desiderate che il demone si avvii automaticamente durante l'avvio, consultate il Capitolo 14 per informazioni sulla gestione dei servizi.

Se disponete di più interfacce di rete per il sistema, ma desiderate che il server DHCP si avvii unicamente su un'interfaccia, potete configurare il server DHCP a tale scopo. Nel file `/etc/sysconfig/dhcpd`, aggiungete il nome dell'interfaccia all'elenco `DHCPDARGS`:

```
# Command line options here
DHCPDARGS=eth0
```

Si rivela utile se avete un firewall con due schede di rete. Una scheda può essere configurata come client DHCP per recuperare un indirizzo IP in Internet, l'altra come server DHCP per la rete interna protetta dal firewall. Se specificate solo la scheda di rete collegata alla rete interna, otterrete un sistema più sicuro in quanto gli utenti non possono collegarsi al demone tramite Internet.

Altre opzioni della linea di comando possono essere specificate nel file `/etc/sysconfig/dhcpd` e includono:

- `-p <numero-porta>` — specificate il numero di porta udp sulla quale il dhcpd deve stare in ascolto. L'impostazione di default è la porta 67. Il server DHCP trasmette le risposte ai client DHCP a un numero di porta superiore di un valore a quello specificato per la porta udp. Per esempio, se si accetta la porta 67, il server si mette in ascolto sulla porta 67 per raccogliere le richieste e le risposte per il client sulla porta 68. Se si specifica una porta e si utilizza il relay agent DHCP, occorre specificare la stessa porta sulla quale il relay agent DHCP è in ascolto. Per maggiori dettagli consultate la Sezione 18.2.4.
- `-f` — eseguite il demone come processo in primo piano. Questo è usato soprattutto per operazioni di debug.
- `-d` — registrate il demone del server DHCP sul descrittore di errori standard. Questo è usato soprattutto per operazioni di debug. Se non è specificato, il log viene scritto nel file `/var/log/messages`.
- `-cf nomefile` — specificate la posizione del file di configurazione. La posizione di default è `/etc/dhcpd.conf`.

- `-lf` *`nomefile`* specificate la posizione della database degli affitti. Se la database esiste già, è importante che lo stesso file venga utilizzato a ogni avvio del server DHCP. Si consiglia di usare questa opzione solo per operazioni di debug su macchine non destinate alla produzione. La posizione di default è `/var/lib/dhcp/dhcpd.leases`.
- `-q` — non stampate l'intero messaggio di copyright quando avviate il demone.

18.2.4. Relay Agent DHCP

Il Relay Agent DHCP (`dhcrelay`) vi consente di comunicare le richieste DHCP e BOOTP provenienti da una sottorete senza server DHCP a uno o più server DHCP su altre sottoreti.

Quando un client DHCP richiede delle informazioni, il Relay Agent inoltra la richiesta all'elenco di server DHCP specificati all'avvio del Relay Agent DHCP. Quando un server DHCP invia una risposta, viene eseguito il broadcast o l'unicast sulla rete che ha inviato la richiesta originale.

Il Relay Agent DHCP ascolta le richieste DHCP su tutte le interfacce a meno che non vengano specificate le interfacce nel file `/etc/sysconfig/dhcrelay` con la direttiva `INTERFACES`.

Per avviare il Relay Agent DHCP, utilizzate il comando `service dhcrelay start`.

18.3. Configurazione di un client DHCP

La prima fase per configurare un client DHCP è assicurarsi che il kernel riconosca la scheda di rete. La maggior parte delle schede è riconosciuta durante il processo d'installazione e il sistema è configurato per utilizzare il modulo kernel corretto per la scheda. Se installate una scheda dopo l'installazione, **Kudzu** [1] dopo il riconoscimento, vi chiederà di configurare il modulo kernel corrispondente. Assicuratevi di controllare l'Elenco di Compatibilità Hardware di Red Hat Linux disponibile su http://hardware.redhat.com/hcl/. Se la scheda di rete non è configurata dal programma d'installazione o **Kudzu** e voi sapete quale modulo kernel caricare, fate riferimento al Capitolo 31 per dettagli sul caricamento dei moduli kernel.

Per configurare manualmente un client DHCP, è necessario modificare il file `/etc/sysconfig/network` e abilitare il file di networking e configurazione per ciascun dispositivo di rete nella directory `/etc/sysconfig/network-scripts`. In questa directory ogni dispositivo avrà il corrispondente file di configurazione chiamato `ifcfg-eth0` dove `eth0` è il nome del dispositivo di rete.

Il file `/etc/sysconfig/network` dovrebbe contenere la riga seguente:

```
NETWORKING=yes
```

Questo file potrebbe fornirvi maggiori informazioni. La variabile `NETWORKING` deve essere impostata su `yes` per attivare le operazioni di rete all'avvio.

Il file `/etc/sysconfig/network-scripts/ifcfg-eth0` deve contenere le seguenti righe:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Sarà necessario un file di configurazione per ogni dispositivo che desiderate configurare per usare il DHCP.

1. **Kudzu** è uno strumento di verifica hardware al momento dell'avvio del sistema per determinare quale hardware è stato aggiunto o rimosso dal sistema.

Se preferite un interfaccia grafica per configurare il client DHCP, consultate Capitolo 12 per dettagli sull'uso del **Strumento di amministrazione di rete** per configurare un interfaccia di rete con DHCP.

18.4. Risorse aggiuntive

Per le opzioni di configurazione non trattate in questa sede, si suggerisce di consultare le seguenti risorse.

18.4.1. Documentazione installata

- Pagina man di `dhcpd` — descrive il funzionamento del demone DHCP.
- Pagina man di `dhcpd.conf` — spiega come configurare il file di configurazione di DHCP con alcuni esempi.
- Pagina man di `dhcpd.leases` — spiega come configurare il file degli affitti DHCP con alcuni esempi.
- Pagina man di `dhcp-options` — spiega la sintassi per dichiarare le opzioni DHCP in `dhcpd.conf` con alcuni esempi.
- Pagina man di `dhcrelay` — spiega il Relay Agent DHCP e le opzioni di configurazione.

Capitolo 19.

Configurazione di Server HTTP Apache

In Red Hat Linux 7.3, il Server HTTP Apache è stato aggiornato alla versione 2.0, la quale usa opzioni di configurazioni diverse. Iniziando anche con Red Hat Linux 7.3, il pacchetto é stato rinominato `httpd`. Se desiderate avere istruzioni su come migrare manualmente un file di configurazione già esistente, consultate la guida relativa alla migrazione in `/usr/share/doc/httpd-<ver>/migration.html` oppure la *Red Hat Linux Reference Guide* per maggiori informazioni.

Se avete configurato il Server HTTP Apache con il **Strumento di configurazione di HTTP** nelle precedenti versioni di Red Hat Linux e avete poi eseguito un aggiornamento, potete utilizzare la medesima applicazione per migrare il file di configurazione nel nuovo formato per la versione 2.0. Lanciate il **Strumento di configurazione di HTTP**, modificate la configurazione in base alle vostre esigenze e poi salvate le modifiche attuate. Il file di configurazione così salvato sarà quindi compatibile con la versione 2.0.

Il **Strumento di configurazione di HTTP** vi consente di configurare il file di configurazione `/etc/httpd/conf/httpd.conf` per il Server HTTP Apache. Poiché i vecchi file di configurazione `srm.conf` o `access.conf` non vengono più utilizzati, lasciateli vuoti. Tramite l'interfaccia grafica, potete configurare direttive quali host virtuali, attributi di login e numero massimo di connessioni.

Soltanto i moduli contenuti nella confezione di Red Hat Linux possono essere configurati mediante il **Strumento di configurazione di HTTP**. Eventuali moduli aggiuntivi installati non possono essere configurati utilizzando questo tool.

Per poter usare il **Strumento di configurazione di HTTP**, i pacchetti RPM `redhat-config-httpd` e `httpd` devono essere installati. Viene anche richiesto il sistema X Window e l'accesso come root. Per avviare l'applicazione, selezionate il **Pulsante menu principale Impostazioni Server => Server HTTP** oppure digitate il comando `redhat-config-httpd` al prompt della shell (per esempio, su un terminale XTerm o GNOME).

Attenzione

Se desiderate utilizzare questo tool, non modificate manualmente il file di configurazione `/etc/httpd/conf/httpd.conf`. **Strumento di configurazione di HTTP** crea questo file dopo che avete salvato le modifiche e siete usciti dal programma. Se desiderate aggiungere moduli o opzioni di configurazione non disponibili con **Strumento di configurazione di HTTP**, non potrete utilizzare questo tool.

Per configurare il Server HTTP Apache mediante il **Strumento di configurazione di HTTP** è sufficiente eseguire quanto segue:

1. Configurate le impostazioni di base nella linguetta **Main**.
2. Fate clic sulla linguetta **Virtual Hosts** e configurate le impostazioni di default.
3. Nella linguetta **Host virtuali**, configurate l'host virtuale predefinito (Default Virtual Host).
4. Se desiderate servire più URL o host virtuali, aggiungete altri host virtuali.
5. Configurate le impostazioni del server nella linguetta **Server**.
6. Configurate le impostazioni di connessione sotto la linguetta **Ottimizzazione delle prestazioni**.
7. Copiate tutti i file necessari nelle directory `DocumentRoot` e `cgi-bin`.

8. Uscite dall'applicazione e selezionate si per salvare le vostre impostazioni.

19.1. Impostazioni di base

Utilizzate la linguetta **Main** per configurare le impostazioni di base del server.

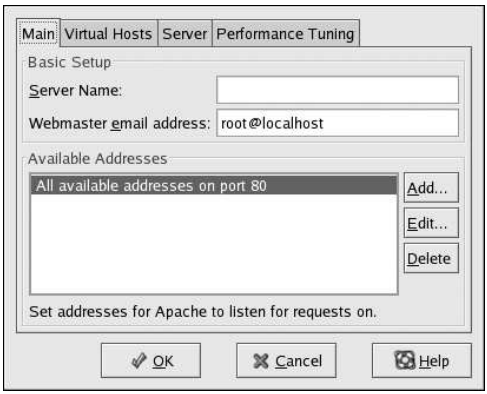

Figura 19-1. Impostazioni di base

Digitate un nome di dominio completo che vi sia consentito usare nell'area di testo **Nome del server**. Questa opzione corrisponde alla direttiva `ServerName` contenuta in `httpd.conf`. La direttiva `Nome del server` imposta l'hostname del server Web e serve per creare URL di reindirizzamento. Se non definite alcun nome per il server, il server Web cercherà di risolverlo sulla base dell'indirizzo IP o dal sistema. Il nome del server non deve necessariamente essere il nome di dominio risolto dall'indirizzo IP del server. Per esempio, potete impostare il nome del server come www.example.com se il nome DNS effettivo del vostro server è foo.example.com.

Inserite l'indirizzo email dell'amministratore del server nell'area di testo **Webmaster email address**. Questa opzione corrisponde alla direttiva `ServerAdmin` contenuta in `httpd.conf`. Se configurate le pagine di errore del server in modo che contengano un determinato indirizzo email, tale indirizzo sarà a disposizione degli utenti per segnalare eventuali problemi all'amministratore del server. Il valore predefinito è root@localhost.

Utilizzate l'area **Indirizzi disponibili** per determinare le porte sulle quali il server accetterà le richieste in entrata. Questa opzione corrisponde alla direttiva `Listen` contenuta in `httpd.conf`. Per default, Red Hat configura il Server HTTP Apache in modo che resti in ascolto sulla porta 80 per le comunicazioni Web non sicure.

Fate clic su **Aggiungi** per definire delle porte aggiuntive sulle quali il server accetterà le richieste. Comparirà una finestra come quella mostrata nella Figura 19-2. A questo punto selezionate l'opzione **Ascolto di tutti gli indirizzi** per far passare tutti gli indirizzi IP dalla porta definita oppure specificate nel campo **Indirizzo** un indirizzo IP dal quale il server accetterà le connessioni. Specificatene uno solo per ogni numero di porta. Se desiderate specificare più di un indirizzo IP per una medisima porta, create una voce per ogni singolo indirizzo IP. Se possibile, utilizzate un indirizzo IP al posto di un nome di dominio onde evitare che un lookup DNS possa fallire. Visitate il sito http://httpd.apache.org/docs-2.0/dns-caveats.html">http://httpd.apache.org/docs-2.0/dns-caveats.html per reperire maggiori informazioni su questioni relative a DNS e Apache (*Questioni inerenti DNS e Apache*).

Inserire un asterisco(*) nel campo **Indirizzo** equivale a selezionare l'opzione **Ascolto di tutti gli indirizzi**. Se fate clic su **Modifica** compare la stessa finestra di **Aggiungi** (cambiano solo i campi relativi all voce selezionata). Per cancellare una voce, selezionatela e fate clic su **Cancella**.

Suggerimento

Se impostate il server in modo che resti in ascolto su una porta inferiore alla 1024, dovete collegarvi come root per avviarlo. Per le porte 1024 e superiori, `httpd` può essere avviato da utenti regolari.

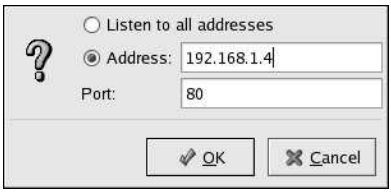

Figura 19-2. Indirizzi disponibili

19.2. Impostazioni predefinite

Dopo aver definito **Nome del server**, **Indirizzo email del Webmaster** e **Indirizzi disponibili**, fate clic sulla linguetta **Host virtuali** e poi su **Modifica impostazioni di Default**. Apparirà la finestra mostrata nella Figura 19-3, nella quale potrete configurare le impostazioni di default per il vostro server Web. Se aggiungete un host virtuale, le impostazioni che configurate per tale host hanno la priorità. Per le direttive non definite nell'ambito delle impostazioni dell'host virtuale viene utilizzato il valore predefinito.

19.2.1. Configurazione del sito

I valori predefiniti per **Elenco di ricerca delle pagine della directory** e **Pagine di errore** sono indicati per quasi tutti i server. Non modificatele se non siete sicuri di saperlo fare.

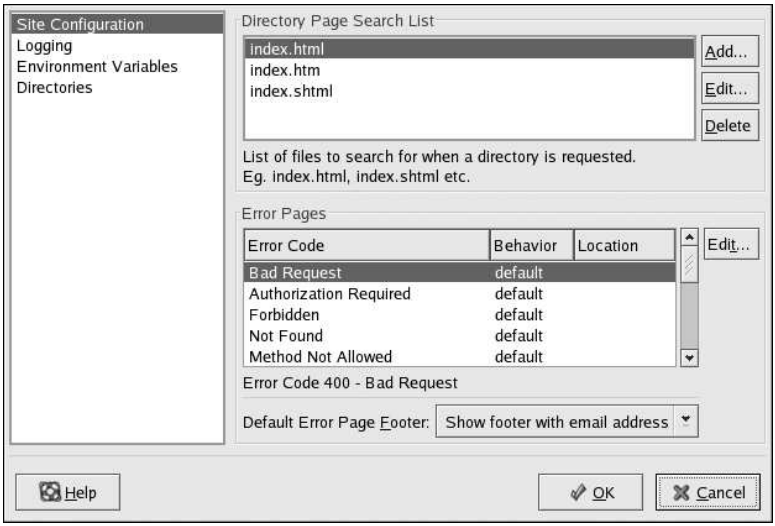

Figura 19-3. Configurazione del sito

Le voci elencate in **Elenco di ricerca delle pagine della directory** definiscono la direttiva `DirectoryIndex`. La pagina `DirectoryIndex` è quella servita dal server per default quando un utente richiede l'indice di una directory specificano uno slash di inoltro al termine del nome della directory.

Per esempio, quando un utente richiede la pagina http://*`www.example.com/questa_directory/`*, accederà alla pagina `DirectoryIndex` (se esiste) o a un elenco di directory generato dal server. Il server cerca uno dei file elencati nella direttiva `DirectoryIndex` e restituisce il primo che trova. Se non trova nemmeno uno dei file e per quella directory è impostata l'opzione `Options Indexes`, il server genera un elenco in formato HTML delle sottodirectory e dei file contenuti nella directory e lo restituisce all'utente.

Utilizzate la sezione **Codice d'errore** per configurare il Server HTTP Apache in modo che, in caso si verifichino problemi o errori, reindirizzi il client a una URL locale o esterna. Questa opzione corrisponde alla direttiva `ErrorDocument`. Qualora si verificassero problemi o errori nel momento in cui un client cerca di connettersi al Server HTTP Apache, per default viene visualizzato un breve messaggio di errore come quello mostrato nella colonna **Codice d'errore**. Per modificare questa configurazione di default, selezionate il codice di errore e fate clic su **Modifica**. Selezionate **Default** per visualizzare il messaggio di errore predefinito. Scegliete **URL** per reindirizzare il client a una URL esterna e inserite una URL completa, con tanto di http://, nel campo **Posizione**. Scegliete **File** per reindirizzare il client a una URL locale e inserite la posizione di un file nel documento root per il server Web. La posizione del file deve iniziare con uno slash (/) ed essere in relazione con il documento root.

Per esempio, per reindirizzare un codice di errore 404 Not Found a una pagina web che avete creato in un file di nome `404.html`, copiate `404.html` in *`DocumentRoot`*`/errors/404.html`. In tal caso, *`DocumentRoot`* è la directory del documento root da voi definita (quella di default è `/var/www/html`). A questo punto, scegliete **File** come Behavior da assegnare al codice di errore **404 - Non trovato** e inserite `/errors/404.html` come **Posizione**.

Dal menu **Pié di _pagina di default della pagina di errore**, potete scegliere una delle opzioni seguentioptions:

- **Mostra pié di pagina con indirizzo e-mail** — visualizza il footer predefinito posto in fondo alle pagine di errore, insieme all'indirizzo email del webmaster specificato dalla direttiva `ServerAdmin`. Per informazioni su come configurare la direttiva `ServerAdmin`, consultate la la Sezione 19.3.1.1.
- **Mostra pié di pagina** — visualizza semplicemente il footer predefinito in fondo alle pagine di errore.
- **Nessun pié di pagina** — Non visualizza alcun footer in fondo alle pagine di errore.

19.2.2. Logging

Per default, il server salva il log di trasferimento nel file `/var/log/httpd/access_log` e il log di errore nel file `/var/log/httpd/error_log`.

Il log di trasferimento contiene un elenco di tutti i tentativi di accesso al server Web. Registra l'indirizzo IP del client che sta tentando di connettersi, la data e l'ora del tentativo e a quale file del server Web sta cercando di accedere. Stabilite il nome del percorso e il file in cui volete salvare tali informazioni. Se il percorso e il nome del file non iniziano con uno slash (/), il percorso è dipendente dalla directory root del server in base alla configurazione. Questa opzione corrisponde alla direttiva `TransferLog`.

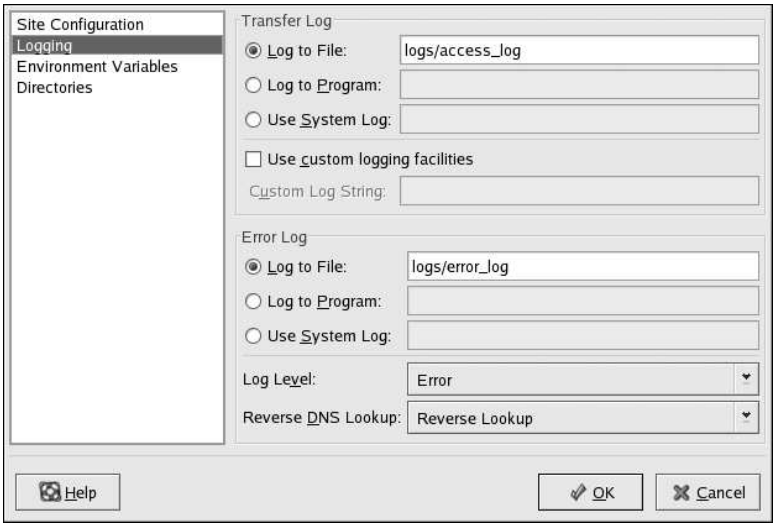

Figura 19-4. Logging

Potete configurare un formato convenzionale per il log selezionando **Utilizza servizi di accesso personalizzati** e inserendo una stringa per definire un log convenzionale nel campo **Stringa di registrazione personalizzata**. In questo modo si configura la direttiva `LogFormat`. Per maggiori dettagli sul formato di questa direttiva, visitate l'indirizzo http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formats.

Il log di errore contiene un elenco di tutti gli errori che si verificano in relazione al server. Inserite il nome del percorso e del file in cui desiderate salvare tali informazioni. Se il percorso e il nome del

file non sono preceduti da uno slash (/), il percorso è dipendente dalla directory root del server in base alla configurazione. Questa opzione corrisponde alla direttiva `ErrorLog`.

Utilizzate il menu **Livello di registrazione** per impostare il grado di verbosità dei messaggi contenuti nei log di errore. Può essere impostato (da meno verboso a più verboso) per le voci "emerg, alert, crit, error, warn, notice, info o debug". Questa opzione corrisponde alla direttiva `LogLevel`.

Il valore scelto nel menu **Lookup DNS inverso** definisce la direttiva `HostnameLookups`. Scegliendo **No Reverse Lookup** si imposta il valore su off, mentre scegliendo **Lookup inverso** lo si imposta su on. Se invece si sceglie **Doppio Lookup inverso** il valore viene impostato su double.

Se scegliete **Lookup inverso**, il vostro server risolve automaticamente l'indirizzo IP per ogni connessione che richieda un documento dal vostro server Web. Risolvere l'indirizzo IP significa che il vostro server eseguira una o più connessioni al DNS per scoprire l'hostname che corrisponde a un determinato indirizzo.

Se selezionate **Doppio Lookup inverso**, il server eseguirà un DNS doppio inverso. In altre parole, dopo l'esecuzione di un lookup inverso, sul risultato ottenuto viene eseguito un lookup di inoltro. Almeno uno degli indirizzi IP nel lookup di inoltro deve corrispondere all'indirizzo ottenuto dal primo lookup inverso.

In genere, è consigliabile lasciare questa opzione impostata su **Nessun Lookup inverso**, poiché le richieste DNS comportano un maggior carico di lavoro per il vostro server, con il rischio di rallentarlo. Se il vostro server è particolarmente oberato di lavoro, il tentativo di eseguire lookup inversi o doppi potrebbe avere ripercussioni evidenti.

I lookup inversi e inversi doppi riguardano Internet nel suo complesso. Tutte le connessioni individuali eseguite per cercare ciascun hostname comportano un ulteriore carico di lavoro. Pertanto, per il bene del vostro server Web, è consigliabile lasciare questa opzione impostata su **Nessun Lookup inverso**.

19.2.3. Variabili di ambiente

Il Server HTTP Apache può servirsi del modulo `mod_env` per configurare le variabili di ambiente che vengono trasmesse agli script CGI e alle pagine SSI. Per configurare le direttive per questo modulo, utilizzate la pagina **Variabili di ambiente**.

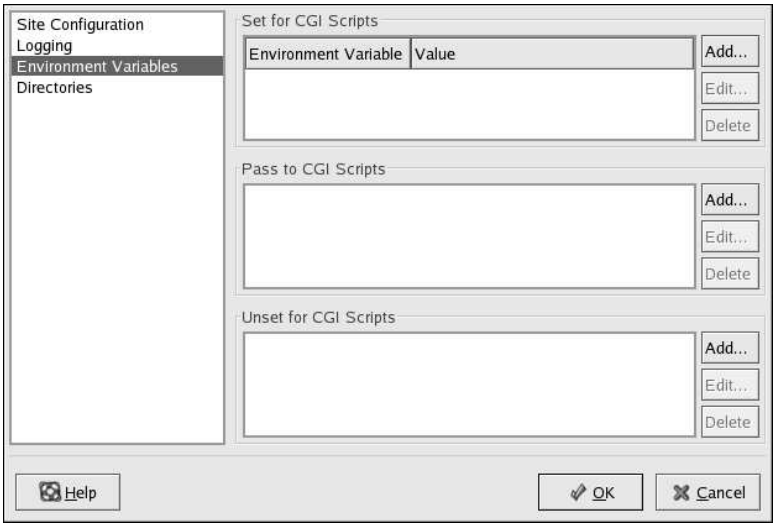

Figura 19-5. Variabili di ambiente

Utilizzate la sezione **Imposta script CGI** per impostare una variabile di ambiente che venga trasmessa agli script CGI e alle pagine SSI. Per esempio, per impostare la variabile di ambiente `MAXNUM` su `50`, fate clic su **Aggiungi** all'interno della sezione **Imposta script CGI** come mostrato nella Figura 19-5; digitate **`MAXNUM`** nel campo di testo **Variabili di ambiente** e **`50`** nel campo **Valore da impostare**. Fate clic su **OK**. La sezione **Imposta script CGI** configura la direttiva `SetEnv`.

Utilizzate la sezione **Passa agli script CGI** per trasmettere agli script CGI il valore di una variabile di ambiente al primo avvio del server. Per vedere questa variabile di ambiente, digitate il comando `env` al prompt di una shell. Fate clic su **Aggiungi** all'interno della sezione **Passa agli script CGI** e inserite il nome della variabile di ambiente nella casella di dialogo che compare. Fate clic su **OK**. La sezione **Passa agli script CGI** configura la direttiva PassEnv directive.

Se desiderate rimuovere una variabile di ambiente in modo che il suo valore non sia trasmesso agli script CGI e alle pagine SSI, utilizzate la sezione **Disattiva script CGI**. Fate clic su **Aggiungi** nella sezione **Disattiva script CGI** e inserite il nome della variabile di ambiente da rimuovere. Fate click su **OK** per aggiungerlo alla lista. Questa opzione corrisponde alla direttiva `UnsetEnv`.

Per modificare qualsiasi di questi valori di ambiente, selezionarlo dalla lista e fare clic sul pulsante **Modifica** corrispondente. Per cancellare qualsiasi entry dalla lista, selezionare la entry e fare clicc sul pulsante **Cancella**

Per saperne di piú sulle variabili di ambiente in Server HTTP Apache, consultate quanto segue:

```
http://httpd.apache.org/docs-2.0/env.html
```

19.2.4. Directory

Utilizzate la pagina **Directory** per configurare le opzioni per directory speficiche. Questa opzione corrisponde alla directory `<Directory>`.

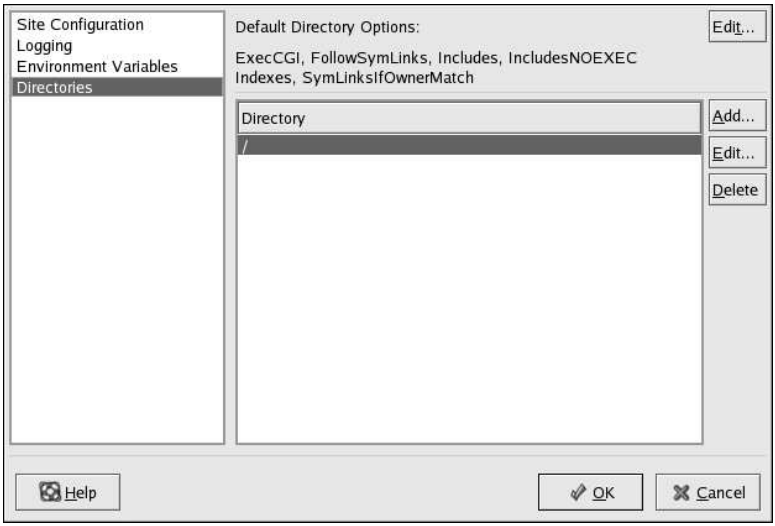

Figura 19-6. Directory

Fate clic su **Modifica** nell'angolo in alto a destra per configurare le **Opzioni directory di default** per tutte le directory non specificate nell'elenco delle **Directory** sottostante. Le opzioni che scegliete sono elencante come Options directive all'interno della direttiva `<Directory>`. Potete configurare le opzioni seguenti:

- **ExecCGI** — consente l'esecuzione di script CGI. Se l'opzione non è selezionata gli script CGI non si possono eseguire.
- **FollowSymLinks** — permette di seguire link simboloci.
- **Includes** — permette l'utilizzo di include "server-side".
- **IncludesNOEXEC** — permette l'utilizzo di include server-side, ma disattiva i comandi `#exec` e `#include` negli script CGI.
- **Indexes** — visualizza un elenco formattato del contenuto della directory, qualora non esista alcun `DirectoryIndex` (come per esempio `index.html`) nella directory in questione.
- **Multiview** — supporta visualizzazioni multiple di contenuti prestabiliti; questa opzione è disattivata per default.
- **SymLinksIfOwnerMatch** — segue solo link simbolici qualora il proprietario del file o directory richiesti coincida con quello del link.

Per specificare opzioni per determinate directory, fate clic su **Aggiungi** accanto alla casella **Directory**. Compare la finestra mostrata nella Figura 19-7. Inserite la directory da configurare nel campo di testo **Directory** posto sul fondo della finestra. Selezionate le opzioni nell'elenco di destra e configurate la direttiva `Order` con le opzioni poste sul lato sinistro. La direttiva `Order` controlla l'ordine con cui le direttive di allow e deny vengono prese in esame. Nei campi di testo **Consenti host da** e **Nega host da** potete specificare una delle opzioni seguenti:

- Permettere a tutti gli host — digitate **`tutti`** per consentire l'accesso a tutti gli host.
- Nome del dominio parziale — consente a tutti gli host il cui nome corrisponde o termina con la stringa specificata.

- Indirizzo IP esteso — consente l'accesso a un indirizzo IP specifico.
- Una sottorete — come per esempio **`192.168.1.0/255.255.255.0`**
- Una specificazione CIDR per la rete — come per esempio **`10.3.0.0/16`**

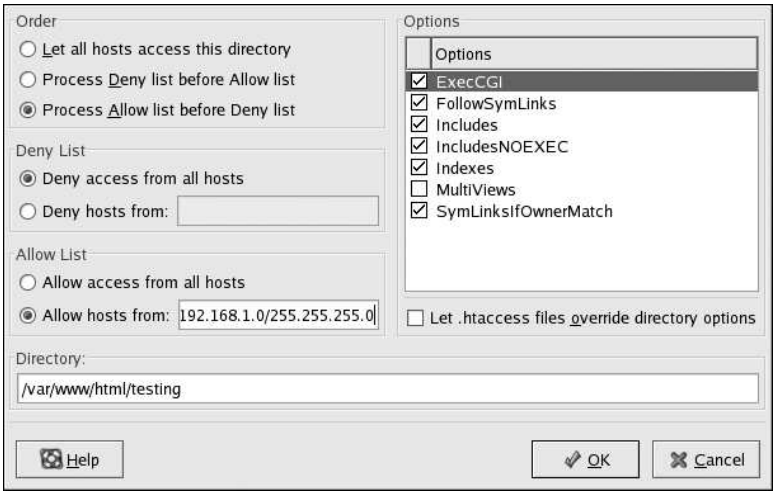

Figura 19-7. Impostazioni di directory

Selezionando **opzioni di directory per la sovrascrittura dei file Let .htaccess**, le direttive contenute nel file `.htaccess` hanno la priorità.

19.3. Impostazioni per gli host virtuali

Potete utilizzare il **Strumento di configurazione di HTTP** per configurare host virtuali. Gli host virtuali vi consento di gestire differenti server per differenti indirizzi IP, nomi di host o porte sulla stessa macchina. Per esempio, potete eseguire i siti Web http://www.example.com e http://www.anotherexample.com sullo stesso server Web utilizzando host virtuali. Questa opzione corrisponde alla direttiva <VirtualHost> directive per l'host virtuale predefinito e host virtuali basati su IP. Corrisponde alla direttiva <`NameVirtualHost`> per un host virtuale basato su nome.

Le direttive impostate per un host virtuale si appliccano soltanto a quel particolare host virtuale. Se una direttiva viene estesa a tutti i server utilizzando il pulsante **Modifica impostazioni di Default** e non viene definita all'interno delle impostazioni relative agli host virtuali, viene utilizzata l'impostazione di default. Per esempio, potete definire un **indirizzo email del Webmaster** nella linguetta **Principale** e non definire invece indirizzi email singoli per ciascun host virtuale.

Strumento di configurazione di HTTP comprende un host virtuale di default, come mostrato nella Figura 19-8.

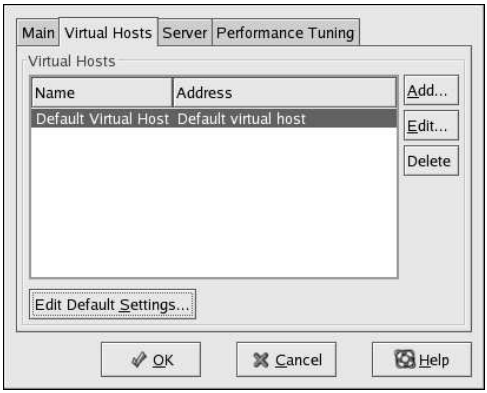

Figura 19-8. Host virtuali

http://httpd.apache.org/docs-2.0/vhosts/ e la documentazione su Server HTTP Apache presente sulla vostra macchina vi fornirà ulteriori informazioni in merito agli host virtuali.

19.3.1. Come aggiungere e modificare un host virtuale

Per aggiungere un host virtuale, fate clic sulla linguetta **Host virtuali** e poi su **Aggiungi**. Potete anche modificare un host virtuale selezionandolo nell'elenco e facendo clic su **Modifica**.

19.3.1.1. Opzioni generali

Le impostazioni delle **Opzioni generali** si applicano solo all'host virtuale che state configurando. Impostate il nome dell'host virtuale nell'area di testo **Nome dell'host virtuale**. Questo nome viene utilizzato dal **Strumento di configurazione di HTTP** per contraddistinguere i vari host virtuali.

Impostate il valore della **Directory del documento root** contenente il documento root (per esempio index.html) per l'host virtuale. Questa opzione corrisponde alla direttiva `DocumentRoot` all'interno della direttiva `VirtualHost`. Nelle versioni precedenti di Red Hat Linux 7, il Server HTTP Apache fornito nella confezione utilizzava `/home/httpd/html` come `DocumentRoot`. In Red Hat Linux 9, invece, il `DocumentRoot` predefinito è `/var/www/html`.

L'**indirizzo email del Webmaster** corrisponde alla direttiva `ServerAdmin` all'interno della direttiva `VirtualHost`. Tale indirizzo email viene utilizzato nel footer delle pagine di errore qualora abbiate scelto di mostrare, in queste pagine, un footer con indirizzo email.

Nella sezione **Informazioni dell'Host**, selezionate **Host virtuale di Default**, **host virtuale basato su IP** o **host virtuale basato sul nome**.

Host virtuale di Default

È consigliabile configurare un solo host virtuale (ricordate che c'è un'impostazione predefinita). Le impostazioni per l'host virtuale vengono utilizzate quando l'indirizzo IP richiesto non è esplicitamente elencato in un altro host virtuale. Se non ci c'è alcun host virtuale definito, vengono utilizzate le impostazioni del server principale.

host virtuale basato su IP

Se selezionate **host virtuale basato su IP**, compare una finestra per configurare la direttiva <VirtualHost> sulla base dell'indirizzo IP del server. Specificate tale indirizzo IP nel campo **Indirizzo IP**. Per specificare più di un indirizzo IP, separate ciascun indirizzo con degli spazi.

Per specificare una porta, utilizzate la sintass *Porta: indirizzo IP*. Utilizzate :* per configurare tutte le porte per l'indirizzo IP. Specificate il nome dell'host per l'host virtuale nel campo **Nome host del Server**.

Host virtuale basato sul nome

Se selezionate **Host virtuale basato sul nome**, compare una finestra per configurare la direttiva `NameVirtualHost` sulla base del nome dell'host del server. Specificate l'indirizzo IP nel campo **Indirizzo IP**. Per specificare più di un indirizzo IP, separate ciascun indirizzo con degli spazi. Per specificare una porta, utilizzate la sintassi *Porta: Indirizzo IP*. Utilizzate :* per configurare tutte le porte per l'indirizzo IP. Specificate il nome dell'host per l'host virtuale nel campo **Nome host del Server**. Nella sezione **Alias**, fate clic **Aggiungi** per aggiungere un alias per il nome dell'host. Aggiungendo un alias qui, significa aggiungere una direttiva `ServerAlias` all'interno della direttiva `NameVirtualHost`.

19.3.1.2. SSL

Nota Bene

Non potete utilizzare host virtuali basati su nomi con SSL, perché l'handshake di SSL (il momento in cui il browser accetta la certificazione del server Web sicuro) avviene prima della richiesta HTTP che identifica il nome appropriato dell'host virtuale. Se volete utilizzare host virtuali basati su nome, sappiate che funzioneranno solo con il vostro server Web non sicuro.

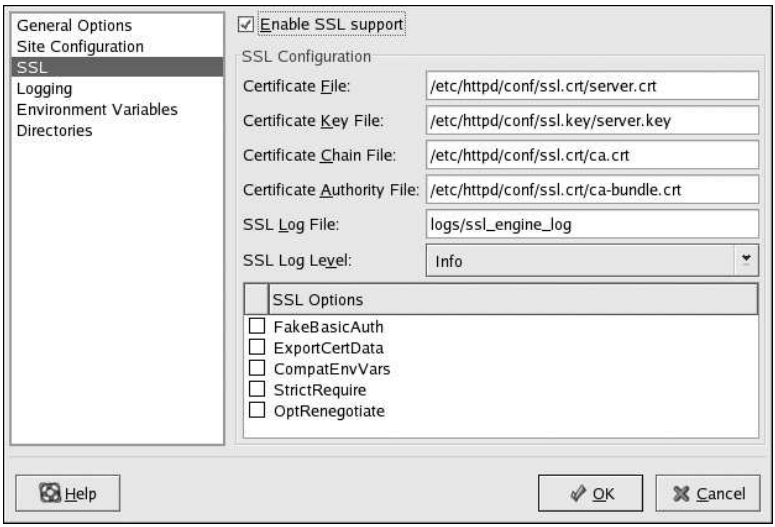

Figura 19-9. Supporto a SSL

Se un Server HTTP Apache non è configurato con il supporto a SSL, le comunicazioni tra un Server HTTP Apache e i suoi client non sono cifrate, il che può andare ben per siti Web privi di informazioni

personali o confidenziali. Per esempio, un sito Open Source che distribuisce software gratuito e documentazione non necessita di comunicazioni sicure. Al contrario, i siti Web connessi al commercio elettronico che richiedono la trasmissione di informazioni relative a carte di credito devono servirsi del supporto a SSL di Apache per cifrare gli scambi di comunicazioni. Abilitare tale supporto rende possibile utilizzare il modulo di sicurezza `mod_ssl`. Per abilitarlo mediante **Strumento di configurazione di HTTP** dovete consentire l'accesso attraverso la porta 443 sotto la linguetta **Principale => Indirizzi disponibili**. Per ulteriori dettagli, consultate la la Sezione 19.1. Successivamente selezionate il nome dell'host virtuale nella linguetta **Host virtuali**, fate clic su **Modifica**, selezionate **SSL** dal menu di sinistra e spuntate l'opzione **Supporto SSL abilitato** come mostrato nella Figura 19-9. La sezione **Configurazione SSL** è preconfigurata con la certificazione digitale dummy. La certificazione digitale fornisce l'autenticazione per il vostro server Web sicuro e identifica il server sicuro per i browser dei client Web. È necessario che acquistiate la vostra certificazione digitale personale. Non utilizzate la certificazione dummy fornita con Red Hat Linux per il vostro sito Web. Per maggiori dettagli su come acquistare una certificazione digitale approvata da una CA, consultate il Capitolo 20.

19.3.1.3. Opzioni aggiuntive per l'host virtuale

Le opzioni **Configurazioni del sito**, **Variabili di ambiente** e **Directory** per gli host virtuali sono le stesse direttive che avete impostato facendo clic su **Modifica impostazioni di default**, solo che le opzioni impostate qui si applicano agli host virtuali che state configurando. Per maggiori dettagli su queste opzioni consultate la la Sezione 19.2.

19.4. Impostazioni del server

La linguetta **Server** vi permette di configurare le impostazioni di base per il server. Le ipostazioni di default per queste opzioni sono adeguate per la maggior parte delle situazioni.

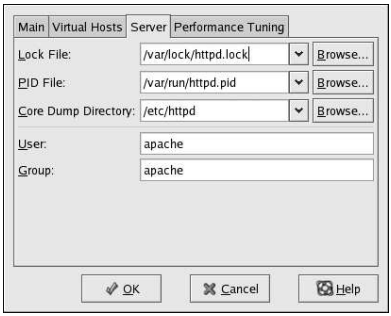

Figura 19-10. Configurazione del server

Il valore **Blocca file** corrisponde alla direttiva `LockFile`. Questa direttiva imposta il percorso verso il lockfile utilizzato quando il server viene compilato con USE_FCNTL_SERIALIZED_ACCEPT o USE_FLOCK_SERIALIZED_ACCEPT. Deve essere salvata sul disco locale ed è consigliabile lasciare impostato il valore predefinito, a meno che la directory `logs` si trovi su una condivisione NFS. In tal caso, il valore predefinito dovrebbe essere spostato sul disco locale in una directory che sia leggibile solo dagli utenti collegati come root.

Il valore **File PID** corrisponde alla direttiva `PidFile`. Tale direttiva imposta il file in cui il server registra il proprio processo ID (pid). Questo file dovrebbe essere leggibile solo da utenti root. Nella maggior parte dei casi, è raccomandabile lasciare impostato il valore predefinito.

Il valore della **Directory Core Dump** corrisponde alla direttiva `CoreDumpDirectory`. Il Server HTTP Apache cerca di passare a questa directory prima di eseguire un core dumping. Il valore di default è il `ServerRoot`. Tuttavia, se l'utente non può eseguire salvataggi in questa directory, non è possibile salvare il core dump. Se volete salvare i core dump sul disco a scopo di debugging, spostate questo valore in una directory su cui l'utente possa operare.

Il valore **Utente** corrisponde alla direttiva `User`. Imposta la userid utilizzata dal server per rispondere alle richieste. Le impostazioni di questo utente determinano l'accesso al server. I file non accessibili da questo utente, non lo saranno neanche per i visitatori del vostro sito Web. Il valore predefinito per `User` è apache.

L'utente deve possedere possedere i privilegi necessari per accedere ai file che dovrebbero essere visibile al mondo esterno. Inoltre, l'utente è il proprietario di tutti i processi CGI generati dal server e non dovrebbe avere il permesso di eseguire codici che non siano intesi a soddisfare le richieste HTTP.

Avvertimento

Se non siete certi di che cosa comporta, non impostate la direttiva `User` come root, poiché tale operazione causerebbe gravi problemi di sicurezza al vostro server Web.

Durante le operazioni di routine, il processo padre `httpd` viene inizialmente eseguito come root, ma poi viene immediatamente passato all'utente apache. Il server deve avviarsi come root perché gli occorre connettersi a una porta inferiore alla 1024. Queste porte sono riservate per l'uso del sistema, in modo che non possano essere utilizzate da utenti non collegati come root. Una volta che il server si è connesso alla sua porta, prima di accettare qualsiasi richiesta di connessione passa il processo all'utente apache.

Il valore **Gruppo** corrisponde alla direttiva `Group`. La direttiva `Gruppo` è simile alla direttiva `User` e imposta il gruppo sotto il quale il server risponderà alle richieste. Il gruppo di default è apache.

19.5. Ottimizzazione delle prestazioni

Fate clic sulla linguetta **Ottimizzazione delle prestazioni** per configurare il numero massimo di processi figli ammessi e le opzioni Server HTTP Apache per le connessioni client. Le impostazioni predefinite per queste opzioni si addicono alla maggior parte delle situazioni. Se le alterate, le prestazioni generali del vostro server Web potrebbero risentirne.

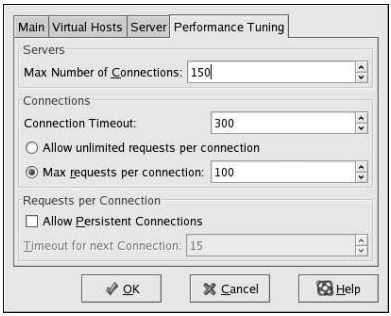

Figura 19-11. Ottimizzazione delle prestazioni

Impostate **Numero massimo di connessioni** sul numero massimo di richieste client che il server dovrà gestire contemporaneamente. Per ciascuna connessione viene creato un processo figlio `httpd`. Dopo che è stato raggiunto il numero massimo di processi, nessuno sarà più in grado di connettersi al server Web fino a quando uno dei processi figli in corso non si libera. Questa opzione corrisponde alla direttiva `MaxClients`.

Sospensione della connessione quantifica, in termini di secondi, l'attesa del server per la ricezione e la trasmissione durante le comunicazione Nello specifico, **Sospensione della connessione** definisce quanto tempo aspetterà il server prima di ricevere una richiesta GET, quanto tempo dovrà attendere prima di ricevere pacchetti TCP su richieste POST o PUT e quanto tempo trascorrerà dal momento in cui degli ACK rispondono ai pacchetti TCP. Per default, **Sospensione della connessione** è impostato su 300 secondi, un valore indicato nella maggior parte delle situazioni. Questa opzione corrisponde alla direttiva `TimeOut`.

Impostate la direttiva **Richieste massime per connessione** sul numero massimo di richieste autorizzate per ciascuna connessione persistente. Il valore di default è 100 e si adatta alla maggior parte delle situazioni. Questa opzione corrisponde alla direttiva `MaxRequestsPerChild`.

Se selezionate l'opzione **Permetti richieste illimitate per connessione**, la direttiva `MaxKeepAlive-Requests` viene impostata su 0 e sarà autorizzato un numero illimitato di richieste.

Se deselezionate l'opzione **Permetti connessioni persistenti**, la diretiva `KeepAlive` viene impostata su "falso". Se invece la selezionate, la direttiva `KeepAlive` viene impostata su "vero" e la direttiva `KeepAliveTimeout` sul numero stabilito come valore per **Sospensione per la connessione successiva**. Questa direttiva determina il numero di secondi per i quali il server, prima di chiudere la connessione, attenderà una nuova richiesta dopo averne soddisfatta una precedente. Una volta ricevuta la nuova richiesta, viene applicato il valore di **Sospensione della connessione**.

Impostando **Connessioni persistenti** su un valore più alto, si rischia di far rallentare il server, a seconda del numero di utenti che stanno cercando di connettersi. Più è altro il numero, maggiore sarà il numero di processi in attesa di una nuova connessione dall'ultimo client che si è collegato.

19.6. Salvataggio delle impostazioni

Se non volete salvare le vostre impostazioni di configurazione per il Server HTTP Apache, fate clic sul pulsante **Cancella** posto nell'angolo destro in fondo alla finestra del **Strumento di configurazione di HTTP**. Vi verrà richiesto di confermare la vostra decisione. Se fate clic su **Sì** per confermare, le vostre impostazioni non verranno salvate.

Se invece desiderate salvare le vostre impostazioni per il Server HTTP Apache, fate clic sul pulsante **OK** posto nell'angolo destro in fondo alla finestra del **Strumento di configurazione di HTTP**. Comparirà una finestra di dialogo. Se rispondete **Sì**, le vostre impostazioni verranno salvate in

`/etc/httpd/conf/httpd.conf`. Ricordatevi che tale operazione comporta la sovrascrittura del file di configurazione originale.

Se state utilizzando il **Strumento di configurazione di HTTP** per la prima volta, vi comparirà una finestra di dialogo che vi avvisa che il file di configurazione è stato modificato manualmente. Se il **Strumento di configurazione di HTTP** rileva che il file di configurazione `httpd.conf` è stato modificato manualmente, salverà il file modificato come `/etc/httpd/conf/httpd.conf.bak`.

Importante

Dopo aver salvato le impostazioni, è necessario riavviare il demone `httpd` con il comando `service httpd restart`. Per eseguire questo comando dovete essere collegati come root.

19.7. Risorse Aggiuntive

Per saperne di più sul Server HTTP Apache, consultate le risorse seguenti.

19.7.1. Documentazione installata

- Documentazione di Server HTTP Apache — se avete installato il pacchetto `httpd-manual` e il demone Server HTTP Apache (`httpd`) è in esecuzione, potete visualizzare la documentazione relativa a Server HTTP Apache. Aprite un browser Web e andate all'indirizzo http://localhost sul server che ha il Server HTTP Apache in esecuzione. Poi fate clic sul link **Documentazione**.
- `/usr/share/docs/httpd-<versione>` — Il documento *Apache Migration HOWTO* contiene un elenco delle modifiche apportate nel passaggio dalla versione 1.3 alla versione 2.0 e informazioni su come migrare manualmente il file di configurazione.

19.7.2. Siti Web utili

- http://www.apache.org — *La Apache Software Foundation*.
- http://httpd.apache.org/docs-2.0/ — La documentazione di Apache Software Foundation su Server HTTP Apache version 2.0, include la *, Server HTTP Apache Version 2.0 User's Guide*.
- http://localhost/manual/index.html — dopo aver avviato il Server HTTP Apache sul vostro sistema locale,, potete visualizzare la Server HTTP Apache Version 2.0 documentation usando questo URL.
- http://www.redhat.com/support/resources/web_ftp/apache.html — il supporto Red Hat offre una lista aggiornata di link utili
- http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html — Il Red Hat Linux Apache Centralized Knowledgebase compilato da Red Hat.

19.7.3. Libri correlati

- *Apache: The Definitive Guide* di Ben Laurie e Peter Laurie; pubblicato da O'Reilly & Associates, Inc.
- *Red Hat Linux Reference Guide*; Red Hat, Inc. — Questo manuale include istruzioni su come migrare da Server HTTP Apache version 1.3 a Server HTTP Apache version 2.0 manualmente,

maggiori dettagli sulle direttive Server HTTP Apache, e istruzioni su come aggiungere i moduli all'Server HTTP Apache.

Capitolo 20.

Configurazione del server sicuro HTTP Apache

20.1. Introduzione

Questo capitolo offre alcune informazioni di base relative ad Server HTTP Apache con il modulo di sicurezza `mod_ssl` abilitato per utilizzare la libreria e il toolkit OpenSSL. Da questo momento in poi, per riferirci a questo tris di elementi combinati (forniti con Red Hat Linux), useremo server Web sicuro o semplicemente secure server.

Il modulo `mod_ssl` è un modulo di sicurezza per il Server HTTP Apache. Il modulo `mod_ssl` utilizza i tool forniti dall'OpenSSL Project per fornire al Server HTTP Apache nuove importanti caratteristiche — per esempio, la capacità di criptare le comunicazioni. Usando il normale protocollo HTTP, le comunicazioni tra browser e server Web sono inviate in formato testo, con il rischio che vengano intercettate e lette da altri lungo il percorso dal browser al server.

Questo capitolo non rappresenta una documentazione completa in merito a questi programmi. Quando possibile, questa guida potrà indicarvi il posto giusto dove trovare maggiori e più dettagliate informazioni relative ad argomenti specifici.

Qui troverete spiegazioni su come installare i programmi e potrete conoscere le operazioni da compiere per creare una chiave privata e una richiesta di certificazione, per generare il vostro personale certificato "self-signed" e per installare un certificato da utilizzare con il vostro secure server.

Il file di configurazione per `mod_ssl` è posizionato su `/etc/httpd/conf.d/ssl.conf`. Per caricare questo file, e, quindi, per far funzionare `mod_ssl`, occorre che in `/etc/httpd/conf/httpd.conf` ci sia lo statement `Include conf.d/*.conf`. Questo statement é incluso per default nel default Server HTTP Apache del file di configurazione in Red Hat Linux9.

20.2. Panoramica sui pacchetti relativi alla sicurezza

Per abilitare il secure server, dovete aver installato almeno i pacchetti seguenti:

`httpd`

Il pacchetto `httpd` contiene il demone `httpd` completo di utility, file di configurazione, icone, moduli Server HTTP Apache, pagine man e altri file utilizzati dal Server HTTP Apache.

`mod_ssl`

Il pacchetto `mod_ssl` comprende il modulo `mod_ssl`, che fornisce un'eccellente crittografia per il Server HTTP Apache tramite i protocolli SSL (Secure Sockets Layer) e TLS (Transport Layer Security).

`openssl`

Il pacchetto `openssl` contiene il toolkit OpenSSL, che implementa i protocolli SSL e TLS e comprende anche una libreria per scopi generali relativa alla cifratura.

Inoltre, vi sono altri pacchetti inclusi in Red Hat Linux che forniscono determinate funzionalità relative alla sicurezza (le quali, tuttavia, non sono indispensabili per il funzionamento del secure server):

`httpd-devel`

Il pacchetto `httpd-devel` contiene l'Server HTTP Apache, file i file header e le utility di APXS. Dovete avere a disposizione tutto questo se intendete caricare dei moduli extra rispetto a quelli forniti con il prodotto. Consultate la *Red Hat Linux Reference Guide* per maggiori informazioni sul caricamento di moduli sul vostro secure server usando la funzionalità DSO di Apache.

Se non intendete caricare altri moduli nel vostro server Apache, non c'è motivo di installare questo pacchetto.

`httpd-manual`

Il pacchetto `httpd-manual` contiene la *Apache User's Guide* del progetto Apache in formato HTML, disponibile anche sul Web all'indirizzo http://httpd.apache.org/docs-2.0/.

Pacchetti OpenSSH

I pacchetti OpenSSH forniscono una serie di tool per la connettività di rete necessari al collegamento a una macchina remota e all'esecuzione di comandi. I tool OpenSSH criptano tutto il traffico (comprese le password) in modo da evitare intercettazioni, dirottamenti della connessione e altri attacchi alla comunicazione tra il vostro computer e la macchina remota.

Il pacchetto `openssh` comprende i file fondamentali richiesti dai programmi client OpenSSH e dal server OpenSSH. Il pacchetto contiene inoltre `scp`, un valido sostituto per `rcp` (per copiare file tra macchine diverse).

Il pacchetto `openssh-askpass` supporta il display di una finestra di dialogo che richiede una password durante l'utilizzo dell'agente OpenSSH.

Il pacchetto `openssh-askpass-gnome` contiene una finestra di dialogo dell'ambiente grafico di GNOME che viene visualizzata quando i programmi OpenSSH richiedono una password utente. Se state utilizzando GNOME e le utility OpenSSH, installate questo pacchetto.

Il pacchetto `openssh-server` contiene il demone della secure shell `sshd` e i relativi file. Il demone della secure shell si trova sul server della suite OpenSSH e deve essere installato sul vostro host se volete permettere ai client SSH di connettersi alla vostra macchina.

Il pacchetto `openssh-clients` contiene i programmi client necessari per cifrare il traffico di rete durante le connessioni con i server SSH, tra cui: `ssh`, un valido sostituto per `rsh`, `sftp`, un valido sostituto di `ftp` (per il trasferimento dei file tra macchine); e `slogin`, un valido sostituto per `rlogin` (per login remoti) e `telnet` (per comunicare con un altro host tramite il protocollo TELNET).

Per maggiori informazioni su OpenSSH, consultate il Capitolo 15 e visitate il sito Web di OpenSSH all'indirizzo http://www.openssh.com.

`openssl-devel`

Il pacchetto `openssl-devel` contiene le librerie statiche e i file include necessari alla compilazione di applicazioni contenenti un supporto per vari algoritmi e protocolli di cifratura. Installate il pacchetto solamente se sviluppate applicazioni che includono il supporto SSL - il pacchetto non è richiesto per l'utilizzo di SSL.

`stunnel`

Il pacchetto `stunnel` fornisce il wrapper StunnelSSL. Stunnel supporta la cifratura in modalità SSL per le connessioni TCP, quindi fornisce la cifratura per demoni non SSL e protocolli (POP, IMAP, LDAP) senza richiedere modifiche al codice del demone.

Tabella 20-1 visualizza la posizione dei pacchetti del secure server e se i pacchetti sono opzionali per l'installazione di secure server.

Nome del pacchetto	Opzionale?
`httpd`	no
`mod_ssl`	no
`openssl`	no
`httpd-devel`	sì
`httpd-manual`	sì
`openssh`	sì
`openssh-askpass`	sì
`openssh-askpass-gnome`	sì
`openssh-clients`	sì
`openssh-server`	sì
`openssl-devel`	sì
`stunnel`	sì

Tabella 20-1. Pacchetti di sicurezza

20.3. Panoramica su certificati e sicurezza

Il vostro secure server fornisce sicurezza grazie al protocollo Secure Sockets Layer (SSL) e, nella maggior parte dei casi, a un certificato digitale rilasciato da una Certificate Ahthority (CA). Il protocollo SSL gestisce le comunicazioni criptate e la reciproca autenticazione tra i browser e il vostro secure server. Il certificato digitale approvato dalla CA fornisce l'autenticazione per il vostro secure server (la CA appone la sua reputazione alla certificazione della vostra organizzazione). Quando il vostro browser comunica tramite la cifratura SSL, il prefisso `https://` compare all'inizio dell URL nella barra di navigazione.

La codifica dipende dall'utilizzo delle chiavi (consideratele anelli di codifica/decodifica in formato dati). Nella cifratura convenzionale, o simmetrica, entrambe le estremità della transazione hanno la stessa chiave e la usano per decodificare reciprocamente le proprie trasmissioni. Nella crittografia pubblica, o asimmetrica, coesistono due chiavi: una pubblica e una privata. Una persona (o una società) tiene segreta la sua chiave privata e rende nota quella pubblica. I dati codificati con la chiave pubblica possono essere decodificati solo con la chiave privata; viceversa, i dati codificati con la chiave privata possono essere decodificati solo con la chiave pubblica.

Impostando il vostro secure server, utilizzate la cifratura pubblica per creare una chiave pubblica e una chiave privata. Nella maggior parte dei casi, dovete inviare la vostra richiesta di certificazione (inclusa la chiave pubblica), un documento che dimostri l'identità della società e il pagamento a una CA. La CA verifica la richiesta e invia una certificato per il vostro secure server.

Per identificarsi a un browser Web, un secure server utilizza un certificato. Potete generare il certificato da voi (il cosiddetto certificato "self-signed") oppure farvene rilascare uno da una Certificate Authority (CA); quest'ultimo tipo di certificato garantisce che un sito Web sia associato a una determinata società o organizzazione.

Alternativamente, potete creare il vostro certificato "self-signed". Tenete presente, tuttavia, che questo genere di certificati non dovrebbe essere usato in molti ambienti di produzione. I certificati "self-signed" non vengono accettati automaticamente dal browser di un utente — il browser chiede all'utente se vuole accettare il certificato e creare la connessione sicura. Per maggiori informazioni sulle differenze tra certificato "self-signed" e certificati rilasciati da un CA, consultate la Sezione 20.5.

Una volta che avete creato o ottenuto il certificato dal CA di vostra scelta, installatelo nel vostro secure server.

20.4. Utilizzo di chiavi e certificati pre-esistenti

Se disponete già di una chiave e di un certificato (per esempio se state installando il secure server in sostituzione di un altro secure server), potete probabilmente usare la vostra chiave e il vostro certificato. Nelle due situazioni seguenti, non potete usare una chiave né un certificato pre-esistente:

- *Se cambiate l'indirizzo IP o il nome di dominio* — I certificati sono rilasciati per un indirizzo IP e un nome di dominio specifici. Se questi vengono modificati, è necessario ottenere un nuovo certificato.
- *Se avete un certificato rilasciato da VeriSign e state cambiando il software del server* — VeriSign è una CA molto famosa. Se disponete già di un certificato VeriSign rilasciato per un altro scopo, vi sarete chiesti se potete utilizzarlo per il vostro nuovo secure server. Ebbene, non potete farlo, poiché VeriSign rilascia certificati per un software server e una combinazione di indirizzoIP/nome dominio specifici.

  Se modificate uno di questi parametri (per esempio, se avete usato in precedenza un altro secure server e adesso volete usare il server Web sicuro), il certificato VerSign che avete ottenuto per la precedente configurazione non funzionerà con quella nuova e, dunque, dovrete richiederne un altro.

Se avete una chiave e un certificato utilizzabili, non dovete generare una nuova chiave né un nuovo certificato. Tuttavia, potreste dover spostare e rinominare i file che contengono la chiave e il certificato.

Spostate il file della vostra chiave in:

```
/etc/httpd/conf/ssl.key/server.key
```

Spostate il file del vostro certificato in:

```
/etc/httpd/conf/ssl.crt/server.crt
```

Dopo averli spostati, leggete la Sezione 20.9.

Se state effettuando un aggiornamento del Server Web sicuro Red Hat, la vostra chiave (`httpsd.key`) e il vostro certificato (`httpsd.crt`) verranno posizionati in `/etc/httpd/conf/`. Dovete spostarli e rinominarli affinché il secure server possa utilizzarli. Per farlo, usate i comandi seguenti:

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

In seguito avviate il vostro secure server con il comando:

```
/sbin/service httpd start
```

Per un secure server, vi viene richiesta una password. Dopo averla digitata e aver premuto [Invio], il server si avvia.

20.5. Tipi di certificati

Se avete installato il secure server usando il pacchetto offerto da Red Hat Linux, una chiave e un certificato di test vengono generati nelle directory appropriate. Tuttavia, prima di iniziare a usare il secure server, dovete generare la vostra chiave e ottenere un certificato che identifichi correttamente il vostro server.

Per usare il secure server dovete avere una chiave e un certificato — ciò significa che potete generare un certificato "self-signed" oppure acquistare un certificato da una CA. Quali sono le differenze tra questi due certificati?

Un certificato rilasciato da una CA fornisce due importanti aspetti al vostro server:

- I browser (di solito) riconoscono automaticamente il certificato e autorizzano una connessione sicura senza chiedere conferma tramite prompt all'utente.
- Quando una CA rilascia un certificato, essa garantisce l'identità dell'organizzazione che sta fornendo le pagine Web al browser.

Se il vostro secure server è accessibile al grande pubblico, il relativo certificato deve essere rilasciato da una CA affinché le persone che visitano il vostro sito Web siano sicure che il sito appartiene all'organizzazione che dice di possederlo. Prima di firmare un certificato, la CA verifica se l'organizzazione è effettivamente quella che dice di essere.

Molti browser Web che supportano l'SSL hanno un elenco delle CA che rilasciano certificati da loro automaticamente accettati. Se un browser trova un certificato rilasciato da una CA che non fa parte di questo elenco, il browser chiede all'utente se accettare o rifiutare la connessione.

Potete creare un certificato "self-signed" per il vostro secure server, ma sappiate che un certificato di questo tipo non fornisce le stesse funzionalità garantite dai certificati rilasciati dalle CA. Infatti, un certificato "self-signed" non viene automaticamente riconosciuto dai browser degli utenti e non fornisce alcuna garanzia sull'identià dell'organizzazione. Un certificato rilasciato dal CA al contrario, fornisce ad un secure server entrambe queste garanzie. Se il vostro secure server viene usato in un ambiente di produzione, vi servirà molto probabilmente un certificato CA.

Il processo per ottenere un certificato da una CA è abbastanza semplice. Di seguito è riportata una breve spiegazione della procedura da seguire:

1. Create una chiave di cifratura privata e una pubblica.
2. Create un certificato basato sulla chiave pubblica. La richiesta del certificato contiene informazioni sul server e sulla relativa società.
3. Inviate la richiesta e i documenti di identità a una CA. Non vi possiamo indicare quale CA scegliere; la vostra decisione dipende dalle esperienze personali o da quelle di vostri amici o colleghi, o semplicemente da motivi economici.

   Una volta deciso quale CA usare, seguite le istruzioni da essa fornite su come ottenere un certificato.
4. Una volta che la CA ha verificato la vostra identità, e che siete effettivamente chi dite di essere, vi spedisce un ceritificato digitale.
5. Installate il certificato sul vostro secure server, e iniziate a gestire transazioni sicure.

Il primo passo consiste nel creare una chiave, sia per il certificato CA sia per quello "self-signed". Per informazioni su come creare una chiave, consultate la Sezione 20.6.

20.6. Creazione di una chiave

Per generare una chiave occorre collegarsi come utente root.

Anzitutto, con il comando `cd` andate alla directory `/etc/httpd/conf`. Cancellate la chiave e il certificato creati durante l'installazione digitando i comandi seguenti:

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

Adesso dovete creare la vostra chiave random. Passate nella directory `/usr/share/ssl/certs` e digitando il comando:

```
make genkey
```

Il sistema visualizza un messaggio simile a questo:

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

Dovete digitare una password. Per maggiore sicurezza, la password deve contenere almeno otto caratteri, numeri e/o punteggiatura e non essere una parola che abbia senso. Ricordate che la vostra password distingue le lettere minuscole da quelle maiuscole.

Nota Bene

La password deve essere inserita ogni volta che avviate il vostro secure server, perciò non ve la dimenticate!

Vi viene chiesto di ridigitare la password per verificare che sia corretta. Dopodiché viene creato un file contenente la chiave, chiamato `/etc/httpd/conf/ssl.key/server.key`.

Se non volete digitare la password ogni volta che avviate il secure server, non usate `make genkey` per creare la chiave, ma i due comandi seguenti.

Usate il seguente comando per creare la vostra chiave:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

Usate il seguente comando per assicurarvi che i permessi sono stati impostati correttamente:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

Se usate questi comandi per creare la chiave, non dovete usare la password per avviare il secure server.

Attenzione

La disattivazione della password per il vostro secure server è vivamente SCONSIGLIATA per motivi di sicurezza.

I problemi associati all'assenza di password sono strettamente legati alla sicurezza della macchina. Per esempio se qualcuno compromette la sicurezza UNIX della macchina host, tale persona potrebbe ottenere la vostra chiave privata (il contenuto del file `server.key`) e usarla per fornire pagine Web che sembreranno provenire dal vostro secure server.

Se le regole di sicurezza UNIX vengono rigorosamente rispettate sul computer host (tutte le correzioni e gli aggiornamenti del sistema operativo vengono installati appena sono disponibili, nessun servizio inutile o pericoloso è in funzione ecc.) la password può sembrare inutile. Tuttavia, poiché il secure

server non deve essere riavviato spesso, l'ulteriore sicurezza fornita dalla password è, nella maggior parte dei casi, di grande aiuto.

Il file `server.key` deve appartenere all'utente root del sistema e non deve essere accessibile ad altri utenti. Create una copia di backup del file e conservatela in un luogo sicuro. La copia di backup è necessaria, poiché se perdete il file `server.key` dopo averlo usato per formulare la richiesta di certificato, il vostro certificato smetterà di funzionare e la CA non vi potrà aiutare. In tal caso non vi resta che acquistare un nuovo certificato.

Se volete acquistare un certificato da una CA, consultate la Sezione 20.7. Se invece volete creare voi stessi il certificato, consultate la Sezione 20.8.

20.7. Come richiedere un certificato a una CA

Una volta creata la chiave dovete formulare una richiesta di certificato da inviare a una CA. Assicuratevi di essere nella directory `/usr/share/ssl/certs` e poi digitate il comando seguente:

```
make certreq
```

Il sistema visualizza il seguente messaggio e vi chiede di digitare la password (se non avete disattivato la funzione password):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Digitate la password che avete scelto durante la creazione della chiave. Il sistema visualizza alcune istruzioni e vi chiede delle informazioni. Le informazioni fornite vengono incorporate nella richiesta. Il messaggio, al quale sono state aggiunte risposte di esempio, è simile a:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.example.com
Email Address []:admin@example.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Le risposte di default compaiono fra parentesi quadre `[]` subito dopo ogni richiesta di informazione. Per esempio la prima informazione richiesta è il paese dove verrà usato il certificato:

```
Country Name (2 letter code) [GB]:
```

La risposta di default, fra parentesi, è `GB`. Per accettarla, premete [Invio], altrimenti digitate le lettere corrispondenti al vostro paese.

Dovrete inserire il resto dei valori. La maggior parte di essi sono molto semplici, ma avrete comunque bisogno di seguire le seguenti regole:

- Non abbreviate la località o lo stato. Scriveteli per esteso (per esempio Novi L. deve essere scritto Novi Ligure).
- Se mandate questa richiesta a una CA, fate attenzione a fornire informazioni corrette per tutti i campi, ma soprattutto per l' `Organization Name` e il `Common Name`. La CA controlla le informazioni fornite. Le richieste contenenti informazioni non valide vengono rifiutate dalle CA.
- For `Common Name`, assicuratevi di inserire il *vero* nome del vostro secure server (un nome DNS valido) e non un eventuale alias del server.
- L'`Email Address` deve corrispondere all'indirizzo e-mail del Webmaster o dell'amministratore di sistema.
- Evitate caratteri speciali quali @, #, &, !, ecc. Alcune CA rifiutano le richieste che contengono caratteri speciali. Se il nome della vostra società contiene il carattere (&), sostituitelo con "e".
- Non usate i campi `A challenge password` e `An optional company name`. Per continuare senza inserire dati in questi campi, premete [Invio] in modo che vengano accettate le informazioni di default.

Quando avete finito di fornire le informazioni richieste, viene creato il file `/etc/httpd/conf/ssl.csr/server.csr`. Questo file contiene la richiesta ed è pronto per essere inviato alla vostra CA.

Quando avete deciso a quale CA rivolgervi, seguite le istruzioni fornite nel sito Web corrispondente. La CA vi dice come inviare la richiesta, se sono necessari altri documenti e quanto dovete pagare.

Una volta che avete eseguito tutte le operazioni richieste, la CA invia (solitamente via e-mail) il certificato. Salvatelo (oppure fate un copia e incolla) come `/etc/httpd/conf/ssl.crt/server.crt`. Assicuratevi di effettuare un back up di questo file.

20.8. Creazione di un certificato "self-signed"

Potete creare voi stessi il certificato. Tenete presente che un certificato self-signed non fornisce le stesse garanzie di sicurezza di un certificato CA. Per maggiori informazioni, consultate la Sezione 20.5.

Per creare un certificato è necessario prima creare una chiave di accesso seguendo le istruzioni che fornisce la Sezione 20.6. Una volta creata la chiave, assicuratevi di trovarvi nella directory `/usr/share/ssl/certs` e digitate il comando seguente:

```
make testcert
```

Compare a video il messaggio seguente e vi viene chiesto di inserire la vostra password (a meno che abbiate creato la chiave senza password):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Una volta inserita la vostra password (oppure se non è comparso il prompt se avete creato una chiave senza password), vi vengono chieste altre informazioni. Il messaggio del computer che compare a

video è riportato qui di seguito (dovete fornire le informazioni corrette relative alla vostra organizzazione e al vostro computer):

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.example.com
Email Address []:myemail@example.com
```

Dopodiché, all'interno di `/etc/httpd/conf/ssl.crt/server.crt` viene creato un certificato self-signed. A questo punto riavviate il vostro secure server dopo aver generato il certificato con il seguente comando:

```
/sbin/service httpd restart
```

20.9. Verifica del certificato

Per effettuare una verifica del certificato di verifica installato per default, un certificato CA e un certificato self-signed indicano la seguente home page (sostituendo *`server.example.com`* con il vostro nome del dominio) al vostro browser Web:

`https://`*`server.example.com`*

Nota Bene

Notare la `s` dopo `http`. Il prefisso `https:` é usato per transazioni HTTP sicure.

Se usate un certificato rilasciato da una CA famosa, il vostro browser accetta automaticamente il certificato (senza chidervi alcun input) e stabilisce la connessione sicura. Il vostro browser non riconosce automaticamente un certificato di prova o self-signed, questo perché esso non é un certisicato CA. Se non usate un certificato CA, seguite le istruzioni fornite dal vostro browser per accettare il certificato.

Una volta che il browser ha accettato il certificato, il vostro secure server visualizza una Home Page di default.

20.10. Accesso al server

Per accedere al vostro secure server, usate un URL simile al seguente:

`https://`*`server.example.com`*

Le URL per il collegamento al vostro non-secure server puó essere simile a quanto segue:

`http://server.example.com`

La porta standard per le comunicazioni Web sicure è la numero 443, mentre quella per le comunicazioni Web non sicure è la numero 80. La configurazione di default del secure server si collega a entrambe le porte standard, pertanto non dovete specificare il numero di porta nell'URL (sottointeso).

Tuttavia, se configurate il vostro server in modo tale che si colleghi a una porta non standard (per esempio qualsiasi numero tranne 80 o 443), dovete specificare il numero di porta in tutte le URL che si collegano al server sulla porta non standard.

Per esempio potete avere configurato il server in maniera da avere un host virtuale che funzioni in modo non sicuro sulla porta 12331. Tutte le URL che si collegano a questo host virtuale devono specificare il numero di porta nell'URL. L'esempio seguente riporta una URL che prova a collegarsi a un non-secure server impostato sulla porta 12331:

`http://server.example.com:12331`

20.11. Risorse aggiuntive

Per ulteriori informazioni relative al Server HTTP Apache, consultate la la Sezione 19.7.

20.11.1. Documentazione installata

- `mod_ssl documentation` — aprite un browser Web e andate alla URL http://localhost/manual/mod/mod_ssl.html sul server sul quale è in esecuzione il Server HTTP Apache ed in possesso del pacchetto `httpd-manual`.

20.11.2. Siti Web utili

- http://www.redhat.com/mailing-lists/ — potete iscrivervi alla mailing list di redhat-secure-server al sopra indicato URL.

  Potete iscrivervi anche mandando un e-mail all'indirizzo <`redhat-secure-server-request@redhat.com`> ponendo come oggetto del messaggio la parola *subscribe*.
- http://www.modssl.org — è la fonte più dettagliata di informazioni relative a `mod_ssl`. Il sito comprende una ricca documentazione, compreso un *Manuale Utente* all'indirizzo http://www.modssl.org/docs.

20.11.3. Libri correlati

- *Apache: The Definitive Guide*, 2a edizione, di Ben Laurie e Peter Laurie, O'Reilly & Associates, Inc.

Capitolo 21.

Configurazione di BIND

Questo capitolo presuppone conoscenze di base di BIND e del DNS e non è un tentativo di spiegarne i concetti. Viene illustrato come usare lo **Strumento di configurazione Bind** (`redhat-config-bind`) per impostare le zone di base del server per la le zone server basiche di BIND. Lo **Strumento di configurazione Bind** crea il file di configurazione `/etc/named.conf` e i file di configurazione della zona nella directory `/var/named` ogni volta che vengono effettuate delle modifiche.

Importante

Non modificate il file di configurazione `/etc/named.conf`. Lo **Strumento di configurazione Bind** genera questo file dopo aver applicato le modifiche. Se desiderate configurare le impostazioni non configurabili mediante Lo **Strumento di configurazione Bind** aggiungetele a `/etc/named.conf`.

Lo **Strumento di configurazione Bind** richiede il sistema X Window e i privilegi di root. Per avviare lo **Strumento di configurazione Bind**, selezionate il **menu principale** (sul pannello) => **Impostazioni del sistema => Impostazioni del Server => Servizio del nome del Dominio** oppure digitate il comando `redhat-config-bind` ad un prompt della shell (per esempio, in un terminale XTerm o di GNOME).

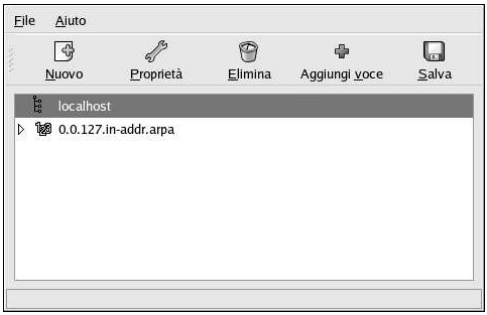

Figura 21-1. Strumento di configurazione Bind

Lo **Strumento di configurazione Bind** imposta `/var/named` come directory predefinita per la zona. Tutti i file di zona specificati fanno riferimento a questa directory. Lo **Strumento di configurazione Bind** comprende, inoltre, il controllo sintattico di base al momento dell'immissione dei valori. Per esempio, se l'inserimento valido è un indirizzo IP, nell'area di testo si possono digitare solo numeri e punti (.).

Lo **Strumento di configurazione Bind** vi consente di aggiungere una zona master e una inversa. Dopo aver aggiunto le zone, potete modificarle o cancellarle dalla finestra principale, come mostra la Figura 21-1.

Dopo aver aggiunto, modificato o cancellato una zona, selezionate **Salva** o **File => Salva** per scrivere il file di configurazione `/etc/named.conf` e tutti i file delle zone individuali nella directory `/var/named`. Con l'applicazione delle modifiche il servizio `named` ricarica i file di configurazione. Selezionate **File => Esci** per salvare i cambiamenti prima di lasciare l'applicazione.

21.1. Aggiungere una zona master

Per aggiungere una zona master (nota anche come master primaria), fate clic sul pulsante **Nuovo**, selezionate **Zona master diretta** e inserite il nome di dominio per la zona master nell'area di testo **Nome del dominio**.

Compare una nuova finestra, come mostrato nella Figura 21-2, contenente le opzioni seguenti:

- **Nome** — nome di dominio appena inserito nella finestra precedente.
- **Nome del file** — nome del file di database del DNS, relativo a `/var/named`. È preimpostato sul nome di dominio con estensione `.zone`.
- **Contatto** — indirizzo e-mail del contatto principale per la zona master.
- **Server di nomi primario (SOA)** — specifica il nome di server primari per questo dominio.
- **Numero seriale** — numero seriale del file database del DNS. Questo valore può essere aumentato ogni volta che il file viene modificato, in modo che i server di nomi slave per la zona ricevano i dati più aggiornati. Lo **Strumento di configurazione Bind** aumenta questo numero ogni volta che cambia la configurazione. Tale valore può anche essere aumentato manualmente, facendo clic sul pulsante **Imposta** accanto al valore **Numero serial**.
- **Impostazioni ora** — comprende i valori TTL (Time to Live) **Aggiorna**, **Riprova**, **Scadenza** e **Minimo** memorizzati nel file database del DNS. Tutti i valori sono espressi in secondi.
- **Registrazione** — aggiunge, modifica e cancella le risorse dei record **Host**, **Alias** e **Server di nomi**.

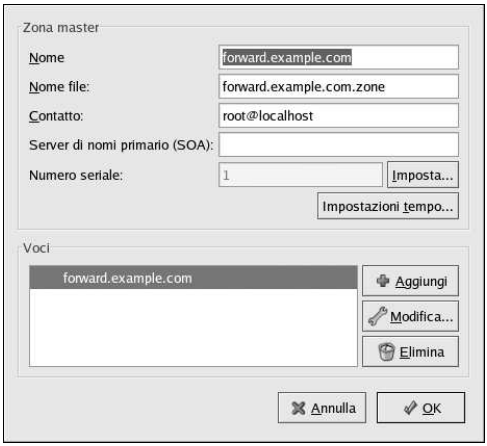

Figura 21-2. Aggiungere una zona master

Deve essere specificato un **Server di nome primario (SOA)**, e almeno una voce del server di nome deve essere specificata facendo clic sul pulsante **Aggiungi** nella sezione **Voci**.

Dopo aver configurato la Zona Master Diretta, fare clicc su **OK** per tornare alla finestra principale, come mostrato su Figura 21-1. Fare clicc su **Salva**, dal menu a tendina, per scrivere il file di configurazione `/etc/named.conf` scrivere tutti i file di zona individuale, nella directory `/var/named`, e permette al demone di ricaricare i file di configurazione.

La configurazione crea una entry in `/etc/named.conf`, simile alla seguente:

```
zone  "forward.example.com" {
 type master;
 file  "forward.example.com.zone";
};
```

Inoltre, crea il file `/var/named/forward.example.com.zone` contenente le informazioni che seguono:

```
$TTL 86400
@       IN      SOA     ns.example.com.  root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )


        IN      NS      192.168.1.1.
```

21.2. Aggiunta di una zona master inversa

Per aggiungere una zona master inversa, fate clic sul pulsante **Nuovo** e selezionate **Zona master inversa**. Inserite i primi tre ottetti del range di indirizzi IP che desiderate considerare. Per esempio, se state configurando il range 192.168.10.0/255.255.255.0, inserite 192.168.10 nell'area di testo **Indirizzo IP (primi 3 ottetti)**.

Compare una nuova finestra, come visualizzato nella Figura 21-3, contenente le opzioni seguenti:

1. **Indirizzo IP** — i primi tre ottetti appena inseriti nella finestra precedente.
2. **Indirizzo IP inverso** — non modificabile. Compilato in base all'indirizzo IP inserito.
3. **Contatto** — indirizzo e-mail del contatto principale per la zona master.
4. **Nome del file** — nome del file database del DNS nella directory `/var/named`.
5. **Server di nomi primario (SOA)** — specifica il nome di server primari per questo dominio.
6. **Numero serial** — numero seriale del file database del DNS. Questo valore può essere aumentato ogni volta che il file viene modificato, in modo che i server di nomi slave per la zona ricevano i dati più aggiornati. Lo **Strumento di configurazione Bind** aumenta questo numero ogni volta che cambia la configurazione. Tale valore può anche essere aumentato manualmente, facendo clic sul pulsante **Imposta** accanto al valore **Numero serial**.
7. **Impostazioni ora** — comprende i valori TTL (Time to Live) **Refresh**, **Retry**, **Expire** e **Minimum** memorizzati nel file database del DNS.
8. **Server di nomi** — aggiunge, modifica e cancella i server di nomi per la zona master inversa. È richiesto almeno un server di nomi.
9. **Tabella degli indirizzi inversi** — lista degli indirizzi IP entro la zona master inversa e i nomi di host. Per esempio, per la zona master inversa 192.168.10, potete aggiungere 192.168.10.1 nella **Tabella degli indirizzi inversi** con il nome host one.example.com. Il nome deve terminare con un (.) per indicare che si tratta di un nome di host completo.

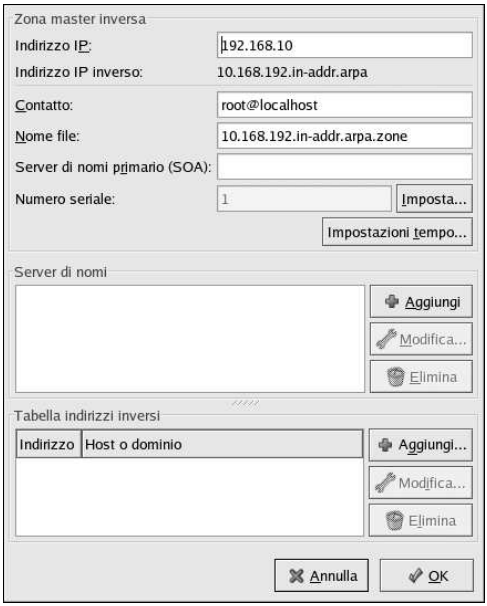

Figura 21-3. Aggiunta di una zona master inversa

Deve essere specificato un **Server di nome primario (SOA)**, e almeno una voce del server di nome deve essere specificata facendo clic sul pulsante **Aggiungi** nella sezione **Server di nomi**.

Dopo aver configurato la Zona Master Inversa, fare clic su **OK** per tornare alla finestra principale, come mostrato su Figura 21-1. Fare clic su **Salva**, dal menu a tendina, per scrivere il file di configurazione `/etc/named.conf` scrivere tutti i file di zona individuale nella directory `/var/named`, e permette al demone di ricaricare i file di configurazione.

La configurazione crea una entry in `/etc/named.conf` simile a quanto segue:

```
zone  "10.168.192.in-addr.arpa" {
        type master;
        file  "10.168.192.in-addr.arpa.zone";
};
```

Inoltre, crea il file `/var/named/10.168.192.in-addr.arpa.zone` con le seguenti informazioni:

```
$TTL 86400
@       IN      SOA     ns.example.com. root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttk
                        )


@       IN      NS      ns2.example.com.

1       IN      PTR     one.example.com.
```

```
2       IN      PTR     two.example.com.
```

21.3. Aggiunta di una zona slave

Per aggiungere una zona slave (nota anche come master secondaria) fate clic sul pulsante **Aggiungi** e selezionate **Zona slave**. Inserite il nome del domino per la zona slave nell'area di testo **Nome del dominio**.

Compare una nuova lista, come mostrato nella Figura 21-4, contenente le opzioni seguenti:

- **Nome** — il nome del dominio inserito nella finestra precedente.
- **Lista dei master** — il server dei nomi da cui la zona slave riceve i suoi dati. Questo valore deve corrispondere a un indirizzo IP valido. Potete inserire solo numeri e punti nell'area di testo.
- **Nome del file** — nome del file database del DNS in `/var/named`.

Figura 21-4. Aggiunta di una zona slave

Dopo aver configurato la zona slave, fate clic su **OK** per tornare alla finestra principale riportata nella Figura 21-1. Fare clic su **Salva** per scrivere i file `/etc/named.conf` di configurazione e per far ricaricare i file dal demone.

La configurazione crea una entry in `/etc/named.conf`, simile a quanto segue:

```
zone "slave.example.com" {
        type slave;
        file "slave.example.com.zone";
        masters {
                 1.2.3.4;
                };
};
```

Il file di configurazione `/var/named/slave.example.com.zone` viene creato dal servizio `named` quando scarica i dati della zona dal/i server del master.

Capitolo 22.

Configurazione di autenticazione

Quando un utente effettua una registrazione in un sistema Red Hat Linux, la combinazione nome utente e password, deve essere controllata, o *autenticata*, come utente valido e attivo. Talvolta l'informazione per verificare l'utente é posizionata sul sistema locale, altre volte il sistema rinvia l'autenticazione ad un database di un utente su di un sistema remoto.

Lo **Strumento di Configurazione per l'Autenticazione** fornisce una interfaccia grafica per configurare NIS, LDAP, e Hesiod per riprendere le informazioni dell'utente e per configurare LDAP, Kerberos, e SMB come protocolli di autenticazione.

Nota Bene

Se avete configurato un livello di sicurezza medio o alto durante l'installazione o con i metodi di autenticazione di rete **Strumento di configurazione del livello di sicurezza** (o selezionato un livello di sicurezza alto o basso con il programma **GNOME Lokkit**), incluso NIS e LDAP, non sono abilitati attraverso il firewall.

Questo capitolo non spiega in dettaglio ogni tipo diverso di autenticazione. Spiega invece come usare lo **Strumento di Configurazione per l'Autenticazione** per configurarli.

Per avviare la versione grafica dello **Strumento di Configurazione per l'Autenticazione** dal desktop, selezionare **Pulsante menu principale** (sul pannello) => **Impostazioni del sistema** => **Autenticazione** o digitare il comando `authconfig-gtk` al prompt della shell (per esempio, in un **XTerm** o un **terminale GNOME**). Per iniziare una versione basata su testo, digitare il comando `authconfig` al prompt della shell.

Importante

Dopo essere usciti dal programma di autenticazione, i cambiamenti epportati saranno confermati immediatamente.

22.1. Informazioni dell'utente

La scheda **informazioni dell'utente** possiede deverse opzioni. Per abilitare una opzione, selezionare la casella posizionata vicino. Per disabilitare una opzione, deselezionare la stessa casella. Fate clic su **OK** per uscire dal programma e confermare i cambiamenti.

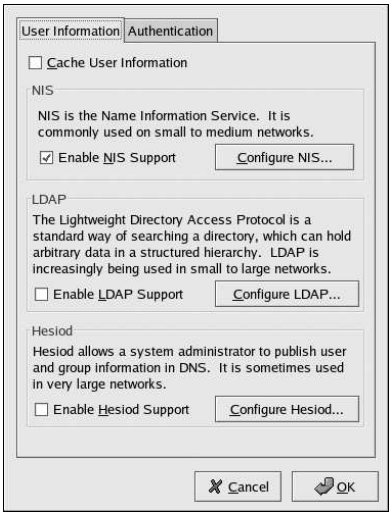

Figura 22-1. informazioni dell'utente

Il seguente elenco riporta le configurazioni possibili che ogni opzione puó effettuare:

- **Cache User Information** — Selezionare questa opzione per abilitare il "name service cache daemon" (`nscd`) e configuratelo in modo da iniziare al momento dell'avvio.

  Il pacchetto `nscd` deve essere installato per poter far funzionare questa opzione.

- **Abilitare il supporto NIS** — Selezionare questa opzione per configurare il sistema come un client NIS, il quale si connette ad un server NIS per l'autenticazione della password e dell'utente. Fate clic sul pulsante **Configura NIS** per specificare il dominio e il server NIS . Se il server NIS non é specificato, il demone cercherá di trovarlo tramite una previsione.

  Il pacchetto `ypbind` deve essere installato per far funzionare questa opzione. Se il supporto NIS é abilitato, i servizi `portmap` e `ypbind` vengono iniziati e sono anche abilitati ad iniziare al momento dell'avvio.

- **Abilitare il supporto LDAP** — Selezionare questa opzione per configurare il sistema in modo tale che riprenda le informazioni dell'utente tramite LDAP. Fate clic sul pulsante **Configura LDAP** per specificare il **LDAP Search Base DN** e **Server LDAP**. Se viene selezionato **Usare TLS per criptare le connessioni**, viene usato il Transport Layer Security per criptare le password inviate dal server LDAP.

  Il pacchetto `openldap-clients` deve essere installato per fare funzionare questa opzione.

  Per maggiori informazioni inerente LDAP, consultare *Red Hat Linux Reference Guide*.

- **Abilitare il supporto Hesiod** — Selezionare questa opzione per configurare il sistema in modo tale che riprenda le informazioni da un database Hesiod remoto, incluso le informazioni dell'utente.

  Il pacchetto `hesiod` deve essere installato.

22.2. Autenticazione

La scheda di **Autenticazione** abilita la configurazione dei metodi di autenticazione della rete. Per abilitare una opzione, selezionare la casella vuota situata al suo fianco. Per disabilitare una opzione, fate clic sulla stessa casella per deselezionarla.

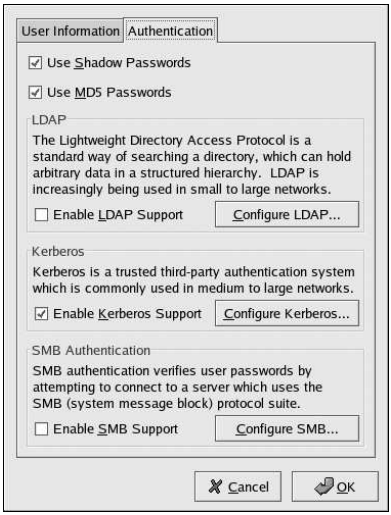

Figura 22-2. Autenticazione

Quanto segue riporta le configurazioni possibili che ogni opzione puó effettuare:

- **Uso delle password shadow** — Selezionare questa opzione per memorizzare le password nel formato password shadownel file `/etc/shadow` invece di `/etc/passwd`. Le password shadow sono abilitate per default durante l'installazione e sono fortemente consigliate per aumentare la sicurezza del sistema.

  Il pacchetto `shadow-utils` deve essere installato per fare funzionare questa opzione. Per maggiori informazioni inerenti la password shadow, consultate il capitolo *Utenti e Gruppi* in *Red Hat Linux Reference Guide*.

- **Uso delle password MD5** — Selezionare questa opzione per abilitare le password MD5, le quali permettono alle password di avere fino a 256 caratteri invece di un massimo di otto. É selezionato per default durante l'installazione ed é fortemente consigliato per aumentare la sicurezza.

- **Abilitare il supporto LDAP** — Selezionare questa opzione per abilitare il PAM standard che permette alle applicazioni di usare LDAP per l'autenticazione. Fate clic sul pulsante **Configura LDAP** per specificare quanto segue:

  - **Uso di TLS per cifrare le password** — Uso del Transport Layer Security per cifrare le password inviate al server LDAP.
  - **LDAP Search Base DN** — Riprende le informazioni dal proprio Distinguished Name (DN).
  - **LDAP Server** — Specifica l'indirizzo IP del server LDAP.

  Il pacchetto `openldap-client` deve essere installato per fare funzionare questa opzione. Consultare *Red Hat Linux Reference Guide* per maggiori informazioni inerenti LDAP.

- **Abilitare il supporto Kerberos** — Selezionare questa opzione per abilitare l'autenticazione Kerberos. Fate clic sul pulsante **Configura Kerberos** per configurare:

  - **Realm** — Configurare il realm per il server di Kerberos. Il realm é la rete che usa Kerberos, composto da uno o piú KDC e daun potenziale gran numero di client.
  - **KDC** — Definisce il Key Distribution Center (KDC), cioé il server che emette i ticket di Kerberos.

- **Server Admin** — Specifica il server di gestione che esegue `kadmind`.

  I pacchetti `krb5-libs` e `krb5-workstation` devono essere installati per fare funzionare questa opzione. Consultate *Red Hat Linux Reference Guide* per maggiori informazioni su Kerberos.

- **Abilita il supporto SMB** — Questa opzione configura PAM per l'uso di un server SMB per effettuare l'autenticazione degli utenti. Fate clic sul pulsante **Configura SMB** per specificare:
  - **Workgroup** — Specifica il gruppo SMB da usare.
  - **Controller del dominio** — Specifica i controller del dominio SMB da usare.

22.3. Versione della linea di comando

Lo **Strumento di Configurazione per l'Autenticazione** puó anche essere eseguito come uno strumento della linea di comando con nessuna interfaccia. La versione della linea di comando puó essere usata in uno script di configurazione o di uno script di kickstart. Le opzioni di autenticazione sono riportate in Tabella 22-1.

Opzione	Descrizione
`--enableshadow`	Abilita le password shadow
`--disableshadow`	Disabilita le password shadow
`--enablemd5`	Abilita le password MD5
`--disablemd5`	Disabilita le password MD5
`--enablenis`	Abilita NIS
`--disablenis`	Disabilita NIS
`--nisdomain=<`*`domain`*`>`	Specifica il dominio NIS
`--nisserver=<`*`server`*`>`	Specifica il server NIS
`--enableldap`	Abilita LDAP per le informazioni dell'utente
`--disableldap`	Disabilita LDAP per le informazioni dell'utente
`--enableldaptls`	Abilita l'uso di TLS con LDAP
`--disableldaptls`	Disabilita l'uso di TLS con LDAP
`--enableldapauth`	Abilita LDAP per l'autenticazione
`--disableldapauth`	Disabilita LDAP per l'autenticazione
`--ldapserver=<`*`server`*`>`	Specifica il server LDAP
`--ldapbasedn=<`*`dn`*`>`	Specifica LDAP base DN
`--enablekrb5`	Abilita Kerberos
`--disablekrb5`	Disabilita Kerberos
`--krb5kdc=<`*`kdc`*`>`	Specifica Kerberos KDC
`--krb5adminserver=<`*`server`*`>`	Specifica il server di gestione di Kerberos
`--krb5realm=<`*`realm`*`>`	Specifica il realm di Kerberos realm
`--enablesmbauth`	Abilita SMB

Opzione	Descrizione
`--disablesmbauth`	Disabilita SMB
`--smbworkgroup=<`*`workgroup`*`>`	Specifica il gruppo di lavoro "workgroup" SMB
`--smbservers=<`*`server`*`>`	Specifica i server SMB
`--enablehesiod`	Abilita Hesiod
`--disablehesiod`	Disabilita Hesiod
`--hesiodlhs=<`*`lhs`*`>`	Specifica Hesiod LHS
`--hesiodrhs=<`*`rhs`*`>`	Specifica Hesiod RHS
`--enablecache`	Abilita `nscd`
`--disablecache`	Disabilita `nscd`
`--nostart`	Non avviare o interrompere i servizi `portmap`, `ypbind`, o `nscd` anche se sono configurati
`--kickstart`	Non mostrare l'interfaccia utente
`--probe`	Cercare e mostrare i default di rete

Tabella 22-1. Opzioni della linea di comando

Suggerimento

Queste opzioni possono essere trovate nella pagina man `authconfig` oppure digitando `authconfig --help` al prompt della shell.

Capitolo 23.

Configurazione del Mail Transport Agent (MTA)

Un *Mail Transport Agent* (MTA) è essenziale per inviare posta da un sistema Red Hat Linux. Il *Mail User Agent* (MUA), per esempio **Evolution**, **Mozilla Mail**, e **Mutt**, consente di leggere e comporre messaggi di posta elettronica. Quando si invia un messaggio di posta elettronica da un MUA, esso viene trasferito all'MTA, che invia il messaggio a una serie di MTA fino ad arrivare a destinazione.

Anche se un utente non intende inviare posta dal sistema, ci sono alcuni compiti (task) automatizzati o programmi di sistema che usano il comando `/bin/mail` per inviare messaggi di posta contenenti messaggi di log all'utente root del sistema locale.

Red Hat Linux 9 fornisce due MTA: Sendmail e Postfix. Se sono installati entrambi, `sendmail` rappresenta l'MTA di default. L'**Agent switcher del trasporto della posta** consente di selezionare `sendmail` o `postfix` come MTA di default per il sistema.

Il pacchetto RPM `redhat-switch-mail` deve essere installato usando una versione basata su testo del programma **Agent switcher del trasporto della posta**. Se desiderate usate una versione grafica, il pacchetto `redhat-switch-mail-gnome` deve inoltre essere installato. For more information on installing RPM packages, refer to Parte V.

Per utilizzare l'**Agent switcher del trasporto della posta**, seleionate il **pulsante del menu principale** (sul pannello) => **Strumenti del sistema** => **Piú strumenti del sistema** => **Agent switcher del trasporto della posta**, oppure digitate il comando `redhat-switchmail` al prompt della shell (per esempio, in un terminale XTerm o GNOME).

Il programma rileva automaticamente se il sistema X Window è in esecuzione. In tal caso, il programma viene avviato in modalità grafica come mostra la Figura 23-1. Se il sistema X Window non è rilevato, viene avviato in modalità di testo. Per eseguire l'**Agent switcher del trasporto della posta** in modalità di testo, usate il comando `redhat-switchmail-nox`.

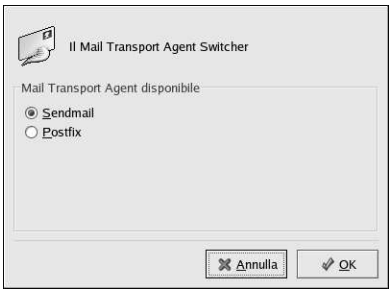

Figura 23-1. Agent switcher del trasporto della posta

Se selezionate **OK** per modificare MTA, il daemon della posta elettronica selezionato viene abilitato ad iniziare durante l'avvio del sistema, e quello che non è selezionato viene disabilitato cosichè non inizia all'avvio del sistema. Inoltre il daemon della posta elettronica selezionato viene iniziato, e l'altro viene arrestato così concedendo che i cambiamenti avvengano immediatamente.

Per ulteriori informazioni sui protocolli di posta elettronica e MTA cosultate la *Red Hat Linux Reference Guide*. Per ulteriori informazioni sui MUA, consultate la *Red Hat Linux Getting Started Guide*.

IV. Configurazione del sistema

Dopo aver discusso dell'accesso alla console e come ottenere informazioni software e hardware da un sistema Red Hat Linux, questa parte spiega i compiti di configurazione comuni del sistema.

Sommario

Capitolo 24.

Accesso alla console

Quando vi collegate a un computer a livello locale come utente standard (non-root), il sistema attribuisce due tipi di permessi speciali:

1. Potete eseguire determinati programmi non accessibili ad altri utenti.
2. Potete accedere a determinati file (di solito ai file di periferica utilizzati per dischetti floppy, CD-ROM e così via) a cui gli altri utenti non hanno accesso.

Poiché in un singolo computer sono disponibili varie console e molti utenti possono connettersi contemporaneamente a livello locale al computer, uno degli utenti deve arrivare per primo per accedere ai file. L'utente che si è connesso per primo alla console ha accesso a quei file. Quando il primo utente si disconnette, l'utente che si collega subito dopo può disporre dei file.

In contrasto, *Tutti* gli utenti che si connettono alla console sono autorizzati a eseguire programmi che svolgono operazioni normalmente limitate all'utente root. Se X è in esecuzione, queste operazioni possono essere incluse come oggetti del menu in un'interfaccia utente grafica. Tra i programmi accessibili dalla console figurano: `halt`, `poweroff` e `reboot`.

24.1. Disabilitazione della chiusura della sessione tramite Ctrl-Alt-Canc

Per default, `/etc/inittab` determina che il vostro sistema venga spento o riavviato in risposta alla combinazione di tasti [Ctrl]-[Alt]-[Canc] usata dalla console. Se desiderate disabilitare completamente quest'opzione, commentate la riga descritta qui sotto nel file `/etc/inittab`, aggiungendo davanti a essa il carattere cancelletto (`#`):

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Se invece desiderate autorizzare determinati utenti non-root a chiudere il sistema dalla console utilizzando [Ctrl]-[Alt]-[Canc], potete limitare questo privilegio ad alcuni utenti seguendo le istruzioni qui riportate:

1. Aggiungete un'opzione `-a` alla riga `/etc/inittab` mostrata sopra, in modo che diventi:
   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```
   L'opzione `-a` indica a `shutdown` di cercare il file `/etc/shutdown.allow`, che provvederete a creare nella prossima fase.
2. Create un file chiamato `shutdown.allow` nella directory `/etc`. Il file `shutdown.allow` deve elencare i nomi degli utenti autorizzati a chiudere il sistema con [Ctrl]-[Alt]-[Canc]. Il file `/etc/shutdown.allow` ha il formato di un elenco, in cui sono contenuti dei nomi utenti, uno per ogni riga:
   ```
   stephen
   jack
   sophie
   ```

Secondo questo file `shutdown.allow` d'esempio, stephen, jack e sophie sono autorizzati a chiudere il sistema dalla console utilizzando la combinazione di tasti [Ctrl]-[Alt]-[Canc]. Quando si utilizza questa combinazione, l'opzione `shutdown -a` in `/etc/inittab` controlla se qualcuno degli utenti elencati nel file `/etc/shutdown.allow` (o root) è connesso a una console virtuale. Se è così, la chiusura del sistema prosegue, in caso contrario viene scritto un messaggio di errore alla console di sistema.

Per maggiori informazioni sul file `shutdown.allow`, leggete la pagina man di `shutdown`.

24.2. Disabilitazione dell'accesso alla console

Per disabilitare l'accesso ai programmi della console da parte degli utenti, connettetevi come root ed eseguite questo comando:

```
rm -f /etc/security/console.apps/*
```

In ambienti dove la console è altrimenti protetta (esistono passwords per BIOS e boot loader, la combinazione di tasti [Ctrl]-[Alt]-[Canc] sono disabilitati,i pulsanti di accensione e di riavvio sono disabilitati e così via), è probabile che volete evitare che qualsiasi utente possa eseguire i programmi `poweroff`, `halt` e `reboot`, accessibili dalla console per default.

Per impedire l'esecuzione di questi programmi, connettetevi come root ed eseguite i comandi seguenti:

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

24.3. Disabilitazione di tutti gli accessi alla console

Il modulo PAM `pam_console.so` gestisce i permessi e le autenticazioni per i file della console (per maggiori dettagli sulla configurazione PAM consultate la *Red Hat Linux Reference Guide*). Se desiderate disabilitare tutti gli accessi alla console, incluso l'accesso ai file e ai programmi, commentate tutte le righe che fanno riferimento a `pam_console.so` nella directory `/etc/pam.d`. Collegatevi come root ed eseguite il seguente script:

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

24.4. Come definire l'accesso alla console

Il modulo `pam_console.so` usa il file `/etc/security/console.perms` per stabilire i permessi utente nella console di sistema. La sintassi di questo file è molto flessibile. Potete modificare il file in modo tale che le istruzioni non siano più valide. Tuttavia nel file predefinito è contenuta una riga simile alla seguente:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

Quando gli utenti si connettono, sono "legati" a una sorta di terminale provvisto di nome, (un server X con un nome simile a `:0` o `mymachine.example.com:1.0` oppure un dispositivo come `/dev/ttyS0` o `/dev/pts/2`). Di solito, solo le console virtuali locali e i server X locali sono considerati locali, ma se desiderate considerare come locale anche il terminale seriale accanto a voi sulla porta `/dev/ttyS1`, modificate la riga sopra illustrata in questo modo:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

24.5. Come rendere i file accessibili dalla console

Nel file `/etc/security/console.perms` è contenuta una sezione con righe simili alle seguenti:

```
<floppy>=/dev/fd[0-1]* \
         /dev/floppy/* /mnt/floppy*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
        /dev/mixer* /dev/sequencer \
        /dev/sound/* /dev/beep
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
```

Se necessario, potete aggiungere delle righe personali a questa sezione. Assicuratevi che le righe aggiunte si riferiscano al dispositivo corretto. Per esempio potete aggiungere la seguente riga:

```
<scanner>=/dev/scanner /dev/usb/scanner*
```

(Accertatevi innanzitutto che `/dev/scanner` sia davvero il vostro scanner e non, per esempio, il disco fisso).

Ora è necessario determinare come vengono utilizzati questi file. Osservate l'ultima sezione del file `/etc/security/console.perms` e cercate delle righe simili alle seguenti:

```
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound>  0640 root
<console> 0600 <cdrom>  0600 root.disk
```

e aggiungete questa riga:

```
<console> 0600 <scanner> 0600 root
```

Pertanto, quando vi connettete alla console, vi viene attribuita la proprietà della periferica `/dev/scanner` e i permessi sono 0600 (solo voi avete privilegi di lettura e scrittura). Quando vi disconnettete, la periferica viene attribuita a root che comunque detiene i permessi 0600 (ora: privilegi di lettura e scrittura solo a root).

24.6. Abilitazione dell'accesso alla console per altre applicazioni

Se desiderate rendere accessibili altre applicazioni agli utenti che usano la console, eseguite attentamente le istruzioni riportate qui di seguito.

Prima di tutto, l'accesso alla console funziona *solo* per le applicazioni che si trovano nelle directory `/sbin` o `/usr/sbin`. Pertanto, dopo aver verificato che l'applicazione desiderata è contenuta in queste directory, procedete come segue:

1. Create un collegamento tra il nome dell'applicazione, per esempio il programma *`foo`* e l'applicazione `/usr/bin/consolehelper`:
   ```
   cd /usr/bin
   ln -s consolehelper foo
   ```
2. Create il file `/etc/security/console.apps/`*`foo`*:
   ```
   touch /etc/security/console.apps/foo
   ```
3. Create un file di configurazione di PAM per il servizio *`foo`* in `/etc/pam.d/`. Un modo semplice per farlo è quello di utilizzare una copia del file di configurazione di PAM per il servizio halt e poi modificare il file:
   ```
   cp /etc/pam.d/halt /etc/pam.d/foo
   ```

Ora, quando eseguite `/usr/bin/foo`, viene richiamata l'applicazione `consolehelper` che, con l'ausilio di `/usr/sbin/userhelper` autentica l'utente. Per farlo `consolehelper` richiede la password dell'utente se `/etc/pam.d/foo` è una copia del file `/etc/pam.d/halt` (in caso contrario esegue quanto specificato nel file `/etc/pam.d/foo`) e poi esegue il file `/usr/sbin/foo` con i permessi di root.

Nel file di configurazione PAM, un'applicazione può essere configurata per utilizzare il modulo *pam_timestamp* per memorizzare (cache) un tentativo di autenticazione riuscito. Quando un'applicazione viene avviata ed viene effettuata un'autenticazione appropriata (la password di root), viene creato un file timestamp. Per default, un'autenticazione riuscita è memorizzata per cinque minuti. In questo periodo di tempo qualsiasi altra applicazione configurata per utilizzare `pam_timestamp` ed essere eseguita dalla stessa sessione viene autenticata automaticamente, senza che l'utente debbe immettere di nuovo la password di root.

Questo modulo è incluso nel pacchetto `pam`. Per abilitare questa funzionalità, il file di configurazione PAM in `etc/pam.d/` deve includere le seguenti righe:

```
auth sufficient /lib/security/pam_timestamp.so
session optional /lib/security/pam_timestamp.so
```

La prima riga che inizia con `auth` deve trovarsi dopo qualsiasi altra riga `auth sufficient` e la riga che inizia con `session` deve trovarsi dopo qualsiasi riga `session optional`.

Se un'applicazione configurata per utilizzare `pam_timestamp` viene autenticata con successo dal pulsante del **Menu principale** (sul pannello), l'icona  è visualizzata nell'area di notifica del pannello se è in esecuzione l'ambiente desktop GNOME. Allo scadere dell'autenticazione (il valore predefinito è cinque minuti), l'icona scompare.

L'utente può scegliere di dimenticare l'autenticazione memorizzata facendo clic sull'icona e selezionando l'opzione relativa.

24.7. Il gruppo `floppy`

Se, per qualsiasi ragione, l'accesso alla console non è adeguato per voi e vi occorre autorizzare l'accesso di utenti non root all'unità floppy del sistema, potete utilizzare il gruppo `floppy`. È sufficiente aggiungere l'utente al gruppo `floppy` usando un tool di vostra scelta. Riportiamo un esempio di come usare `gpasswd` per aggiungere l'utente Fred al gruppo `floppy`:

```
[root@bigdog root]# gpasswd -a fred floppy
Adding user fred to group floppy
[root@bigdog root]#
```

Adesso l'utente Fred può accedere all'unità floppy del sistema dalla console.

Capitolo 25.

Configurazione di utenti e gruppi

Utente Manager vi consente di visualizzare, modificare, aggiungere e cancellare utenti e gruppi locali.

Per utilizzare **Utente Manager**, è necessario avviare il sistema X Window, disporre dei privilegi di root e avere installato il pacchetto RPM `redhat-config-users`. Per avviare **Utente Manager** dal desktop selezionate **Pulsante del Menù principale** (sul Pannello) => **Impostazioni di sistema** => **Utenti e Gruppi** oppure digitate il comando `redhat-config-users` al prompt della shell (per esempio in un terminale XTerm o GNOME).

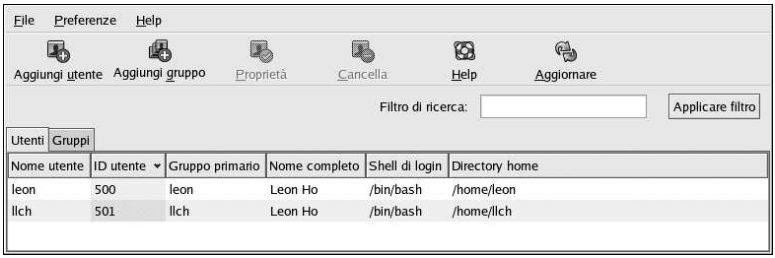

Figura 25-1. Utente Manager

Per visualizzare un elenco di tutti gli utenti locali sul sistema, fate clic sulla scheda **Utenti**. Per visualizzare un elenco di tutti i gruppi locali sul sistema, fate clic sulla scheda **Gruppi**.

Se desiderate un utente o un gruppo specifico, digitate le prime lettere del nome nel campo del **Filtro di Ricerca**. Premete [Invio] o fate clic sul pulsante **Applica filtro**. L'elenco filtrato viene visualizzato.

Per ordinare gli utenti o i gruppi, fate clic sul nome della colonna. Gli utenti o i gruppi saranno ordinati in funzione del valore di quella colonna.

Red Hat Linux riserva gli ID degli utenti al di sopra di 500 per gli utenti di sistema. Per default, **Utente Manager** non visualizza gli utenti di sistema. Per visualizzare tutti gli utenti, dunque anche quelli di sistema, togliete la spunta da **Preferenze => Filtra utenti e gruppi di sistema** dal menù a tendina.

Per maggiori informazioni su utenti e gruppi, consultate la *Red Hat Linux Reference Guide* e *Red Hat Linux System Administration Primer*.

25.1. Aggiunta di un nuovo utente

Per aggiungere un nuovo utente, fate clic sul pulsante **Aggiungi utente**. Come illustrato nella Figura 25-2 viene visualizzata una nuova finestra. Digitate il nome utente e il nome completo del nuovo utente nei rispettivi campi. Digitate la password dell'utente nei campi **Password** e **Confermare password** e ricordatevi che deve contenere almeno sei caratteri.

Suggerimento

Più la password è lunga, più risulta difficile che qualcuno la indovini e si connetta al vostro account senza permesso. Non utilizzate come password una parola comune, ma cercate di combinare lettere, numeri e caratteri speciali.

Selezionate una shell di accesso. Se non sapete quale scegliere, accettate quella predefinita (`/bin/bash`). La directory home predefinita è `/home/`*`nomeutente`*. È possibile modificare la directory home creata per l'utente oppure decidere di non crearla affatto, deselezionando l'opzione **Creare directory home**.

Se selezionate di creare la directory home, i file di configurazione predefiniti sono copiati dalla directory `/etc/skel` nella nuova directory home.

Red Hat Linux utilizza uno schema di *utente gruppo privato* (UPG). Lo schema UPG non aggiunge né modifica nulla nella gestione standard dei gruppi di UNIX. Quando aggiungete un nuovo utente, per default viene creato un unico gruppo con lo stesso nome dell'utente. Se non desiderate creare questo gruppo, deselezionate l'opzione **Creare un gruppo personale per l'utente**.

Per specificare un ID utente, selezionate **Specificare ID utente manualmente**. Se questa opzione non è selezionata, al nuovo utente viene assegnato il primo ID utente disponibile iniziando dal numero 500. Red Hat Linux riserva gli ID utenti al di sotto di 500 per gli utenti del sistema.

Fate clic su **OK** per creare l'utente.

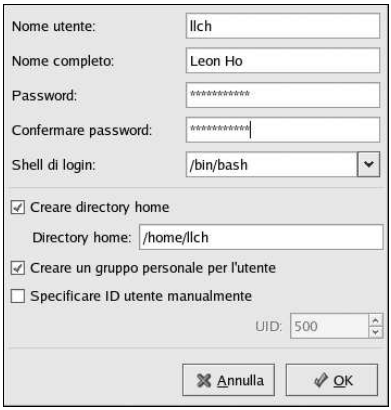

Figura 25-2. Nuovo utente

Per configurare proprietà più avanzate per l'utente, come per esempio la data di scadenza della password, modificate le proprietà dell'utente dopo averlo aggiunto. Per maggiori informazioni, consultate la Sezione 25.2.

Per aggiungere un utente in più gruppi, fate clic sulla scheda **Utenti**, selezionate l'utente e fate clic sul pulsante **Proprietà**. Nella finestra **Proprietà utente**, fate clic sulla scheda **Gruppi**. Infine selezionate i gruppi a cui volete aggiungere l'utente, selezionate il gruppo primario per l'utente e fate clic su **OK**.

25.2. Modifica delle proprietà dell'utente

Per visualizzare le proprietà di un utente già esistente, fate clic sulla scheda **Utenti**, selezionate l'utente interessato e **Proprietà** nel menù a pulsanti (oppure selezionate **File**ù> => **Proprietà** nel menù a tendina). Viene visualizzata una finestra come quella della Figura 25-3.

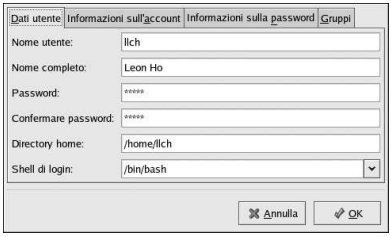

Figura 25-3. Proprietà dell'utente

La finestra **Proprietà utente** é divisa in pagine schedate multiple:

- **Dati utente** — fornisce informazioni di base configurate al momento dell'aggiunta dell'utente. Utilizzate questa scheda per modificare il nome completo, la password, la directory home o la shell di accesso dell'utente.
- **Informazioni sull'account** — selezionate l'opzione **Abilitare scadenza account** se desiderate che l'account abbia una determinata data di scadenza. Inserite la data nei relativi campi. Se selezionate **Account utente bloccato**, l'account viene bloccato e l'utente non è più in grado di accedere al sistema.
- **Informazioni sulla password** — Questa tabella visualizza la data dell'ultima modifica della password effettuata dall'utente. Per imporre la modifica della password dopo un determinato numero di giorni, selezionare **Abilitare scadenza password**. Potete inoltre modifcare i giorni prima del permesso di modifica,i giorni prima di avviso di modifica e i giorni prima della disattivazione dell'account.
- **Gruppi** — selezionate i gruppi a cui desiderate aggiungere l'utente e il suo gruppo primario.

25.3. Aggiunta di un nuovo gruppo

Per aggiungere un nuovo gruppo di utenti, fate clic sul pulsante **Aggiungi gruppo**. Compare una finestra simile a quella rappresentata nella Figura 25-4. Digitate il nome del gruppo che desiderate creare. Per specificare un ID per il nuovo gruppo, selezionate **Specificare ID gruppo manualmente** e selezionate la GID. Red Hat Linux riserva gli ID di gruppo inferiori a 500 per i gruppi di sistema.

Fate clic su **OK** per creare il gruppo. Il nuovo gruppo comparirà nell'elenco dei gruppi.

Figura 25-4. Nuovo gruppo

Per l'aggiunta di utenti al gruppo, consultate la Sezione 25.4.

25.4. Modifica delle proprietà del gruppo

Per visualizzare le proprietà di un gruppo esistente, selezionate il gruppo interessato e fate clic su **Proprietà** nel menù a pulsanti (oppure selezionate **Azione => Proprietà** dal menù a tendina). Viene visualizzata una finestra come quella della Figura 25-3.

Figura 25-5. Proprietà del gruppo

Nella scheda **Membri del gruppo** vengono elencati gli utenti che appartengono al gruppo. Selezionate altri utenti da aggiungere al gruppo e deselezionate gli utenti che invece desiderate rimuovere. Per applicare le modifiche, fate clic su **OK** oppure su **Applica**.

25.5. Configurazione dalla linea di comando

Se preferite i strumenti dalla linea di comando oppure non avete un sistema X installato, usate questo capitolo per configurare utenti e gruppi.

25.5.1. Aggiunta di utente

Per aggiungere un nuovo utente al sistema:

1. Usate il comando `useradd` per creare un account di utente bloccato:
   `useradd <username>`
2. Sblocchi l'account usando il comando `passwd` per assegnare una password e impostare la guida di riferimento per la scadenza:
   `passwd <username>`

le opzioni per la linea di comando per `useradd` sono nella Tabella 25-1.

Opzione	Descrizione
`-c commento`	Commento per l'utente
`-d dir-home`	La directory home da usare invece della predefinita directory `/home/nomeutente`
`-e date`	Data di scadenza dell'account nel formato AAAA-MM-GG

Opzione	Descrizione
`-f` *giorni*	Giorni prima della disattivazione dell'account dopo la scadenza della password. (Se **0** viene specificato, l'account viene disattivato immediatamente dopo la scadenza della password. Se **-1** viene specificato, l'account non sarà disattivato dopo la scadenza della password.)
`-g` *nome-gruppo*	Nome del gruppo o numero del gruppo per il gruppo predefinito dell'utente (Il gruppo deve esistere prima di specificarlo qui)
`-G` *elenco-gruppo*	Elenco di nomi o numeri di gruppi addizionali (tranne i predefiniti), separati da virgole, di cui l'utente è membro. (I gruppi devono esistere prima di specificarli qui.)
`-m`	Creare la directory home se non esiste.
`-M`	Non creare la directory home.
`-n`	Non creare un gruppo privato per l'utente.
`-r`	Creare un account di sistema con una UID minore a 500 e senza una directory home.
`-p` *password*	La password cifrata con `crypt`.
`-s`	La shell login dell'utente, predefinita come `/bin/bash`.
`-u` *uid*	La ID-Utente (UID) per l'utente, che deve essere unica e maggiore a 499.

Tabella 25-1. `useradd` Opzioni per la linea di comando

25.5.2. Aggiunta di un nuovo gruppo

Per aggiungere un nuovo gruppo al sistema, utilizzate il comando `groupadd`:

`groupadd <`*group-name*`>`

Le opzioni per la linea di comando per `groupadd` sono nella Tabella 25-2.

Opzione	Descrizione
`-g` *gid*	La ID-GRUPPO (GID) per il gruppo, che deve essere unica e maggiore a 499.
`-r`	Creare un gruppo di sistema con una GID minore a 500.
`-f`	Esci con un errore se il gruppo già esiste. (Il gruppo non viene modificato.) Se `-g` e `-f` sono specificate, ma il gruppo già esiste, la opzione `-g` non viene considerata.

Tabella 25-2. `groupadd` Opzioni per la linea di comando

25.5.3. Scadenza password

Per ragioni di sicurezza, é buona abitudine richiedere agli utenti di cambiare le loro password periodicamente. Questo puó essere fatto aggiungendo o modificando un utente sulla scheda **Informazione sulla password** di **Utente Manager**.

Per configurare la scadenza della password per un utente da un prompt della shell, utilizzate il comando, `chage`, seguito da una opzione nella Tabella 25-3, seguito dal nome utente per l'utente.

Importante

Le password shadow devono essere abilitati per usare il comando `chage`.

Opzione	Descrizione
`-m` *giorni*	Specificare il numero minimo di giorni prima della richiesta di modifica. Se il valore è 0, la password non scade.
`-M` *giorni*	Specificare il numero massimo di giorni per quale la password è valida. Quando il numero di giorni specificato da questa opzione più il numero di giorni specificato con la opzione `-d` è di meno che il giorno corrente, l'utente deve cambiare la sua password prima di poter usare questo account.
`-d` *giorni*	Specificare il numero di giorni dal primo gennaio, 1970 che la password è stata cambiata.
`-I` *days*	Specificare il numero di giorni inattivi dopo la scadenza della password prima di bloccare l'account. Se il valore è 0, l'account non viene bloccato dopo la scadenza della password.
`-E` *data*	Specificare la data in cui l'account viene bloccato, nel formato AAAA-MM-GG. Anzichè la data, il numero di giorni da January 1, 1970 può anche essere usato.
`-W` *giorni*	Specificare il numero di giorni prima di avviso di modifica.

Tabella 25-3. `change` Opzioni per la linea di comando

Suggerimento

Se il comando `chage` è seguito direttamente dal nome utente (senza opzioni), visualizza i valori per la scadenza della password corrente e consente di modificarli.

Se l'amministratore del sistema desidera che l'utente imposta una password quando accede al sistema per la prima volta, la password dell'utente può essere impostata cosichè scade immediatamente, forzando l'utente a modificare la password immediatamente dopo aver accesso al sistema per la prima volta.

Per forzare l'utente a configurare una password per la prima volta che accede al sistema mediante la console, seguite la procedura seguente. Nota bene, questo processo non funziona se l'utente accede al sistema mediante il protocollo SSH.

1. *Bloccare la password dell'utente* — se l'utente non esiste, usate il comando `useradd` per creare un account utente, ma non assegnate una password cosichè rimane bloccato.

   Se la password è già abilitata, bloccatela usando il comando:
   `usermod -L username`

2. *Forza immediatamente la scadenza della password* — Digitate il seguente comando:
   ```
   chage -d 0 username
   ```
   Questo comando sovrappone il valore della data dell'ultima modifica della password con l'epoca (Gennaio, 1 1970). Questo valore forza immediatamente la scadenza della password, a dispetto di qualsiasi polizza di scadenza che sia impostata.
3. *Sblocchi l'account* — Ci sono due metodi comuni a questo punto. L'amministratore può assegnare una password iniziale oppure una password di valore null.

   
   Attenzione

   Non usate il comando `passwd` per impostare la password poichè disattiva immediatamente la scadenza della password appena configurata.

   Per assegnare una password iniziale, usate la procedura seguente:

   - Avvia dalla linea di comando l'interprete `python` usando il comando `python`. Visualizza quanto segue:
     ```
     Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
     [GCC 3.2.1 20021207 (Red Hat Linux 8.0 3.2.1-2)] on linux2
     Type "help", "copyright", "credits" or "license" for more information.
     >>>
     ```
   - Al prompt, digitate il seguente (sostituendo *`password`* con la password cifrata e *`salt`* con una combinazione esatta di 2 caratteri alfabetici maiuscoli o minuscoli, numeri, il carattere puntino (.), oppure (/), come ad esempio: `ab` o `12`:
     ```
     import crypt; print crypt.crypt("password","salt")
     ```
     L'output è la password cifrata simile a `12CsGd8FRcMSM`.
   - Digitate [Ctrl]-[D] per uscire dall'interprete Python.
   - Tagliate e incollate l'output esatto della password cifrata, senza spazi all'inizio o alla fine, nel comando seguente:
     ```
     usermod -p "encrypted-password" username
     ```

   Invece di assegnare una password iniziale, una password di valore null può essere assegnata usando il comando:
   ```
   usermod -p "" username
   ```

   
   Avvertenza

   Mentre usando una password di valore null può essere conveniente per entrambi l'amministratore e l'utente, c'è un rischio minimo che una terza persona può accedere al sistema per prima. Per minimizzare questo rischio, è raccomandato che l'amministratore verifichi che l'utente è pronto ad accedere il sistema quando l'account viene sbloccato.

   Sia nell'uno che nell'altro, durante l'accesso iniziale al sistema, l'utente è richiesto di inserire una password nuova.

25.6. Spiegare il processo

I punti seguenti illustrano che cosa accade quando il comando `useradd juan` viene usato su un sistema che ha le password d'ombra abilitati:

1. Una nuova riga per `juan` è creata in `/etc/passwd`. La riga possiede le seguenti caratteristiche:
   - Inizia con il nome utente `juan`.

- C'è una `x` nel campo della password indicando che il sistema sta utilizzando le password d'ombra.
- Una UID a o superiore a 500 è creata. (In Red Hat Linux, le UID e le GID al di sotto di 500 sono riservati per il sistema.)
- Una GID a o superiore a 500 è creata.
- L'informazione facoltativa su GECOS è lasciata vuota.
- La home directory per `juan` è impostata come `/home/juan/`.
- La shell predefinita è impostata come `/bin/bash`.

2. Una nuova riga per `juan` è creata in `/etc/shadow`. La riga ha le seguenti caratteristiche:
   - Inizia con il nomeutente `juan`.
   - Due punti esclamativi (`!!`) comparono nel campo della password nel file `/etc/shadow`, che blocca l'account.

     

     Nota bene

     Se una password cifrata viene passata usando la bandierina `-p` , viene messa nel file `/etc/shadow` su una nuova riga per l'utente.

   - La password viene impostata per non scadere mai.

3. Una nuova riga per il gruppo chiamato `juan` è creato in `/etc/group`. Un gruppo con lo stesso nome dell'utente si chiama *gruppo privato di utente*. Per ulteriori infomazioni su gruppi privati di utente, consultate la Sezione 25.1.

   La riga creata in `/etc/group`ha le seguenti caratteristiche:
   - Inizia con il nome del gruppo `juan`.
   - Una `x` compare nel campo della password indicando che il sistema sta usando le password gruppi d'ombra.
   - La GID corrisponde a quella elencata per l'utente `juan` in `/etc/passwd`.

4. Una nuova riga per il gruppo chiamato `juan` viene creata in `/etc/gshadow`. La riga ha le seguenti caratteristiche:
   - Inizia con il nome del gruppo `juan`.
   - Un punto esclamativo (`!`) appare nel campo della password nel file `/etc/gshadow`, che blocca il gruppo.
   - Tutti gli altri campi sono vuoti.

5. Una directory per l'utente `juan` viene creata nella directory `/home/`. Questa directory è posseduta dall'utente `juan` e il gruppo `juan`. Tuttavia, i privilegi di lettura, scrittura ed esecuzione sono*solo* per l'utente `juan`. Tutti gli altri permessi sono negati.
6. I file all'interno della directory `/etc/skel/` (che contengono le impostazioni predefinite per l'utente) sono copiate nella nuova directory `/home/juan/`.

A questo punto, un account bloccato chiamato `juan` esiste nel sistema. Per attivarlo, l'amministratore deve assegnare una password all'account usando il comando `passwd` e, facoltativamente, impostare la guida di riferimento per la scadenza della password.

Capitolo 26.

Reperimento di informazioni sul sistema

Prima di imparare a configurare il sistema, raccogliete le informazioni essenziali sul sistema. Per esempio dovete sapere come trovare la quantità di memoria libera e di spazio su disco fisso, come viene partizionato il disco fisso e quali processi sono in esecuzione. Questo capitolo chiarisce come individuare questo tipo di informazioni dal sistema Red Hat Linux usando comandi e programmi semplici.

26.1. Processi di sistema

Il comando `ps ax` visualizza l'elenco dei processi in esecuzione sul sistema, tra cui i processi eseguiti da altri utenti. Per visualizzare chi esegue gli altri processi, utilizzate il comando `ps aux`. Si tratta di un elenco statico, ovvero di una sorta di "fotografia" dei processi in esecuzione nel momento in cui avete lanciato il comando. Se desiderate un elenco costantemente aggiornato dei processi in esecuzione, utilizzate il comando `top` come descritto qui sotto.

L'output `ps` può essere lungo. Per evitare che esca dallo schermo, potete collegarlo mediante less:

```
ps aux | less
```

Per vedere se un processo è in esecuzione, potete usare il comando `ps` con il comando `grep`. Per esempio, per determinare se **emacs** è in esecuzione, digitate il comando:

```
ps ax | grep emacs
```

Il comando `top` visualizza i processi attualmente in esecuzione e le informazioni importanti relative a tali processi, tra cui l'uso della memoria e della CPU. L'elenco visualizza i processi in tempo reale ed è interattivo. Un esempio dell'output di `top` viene fornito nel modo seguente:

```
 00:53:01  up 6 days, 14:05,  3 users,  load average: 0.92, 0.87, 0.71
71 processes: 68 sleeping, 2 running, 1 zombie, 0 stopped
CPU states:  18.0% user   0.1% system   16.0% nice   0.0% iowait  80.1% idle
Mem:  1030244k av,  985656k used,   44588k free,       0k shrd,  138692k buff
                    424252k actv,   23220k in_d,  252356k in_c
Swap: 2040212k av,  330132k used, 1710080k free                  521796k cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME COMMAND
15775 joe      5    0 11028  10M  3192 S     1.5  4.2   0:46 emacs
14429 root     15   0 63620  62M  3284 R     0.5 24.7  63:33 X
17372 joe      11   0  1056 1056   840 R     0.5  0.4   0:00 top
17356 joe      2    0  4104 4104  3244 S     0.3  1.5   0:00 gnome-terminal
    1 root     0    0   544  544   476 S     0.0  0.2   0:06 init
    2 root     0    0     0    0     0 SW    0.0  0.0   0:00 kflushd
    3 root     1    0     0    0     0 SW    0.0  0.0   0:24 kupdate
    4 root     0    0     0    0     0 SW    0.0  0.0   0:00 kpiod
    5 root     0    0     0    0     0 SW    0.0  0.0   0:29 kswapd
  347 root     0    0   556  556   460 S     0.0  0.2   0:00 syslogd
  357 root     0    0   712  712   360 S     0.0  0.2   0:00 klogd
  372 bin      0    0   692  692   584 S     0.0  0.2   0:00 portmap
  388 root     0    0     0    0     0 SW    0.0  0.0   0:00 lockd
  389 root     0    0     0    0     0 SW    0.0  0.0   0:00 rpciod
  414 root     0    0   436  432   372 S     0.0  0.1   0:00 apmd
  476 root     0    0   592  592   496 S     0.0  0.2   0:00 automount
```

Per uscire da `top`, premete il tasto [q].

Ecco alcuni comandi interattivi utili che potete usare con `top`:

Comando	Descrizione
[Spazio]	Aggiorna subito la visualizzazione
[h]	Visualizza una schermata di help
[k]	Termina un processo. Vi viene richiesto l'ID del processo e il segnale da inviargli.
[n]	Modifica il numero dei processi visualizzati. Vi viene chiesto di inserire un numero.
[u]	Ordina per utente.
[M]	Ordina per uso della memoria.
[P]	Ordina per uso di CPU.

Tabella 26-1. Comandi interattivi `top`

Suggerimento

Applicazioni come **Mozilla** e **Nautilus** sono in grado di *rilevare i thread* — cioè, vengono creati più thread per gestire più utenti o richieste e a ciascun thread viene assegnato un ID di processo. Di default, `ps` e `top` visualizzano solo il thread principale o iniziale. Per visualizzare tutti i thread, utilizzate il comando `ps -m` o premete [Maiusc]-[H] in `top`.

Se preferite un'interfaccia grafica per il comando `top`, potete utilizzare **GNOME System Monitor**. Per avviarlo in ambiente desktop, selezionate **Pulsante del menu Principale** (sul Pannello) => **Programmi => Sistema => Monitor di sistema** oppure digitate `gnome-system-monitor` al prompt della shell dal sistema X Window. Selezionate quindi la scheda **Process Listing**.

GNOME System Monitor vi consente di cercare il processo nell'elenco dei processi in esecuzione oltre a visualizzare tutti i processi, i vostri processi o i processi attivi.

Per ulteriori informazioni su un processo, selezionatelo e fate clic sul pulsante **More Info**. I dettagli relativi al processo verranno visualizzati nella parte inferiore della finestra.

Per interrompere un processo, selezionatelo e fate clic sul pulsante **End Process**. Questa funzione è utile per i processi che hanno smesso di rispondere all'input degli utenti.

Per ordinare le informazioni in una colonna specifica, fate clic sul sul nome della colonna che verrà visualizzato in un colore grigio più scuro.

Di default, **GNOME System Monitor** non visualizza i thread. Per modificare queste preferenze, selezionate **Edit => Preferences**, fate clic sulla scheda **Process Listing** e selezionate **Show Threads**. Le preferenze consentono inoltre di configurare l'intervallo di aggiornamento, il tipo di informazioni di default da visualizzare per ciascun processo e i colori delle immagini del monitor di sistema.

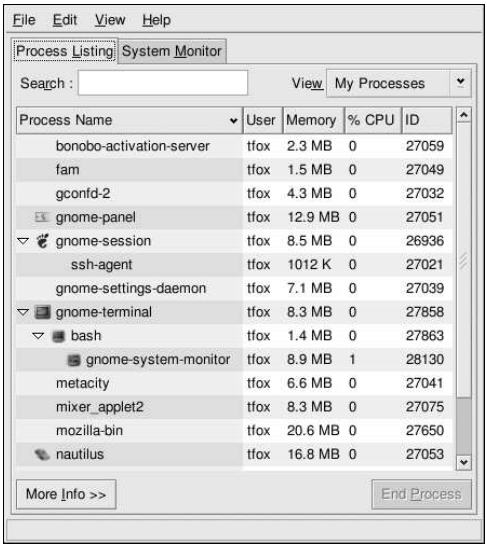

Figura 26-1. GNOME System Monitor

26.2. Uso della memoria

Il comando `free` visualizza la quantità totale di memoria fisica e di spazio swap per il sistema. Indica inoltre la quantità di memoria usata, libera, condivisa, nei buffer del kernel e cache.

```
             total       used       free     shared    buffers     cached
Mem:        256812     240668      16144     105176      50520      81848
-/+ buffers/cache:     108300     148512
Swap:       265032        780     264252
```

Il comando `free -m` mostra le stesse informazioni in megabyte, più semplici da leggere.

```
             total       used       free     shared    buffers     cached
Mem:           250        235         15        102         49         79
-/+ buffers/cache:        105        145
Swap:          258          0        258
```

Se preferite un'interfaccia grafica per il comando `free`, potete utilizzare **GNOME System Monitor**. Per avviarla dal desktop, selezionate **Pulsante del menu Principale** (sul Pannello) => **System Tools => System Monitor** o digitate `gnome-system-monitor` al prompt della shell dal sistema X Window. Scegliete poi la scheda **System Monitor**.

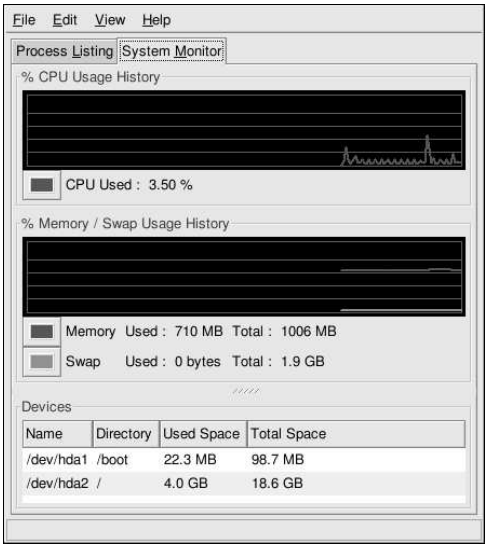

Figura 26-2. GNOME System Monitor

26.3. Filesystem

Il comando `df` indica l'uso dello spazio su disco del sistema. Se digitate questo comando al prompt della shell, l'output sarà simile al seguente:

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda2             10325716   2902060   6899140  30% /
/dev/hda1                15554      8656      6095  59% /boot
/dev/hda3             20722644   2664256  17005732  14% /home
none                    256796         0    256796   0% /dev/shm
```

Questa utility mostra, per default, le dimensioni delle partizioni in blocchi da 1 kilobyte e la quantità di spazio su disco usata e disponibile (sempre in kilobyte). Per visualizzare le informazioni in megabyte e in gigabyte, utilizzate il comando `df -h`. L'argomento `-h` indica un formato leggibile. L'output visualizzato è simile al seguente:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda2             9.8G  2.8G  6.5G  30% /
/dev/hda1              15M  8.5M  5.9M  59% /boot
/dev/hda3              20G  2.6G   16G  14% /home
none                  251M     0  250M   0% /dev/shm
```

Nell'elenco delle partizioni c'è una voce per `/dev/shm` che rappresenta il filesystem di memoria virtuale del sistema.

Il comando `du` mostra una stima della quantità di spazio utilizzata dai file in una directory. Se digitate `du` al prompt della shell, viene visualizzato in un elenco l'uso del disco per ogni sottodirectory. Inoltre, nell'ultima riga dell'elenco, viene indicato il totale per la directory attuale e quella delle sottodirectory. Se non desiderate vedere il totale per tutte le sottodirectory usate il comando `du -hs` per visualizzare

solo il totale per la directory in formato leggibile. Usate il comando `du --help` per visualizzare maggiori opzioni.

Per visualizzare le partizioni del sistema e l'utilizzo dello spazio su disco in un formato grafico, utilizzate la scheda **System Monitor** come illustrato nella parte inferiore della Figura 26-2.

Suggerimento

Per informazioni sull'implementazione del disk quotas, consultare Capitolo 6.

26.3.1. Monitoraggio dei filesystem

Red Hat Linux fornisce l'utility `diskcheck`, che controlla la quantità di spazio libero del disco sul sistema. In base al file di configurazione, l'utility invia un'e-mail all'amministratore del sistema quando uno o più dischi fissi raggiungono la capacità specificata. Per impiegare questa utility dovete avere installato il pacchetto RPM `diskcheck`.

Questa utility viene eseguita come un cron orario. [1]

Potete definire le seguenti variabili in `/etc/diskcheck.conf`:

- `defaultCutoff` — Indica quando il disco fisso raggiunge questa capacità percentuale. Per esempio, se `defaultCutoff = 90`, quando il disco fisso monitorato raggiunge una capacità del 90% verrà inviata un'e-mail.
- `cutoff[`*`/dev/partition`*`]` — Sovrascrive il valore `defaultCutoff` per la partizione. Per esempio, se è specificato `cutoff['/dev/hda3'] = 50`, `diskcheck` avviserà l'amministratore del sistema qualora la partizione `/dev/hda3` raggiunga la capacità del 50%.
- `cutoff[`*`/mountpoint`*`]` — Sovrascrive il valore `defaultCutoff` per i mount point. Per esempio, se è specificato `cutoff['/home'] = 50`, `diskcheck` avviserà l'amministratore del sistema qualora il mount point `/home` raggiunga la capacità del 50%.
- `exclude` — Specifica una o più partizioni che devono essere ignorate da `diskcheck`. Se, per esempio, è specificato `exclude = "/dev/sda2 /dev/sda4"`, `diskcheck` non avvisa l'amministratore di sistema quando `/dev/sda2` o `/dev/sda4` raggiungono la percentuale specificata.
- `ignore` — Specifica uno o più tipi di filesystem da ignorare nel formato `-x` *`filesystem-type`*. Se, per esempio, è specificato `ignore = "-x nfs -x iso9660"`, l'amministratore di sistema non riceve alcun avviso quando i filesystem nfs o iso9660 raggiungono la capacità indicata.
- `mailTo` — Indirizzo e-mail dell'amministratore di sistema da utilizzare quando le partizioni e i mount point raggiungono la capacità specificata. Per esempio, se è specificato `mailTo = "webmaster@example.com"`, gli avvisi verranno inviati a webmaster@example.com.
- `mailFrom` — Specifica l'identità del mittente dell'e-mail. Questo si rivela uno strumento utile se l'amministratore del sistema desidera filtrare i messaggi di `diskcheck`. Per esempio, se è specificato `mailFrom = "Disk Usage Monitor"`, questo sarà il mittente del messaggio.
- `mailProg` — Specifica il programma di posta da utilizzare per inviare gli avvisi e-mail. Per esempio, se è specificato `mailProg = "/usr/sbin/sendmail"`, Sendmail sarà usato come programma di posta.

Se cambiate il file di configurazione non è necessario riavviare il servizio poiché il file viene letto ogni volta che il task cron è in esecuzione. Il servizio `crond` deve essere installato perché le attività cron siano eseguite. Per determinare se il demone è installato, utilizzate il comando `/sbin/service`

1. Fate riferimento a Capitolo 28 per ulteriori informazioni su cron.

`crond status`. È consigliabile eseguire il servizio al momento dell'avvio. Per ulteriori informazioni sull'esecuzione automatica del servizio cron in fase di avvio, consultate il Capitolo 14.

26.4. Hardware

Se avete problemi nel configurare il vostro hardware o volete semplicemente sapere quale hardware è presente sul vostro sistema, potete utilizzare l'applicazione **Browser Hardware** per visualizzare l'hardware che è possibile rilevare. Per lanciare il programma dal desktop, selezionate **Pulsante del menu principale => System Tools => Hardware Browser** o digitate `hwbrowser` al prompt della shell. Come mostrato nella Figura 26-3, verranno visualizzati i lettori CD-ROM, i floppy disk, i dischi fissi e le relative partizioni, i dispositivi di rete, di puntamento e di sistema nonché le schede video. Per visualizzare le informazioni, fate clic sulla categoria che vi interessa nel menu di sinistra.

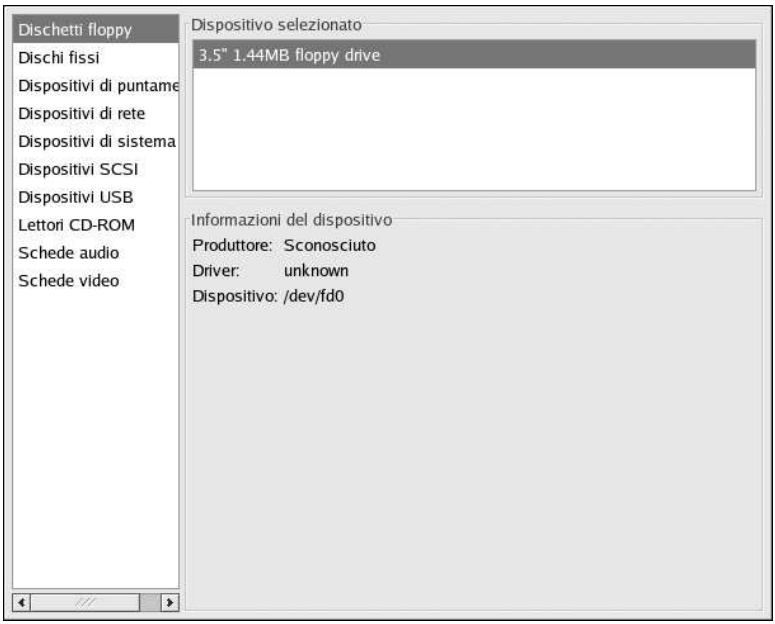

Figura 26-3. Browser Hardware

Potete anche utilizzare il comando `lspci` per ottenere un elenco di tutti i dispositivi PCI. Se volete informazioni più dettagliate usate il comando `lspci -v`;. Per output più complessi occorre il comando `lspci --v`.

`lspci` può essere utilizzato per determinare produttore, modello e memoria di una scheda video di sistema:

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04) (prog-
if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max
Flags: medium devsel, IRQ 16
Memory at f4000000 (32-bit, prefetchable) [size=32M]
```

```
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

Il comando `lspci` è anche utile per determinare la scheda di rete del sistema se non è noto il produttore o il numero del modello.

26.5. Risorse aggiuntive

Per maggiori informazioni sulla raccolta di informazioni sul sistema, consultate le risorse elencate qui di seguito.

26.5.1. Documentazione installata

- `ps --help` — visualizza un elenco di opzioni che può essere utilizzato con `ps`.
- Pagina man di `top` — digitate `man top` per maggiori informazioni sul comando `top` e sulle numerose opzioni relative.
- Pagina man di `free` — digitate `man free` per maggiori informazioni sul comando `free` e sulle relative opzioni.
- Pagina man di `df` — digitate `man df` per maggiori informazioni sul comando `df` e sulle relative opzioni.
- Pagina man di `du` — digitate `man du` per maggiori informazioni sul comando `du` e sulle relative opzioni.
- `lspci` pagina manual — Digitare `man lspci` per saperne di piú sul comando `lspci` e sulle sue numerose opzioni.
- `/proc` — i contenuti della directory `/proc` possono anche essere utilizzati per raccogliere informazioni di sistema più dettagliate. Per maggiori informazioni su questa directory, consultate la *Red Hat Linux Reference Guide*.

26.5.2. Related Books

- *Red Hat Linux System Administration Primer*; Red Hat, Inc. — Include un capitolo sul controllo delle risorse.

Capitolo 27.
Configurazione della stampante

Lo **Strumento di configurazione della stampante** permette agli utenti di configurare una stampante in Red Hat Linux. Questo tool aiuta a gestire il file di configurazione della stampante, le direttori spool e i filtri di stampa.

Iniziando con la versione 9, default di Red Hat Linux per il sistema di stampa CUPS. Il sistema precedente di default di stampa LPRng, viene ancora fornito. Se il sistema fosse stato migliorato da una versione precedente di Red Hat Linux usando LPRng, il procedimento di miglioramento non avrá sostituito LPRng con CUPS; il sistema continuerá ad usare LPRng.

Se il sistema é stato migliorato da una versione precedente di Red Hat Linux usando CUPS, il processo di miglioramento non avrá intaccato le code precedentemente configurate, e il sistema continuerá ad usare CUPS.

Lo **Strumento di configurazione della stampante** configura entrambi i sistemi di stampa CUPS e LPRng, a seconda del tipo di configurazione usato dal sistema. Quando si apportano modifiche, viene configurato il sistema di stampa attivo.

Per usare lo **Strumento di configurazione della stampante** dovete avere i privilegi root. Per iniziare un'applicazione, selezionare **Pulsante del menu principale** (sul pannello) => **Impostazioni del sistema => stampa**, o inserire il comando `redhat-config-printer`. Questo comando determina automaticamente se eseguire la versione grafica o di testo, a seconda se il comando viene eseguito da un ambiente X Window grafico oppure da una console di testo.

Potete anche forzare **Strumento di configurazione della stampante** ad eseguire come se fosse un'applicazione di testo, usando il comando `redhat-config-printer-tui` dal prompt della shell.

Importante

Non modificate il file `/etc/printcap` o i file nella directory `/etc/cups/`. Ogni volta che il demone della stampante (`lpd` o `cups`) viene avviato o riavviato, vengono creati dinamicamente, nuovi file di configurazione. I suddetti file vengono altresí creati quando vengono apportati cambiamenti con **Strumento di configurazione della stampante**.

Se state usando LPRng e volete aggiungere una stampante senza usare **Strumento di configurazione della stampante**, modificate il file `/etc/printcap.local`. Le entry non vengono mostrate in `/etc/printcap.local` ma vengono lette dal demone della stampante. Se avete effettuato un miglioramento del vostro sistema da una versione Red Hat Linux precedente, il vostro file di configurazione esistente, é stato convertito al nuovo formato usato da questa applicazione. Ogni volta che un nuovo file di configurazione viene generato, il vecchio file viene salvato come `/etc/printcap.old`.

Se state usando CUPS, **Strumento di configurazione della stampante** non mostra alcuna coda o condivisione che non é stata configurata usando **Strumento di configurazione della stampante**; tuttavia non rimuovendole dal file di configurazione.

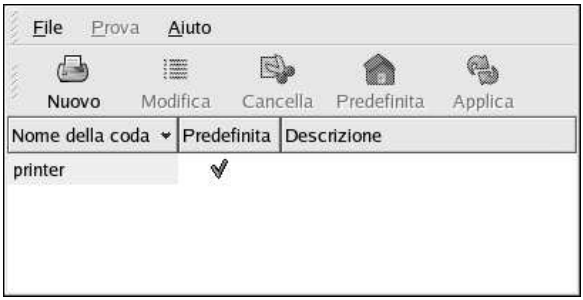

Figura 27-1. Strumento di configurazione della stampante

Le seguenti code di stampa possono essere configurate:

- **Collegata-localmente** — Una stampante collegata direttamente al computer attraversi una porta parallela o USB.
- **CUPS Rete (IPP)** — Una stampante collegata ad un sistema CUPS diverso che puó essere accesso attraverso una rete TCP/IP (per esempio, una stampante collegata ad un altro sistema Red Hat Linux che esegue CUPS sulla rete).
- **UNIX Rete (LPD)** — Una stampante collegata ad un sistema UNIX diverso che puó essere accesso tramite una rete TCP/IP (per esempio, una stampante collegata ad un altro sistema Red Hat Linux che esegue LPD sulla rete).
- **Windows Rete (SMB)** — Una stampante collegata ad un sistema diverso il quale condivide una stampante attraverso una rete SMB (per esempio, una stampante collegata ad una macchina Microsoft Windows).
- **Novell Rete (NCP)** — Una stampante collegata ad un sistema diverso il quale usa una tecnologia di rete NetWare di Novell.
- **JetDirect Rete** — Una stampante collegata direttamente alla rete attraverso HP JetDirect invece di un computer.

Importante

Se aggiungete una nuova coda di stampa o modificate una giá esistente, siete richiesti a confermare i cambiamenti.

Facendo clic sul pulsante **Applica**, salvate qualsiasi cambiamento che avete apportato riavviando il demone della stampante. I cambiamenti non verranno scritti sul file di configurazione fino a quando il demone della stampante non viene riavviato. Alternativamente, potete scegliere **File => Salva cambiamenti** e poi scegliere **Action => Applica**.

27.1. Aggiunta di una stampante locale

Per aggiungere una stampante locale, come ad esempio una stampante collegata attraverso una porta parallela o una porta USB al vostro computer, fate clic sul pulsante **Nuovo** nella finestra principale **Strumento di configurazione della stampante** per visualizzare la finestra in Figura 27-2. Fate clic su **Avanti** per procedere.

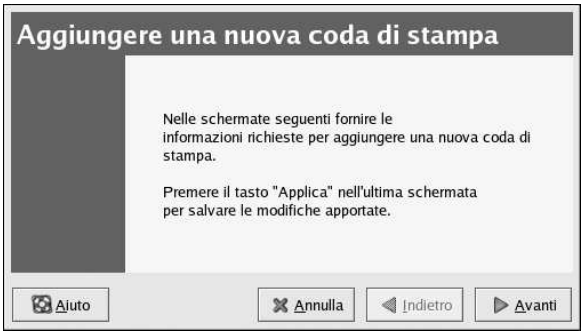

Figura 27-2. Aggiunta di una stampante

Nella finestra mostrata in Figura 27-3, inserire un nome unico per la stampante nel campo di testo **Nome**. Il nome della stampante non puó contenere spazi e deve iniziare con una lettera. Il suddetto nome puó contenere lettere, numeri, trattini (-), e line (_). Facoltativo, inserire una breve descrizione della stampante, la quale puó contenere spazi.

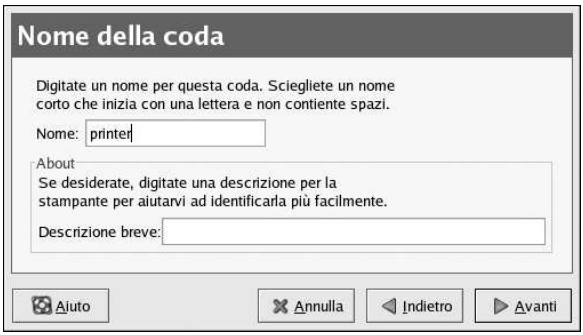

Figura 27-3. Selezionare un nome della coda

Dopo aver fatto clic su **Avanti**, apparirá Figura 27-4. Selezionare **Collegato-localmente** dal menu **Selezionare un tipo di coda**, e scegliere il dispositivo. Il dispositivo é generalmente `/dev/lp0` per una stampante parallela o `/dev/usb/lp0` per una stampante USB. Se non appare nella lista alcun dispositivo, fate clic su **Riesamina dispositivi** per riesaminare il computer o fate clic su **Personalizza dispositivo** per specificarlo manualmente. Fate clic su **Avanti** per continuare.

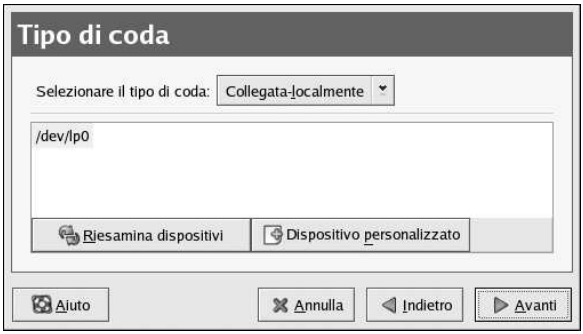

Figura 27-4. Aggiunta di una stampante locale

La fase successiva é quella di selezionare il tipo di stampante. Per continuare, andate su la Sezione 27.7

27.2. Aggiunta di una stampante CUPS Rete (IPP)

Una stampante CUPS Rete (IPP) é una stampante collegata ad un sistema Linux diverso sulla stessa rete che esegue CUPS. Per default **Strumento di configurazione della stampante** controlla la rete per qualsiasi stampante CUPS condivisa. (Questa opzione puó essere cambiata dalla scheda **Generale** dopo aver selezionato **Action => Condividere** dal menu a tendina.) Qualsiasi stampante CUPS di rete appare nella finestra principale come una coda giá controllata.

Se avete configurato un firewall sul server di stampa, esso sará in grado di inviare e ricevere collegamenti sulla porta di entrata UDP, 631. Se avete invece un firewall configurato sul client (il computer che invia la richiesta di stampa), esso deve essere abilitato ad inviare e ricevere connessioni sulla porta 631.

Se disabilitate il contenuto del browsing automatico, potete ancora aggiungere una stampante CUPS rete, ció é possibile facendo clic sul pulsante **Nuovo** nella finestra principale **Strumento di configurazione della stampante** per mostrare la finestra in Figura 27-2. Fate clic su **Avanti** per procedere.

Nella finestra mostrata in Figura 27-3, inserire un nome unico per la stampante nel campo di testo **Nome**. Il nome della stampante non puó contenere spazi e deve iniziare con una lettera. Il suddetto nome puó contenere lettere, numeri, trattini (-), e line (_). Facoltativo, inserire una breve descrizione della stampante, la quale puó contenere spazi.

Dopo aver fatto clic su **Avanti**, apparirá Figura 27-5. Selezionate **CUPS rete (IPP)** dal menu **Selezionare un tipo di coda**.

Figura 27-5. Aggiunta di una stampante CUPS rete (IPP)

Appaiono le seguenti opzioni per i campi di testo:

- **Server** — L'hostname o l'indirizzo IP della macchina remota alla quale la stampante é collegata.
- **Percorso** — Il percorso per la coda di stampa sulla macchina remota.

Fate clic su **Avanti** per continuare.

La fase successiva é quella di selezionare il tipo di stampante. Per continuare, andate su la Sezione 27.7

Importante

Il server di stampa CUPS rete, deve permettere il collegamento dal sistema locale. Consultare la Sezione 27.13 per maggiori informazioni.

27.3. Aggiunta di una stampante remota UNIX (LPD)

Per aggiungere una stampante remota UNIX, come ad esempio una stampante collegata ad un sistema Linux differente ma sulla stessa rete, fate clic sul pulsante **Nuovo** nella finestra principale **Strumento di configurazione della stampante**. ApparirÃ¡ una finestra, come mostrato in Figura 27-2. Fate clic su **Avanti** per procedere.

Nella finestra mostrata in Figura 27-3, inserire un nome unico per la stampante nel campo di testo **Nome**. Il nome della stampante non puó contenere spazi e deve iniziare con una lettera. Il suddetto nome puó contenere lettere, numeri, trattini (-), e line (_). Facoltativo, inserire una breve descrizione della stampante, la quale puó contenere spazi.

Selezionare **Networked UNIX (LPD)** dal menu **Selezionare un tipo di coda**, e fate clic su **Avanti**.

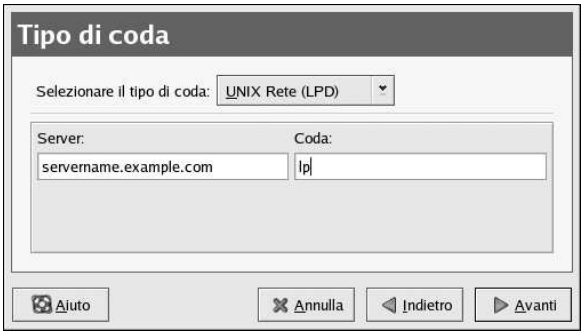

Figura 27-6. Aggiunta di una stampante remota UNIX (LPD)

Appaiono i campi di testo per le seguenti opzioni:

- **Server** — l'hostname o l'indirizzo IP di macchine remote alle quali la stampante Ã© collegata.
- **Coda** — La coda della stampante remota. La coda di default della stampante Ã© generalmente `lp`.

Fate clic su **Avanti** per continuare.

La fase successiva é quella di selezionare il tipo di stampante. Per continuare, andate su la Sezione 27.7

Importante

Il server remoto della stampante deve accettare i lavori di stampa assegnati dal sistema locale. Consultate la Sezione 27.13.1 per maggiori informazioni.

27.4. Aggiungere una stampante Samba (SMB)

Per aggiungere una stampante accessa usando il protocollo SMB (come ad esempio una stampante collegata direttamente ad un sistema Microsoft Windows), fate clic sul pulsante **Nuovo** nella finestra **Strumento di configurazione della stampante** principale. Apparirá una finestra come mostrato in Figura 27-2. Fate clic su **Avanti** per procedere.

Nella finestra mostrata in Figura 27-3, inserire un nome unico per la stampante nel campo di testo **Nome**. Il nome della stampante non puó contenere spazi e deve iniziare con una lettera. Il suddetto nome puó contenere lettere, numeri, trattini (-), e line (_). Facoltativo, inserire una breve descrizione della stampante, la quale puó contenere spazi.

Selezionare **Networked Windows (SMB)** dal menu **Selezionare un tipo di coda**, a fate clic su **Avanti**. Se la stampante é collegata ad un sistema Microsoft Windows, scegliere questo tipo di coda.

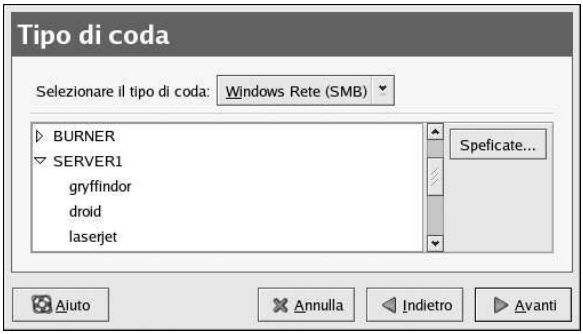

Figura 27-7. Aggiunta di una stampante SMB

Come mostrato in Figura 27-7, le condivisioni share sono automaticamente rilevate ed elencate. Fate clic sulla freccetta vicino ad ogni nome per ingrandire la lista. Dalla suddetta lista, selezionate una stampante.

Se la stampante che state cercando non é presente nella lista, fate clic sul pulsante **Specificare** sulla destra. Appariranno per le seguenti opzioni dei campi di testo:

- **Workgroup** — Il nome del workgroup di Samba per la stampante condivisa.
- **Server** — Il nome del server che condivide la stampante.
- **Share** — Il nome della stampante condivisa sulla quale desiderate stampare. Il nome deve essere simile a quello definito della stampante Samba sulla macchina Windows remota.
- **Nome utente** — Il nome dell'utente usato per effettuare il login alla stampante. Questo utente deve esistere nel sistema Windows, e lo stesso utente deve avere permesso di accesso alla stampante. Il nome utente di default é tipicamente **`ospite`** per i server Windows, o **`nessuno`** per server di Samba.
- **Password** — La password (se richiesta) per l'utente specificato nel campo **Utente**.

Fate clic su **Avanti** per continuare. Lo **Strumento di configurazione della stampante** cerca poi di collegarsi alla stampante condivisa. Se la stessa stampante richiede un nome utente e una password, apparirá una finestra di dialogo richiedendovi di fornire un nome utente e una password validi. Se viene fornito un nome di condivisione errato, é possibile cambiarlo in questo istante. Se viene richiesto un nome di workgroup per collegarsi alla condivisione, potete specificarlo in questa finestra di dialogo. Essa é la stessa di quella mostrata quando si effettua un clic sul pulsante **Specificare**

La fase successiva é quella di selezionare il tipo di stampante. Per continuare, andate su la Sezione 27.7

Warning

Se richiedete un nome utente e una password, esse sono contenute in chiaro solo in file leggibili da utenti root e lpd. Cosí, é solo possibile per gli altri utenti conoscere la password ed il nome utente solo se hanno accesso root. Per evitare questo, sia il nome utente che la password usati per accedere alla stampante, devono essere diversi da quelli usati per accedere all'account utente sul sistema Red Hat Linux locale. Se sono diversi, l'unico compromesso sarebbe l'uso non autorizzato della stampante. Se ci sono delle condivisioni di file dal server, é consigliato che anch'essi usino password diverse da quella della coda di stampa.

27.5. Aggiungere una stampante Novell NetWare (NCP)

Per aggiungere una stampante Novell NetWare (NCP), fate clic sul pulsante **Nuovo** nella finestra **Strumento di configurazione della stampante** principale. Apparirá la finestra mostrata in Figura 27-1. Fate clic su **Avanti** per procedere.

Nella finestra mostrata in Figura 27-3, inserire un nome unico per la stampante nel campo di testo **Nome**. Il nome della stampante non puó contenere spazi e deve iniziare con una lettera. Il suddetto nome puó contenere lettere, numeri, trattini (-), e line (_). Facoltativo, inserire una breve descrizione della stampante, la quale puó contenere spazi.

Selezionare **Networked Novell (NCP)** dal menu **Selezionare un tipo di coda**.

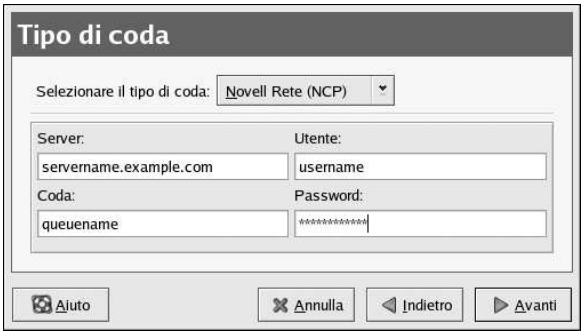

Figura 27-8. Aggiungere una stampante NCP

Appariranno i seguenti campi di testo:

- **Server** — l'hostname o l'indirizzo IP del sistema NCP al quale la stampante é collegata.
- **Coda** — La coda remota per la stampante sul sistema NCP
- **Utente** — Il nome dell'utente utilizzato per effettuare un login per l'accesso alla stampante.
- **Password** — La password per l'utente specificata nel campo sopra indicato **Utente**.

La fase successiva é quella di selezionare il tipo di stampante. Per continuare, andate su la Sezione 27.7

Warning

Se richiedete un nome utente e una password, esse sono contenute in chiaro solo in file leggibili da utenti root e lpd. Cosí, é solo possibile per gli altri utenti conoscere la password ed il nome utente solo se hanno accesso root. Per evitare questo, sia il nome utente che la password usati per accedere alla stampante, devono essere diversi da quelli usati per accedere all'account utente sul sistema Red Hat Linux locale. Se sono diversi, l'unico compromesso sarebbe l'uso non autorizzato della stampante. Se ci sono delle condivisioni di file dal server, é consigliato che anch'essi usino password diverse da quella della coda di stampa.

27.6. Aggiunta di una stampante JetDirect

Per aggiungere una stampante JetDirect, fate clic sul pulsante **Nuovo** nella finestra principale **Strumento di configurazione della stampante**. Apparirá la finestra come mostrata su Figura 27-1. Fate clic su **Successivo** per procedere.

Nella finestra mostrata in Figura 27-3, inserire un nome unico per la stampante nel campo di testo **Nome**. Il nome della stampante non puó contenere spazi e deve iniziare con una lettera. Il suddetto nome puó contenere lettere, numeri, trattini (-), e line (_). Facoltativo, inserire una breve descrizione della stampante, la quale puó contenere spazi.

Selezionare **JetDirect rete** dal menu **Selezionare un tipo di coda**, e fate clic su **Avanti**.

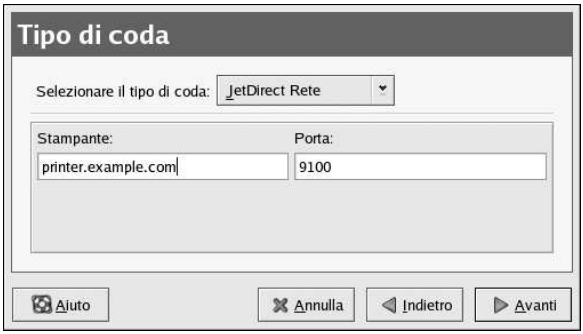

Figura 27-9. Aggiunta di una stampante JetDirect

Appaiono i seguenti campi di testo:

- **Stampante** — l'hostname o l'indirizzo IP della stampante JetDirect.
- **Porta** — La porta sulla stampante JetDirect che é in ascolto per la stampa dei lavori. La porta di default é 9100.

La fase successiva é quella di selezionare il tipo di stampante. Per continuare, andate su la Sezione 27.7

27.7. Selezione e conferma del modello di stampante

Dopo aver selezionato il tipo di coda della stampante, potete selezionare il modello della stampante.

Visualizzerete una finestra simile a Figura 27-10. Se non é stata rilevata automaticamente, selezionare il modello dalla lista. Le stampanti sono suddivise in base alle ditte produttrici. Selezionare il nome della ditta dal menu a tendina. I modelli della stampante vengono aggiornati ogni qualvolta si seleziona una ditta. Selezionare il modello di stampante dalla lista.

Figura 27-10. Selezionare un modello di stampante

Il driver di stampa viene selezionato in base al modello di stampante selezionato. Il suddetto driver processa i dati che desiderate stampare in un formato comprensibile alla stampante. Dato che stampante locale é collegata direttamente al vostro computer, avete bisogno che il driver di stampa processi i dati inviati alla stampante.

Se state configurando una stampante remota (IPP, LPD, SMB, o NCP), il server di stampa remoto generalmente ha i propri driver di stampa. Se ne selezionate uno aggiuntivo sul vostro computer locale, i dati vengono filtrati piú volte e convertiti in un formato che la stampante puó comprendendere.

Per assicurarsi che i dati non vengano filtrati piú di una volta, tentate di selezionare prima **Generico** come fornitore e **Raw Print Queue** o **Stampante postscript** come modello. Dopo aver confermato i cambiamenti, effettuate un test di stampa per provare questa nuova configurazione. Se avete un esito negativo, il server di stampa remoto potrabbe non avere configurato il driver di stampa. Tentate quindi di selezionare il driver in accordo al fornitore e modello della stampa remota, confermate i cambiamenti ed effettuate un test di stampa.

Suggerimento

Potete selezionare un driver diverso dopo aver aggiunto una stampante, avviando **Strumento di configurazione della stampante**, selezionando la stampante dalla lista, e effettuando un clic su **Modifica**, facendo clic successivamente sulla scheda **Driver**, selezionando un driver diverso e confermando poi i cambiamenti.

27.7.1. Conferma della configurazione della stampante

L'ultimo passo é quello di confermare la configurazione della stampante. Fare clic su **Applica** per aggiungere la coda di stampa se le impostazioni sono corrette. Fate clic su **Indietro** per modificare la configurazione.

Fate clic sul pulsante **Applica** nella finestra principale per salvare i cambiamenti e riavviare il demone della stampante. Dopo aver confermato i cambiamenti, effettuate una stampa test per assicurarsi che la configurazione sia quella corretta. Consultare la Sezione 27.8 per maggiori informazioni.

Se avete bisogno di effettuare una stampa dei caratteri oltre il set di base ASCII (includendo quelli usati per le lingue come il giapponese), dovete allora rivedere le opzioni del driver e selezionare **Prerender Postscript**. Consultare la Sezione 27.9 per maggiori informazioni. Potete configurare anche le opzioni inerenti la misura della carta, se modificate la coda di stampa dopo averla aggiunta.

27.8. Stampa di una pagina test

Dopo aver configurato la vostra stampante, dovreste stampare una pagina test per assicurarsi che la stampante funzioni propriamente. Per stampare una pagina test, selezionare la stampante che desiderate provare e selezionate la pagina test appropriata dal menu a tendina **Test**.

Se cambiate il driver di stampa o modificate le opzioni del driver, dovreste stampare una pagina test per provare le diverse configurazioni.

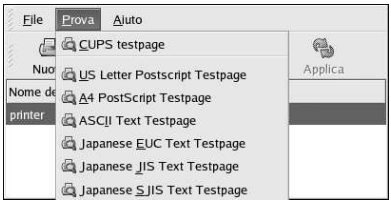

Figura 27-11. Opzioni della pagina test

27.9. Modifica delle stampanti giá esistenti

Per cancellare una stampante giá esistente, selezionare la stampante e fate clic sul pulsante **Cancella** sulla barra degli strumenti. La stampante viene cosí rimossa dalla lista. Fate clic su **Applica** per salvare i cambiamenti e riavviare il demone della stampante.

Per impostare una stampante di default, selezionate la stampante dalla lista e fate clic sul pulsante di **Default** sulla barra degli strumenti. L'icona della stampante di default appare nella collonna **Default** della stampante di default nella lista.

Dopo aver aggiunto la stampante, si possono modificare le impostazioni selezionando la stampante dalla lista e facendo clic sul pulsante **Modifica**. Verrá visualizzata la finestra mostrata in Figura 27-12. La suddetta finestra contiene i valori attuali per la stampante selezionata. Apportare i cambiamenti e fare clic sul pulsante **OK**. Fare clic su **Applica** nella finestra **Strumento di configurazione della stampante** principale per salvare i cambiamenti e riavviare il demone della stampante.

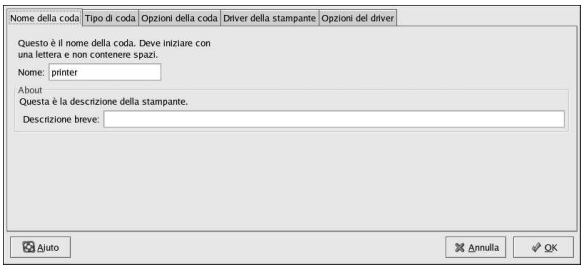

Figura 27-12. Modifica di una stampante

27.9.1. Nome della coda

Per rinominare una stampante o cambiare la sua descrizione, cambiare il valore nella scheda **Nome della coda**. Fate clic su **OK** per ritornare alla finestra principale. Il nome della stampante nella lista,

a questo punto dovrebbe essere diverso. Fare clic su **Applica** per salvare i cambiamenti e riavviare il demone della stampante.

27.9.2. Tipo di coda

La scheda **Tipo di coda** mostra il tipo di coda selezionato durante l'aggiunta della stampante e delle sue impostazioni. Esso puó essere cambiato oppure si possono cambiare solo le impostazioni. Dopo aver apportato le modifiche, fate clic su **OK** per ritornare alla finestra principale. Fate clic su **Applica** per salvare le modifiche e riavviare il demone.

A seconda della scelta del tipo di coda, vengono visualizzate diverse opzioni. Fate riferimento alle sezioni appropriate sull'aggiunta di una stampante e per una descrizione delle opzioni.

27.9.3. Driver della stampante

La scheda **driver della stampante** mostra quale driver della stampante é correntemente usato. Se é cambiato, fate clic su **OK** per ritornare alla finestra principale. Fate clic su **Applica** per salvare il cambiamento e riavviare il demone.

27.9.4. Opzioni del Driver

La scheda **Opzioni del driver** mostra le opzioni avanzate della stampante. Le opzioni variano ad ogni driver. Le opzioni comuni includono:

- **Send Form-Feed (FF)** dovrebbe essere selezionato se l'ultimo lavoro di stampa non é stato stampato (per esempio, se lampeggia la lucetta form feed). Se ció non funziona, provate a selezionare **invio End-of-Transmission (EOT)**. Alcune stampanti richiedono entrambi **Invio Form-Feed (FF)** e **invio End-of-Transmission (EOT)** per stampare o emettere l'ultima pagina. Questa opzione é solo disponibile con il sistema di stampa LPRng.
- **Invio End-of-Transmission (EOT)** se l'invio di un form-feed non dá i risultati voluti. Fate riferimento a **Invio Form-Feed (FF)**. Questa opzione é solo disponibile con il sistema di stampa LPRng.
- **Supponete che i dati sconosciuti siano di testo** dovrebbe essere selezionato se il driver non riconosce alcuni dei dati da lui ricevuti. Selezionate questa opzione solo se si verificano dei problemi nella stampa. Se si seleziona questa opzione, il driver assume che ogni dato non riconosciuto é un testo e tenterá di stamparlo come testo. Se questa opzione viene selezionata con l'opzione **Converti il testo in postscript** il driver assume che i dati sconosciuti siano dei testi e li converte in PostScript. Questa opzione é solo disponibile con il sistema di stampa LPRng.
- **Prepara Postscript** dovrebbe essere selezionato solo quando i caratteri oltre agli ASCII di base impostati, sono stati inviati alla stampante ma non vengono stampati correttamente (come ad esempio i caratteri in giapponese). Questa opzione prepara le font PostScript non-standard in modo tale da stamparle in modo corretto.

  Se la stampante non supporta le font che state cercando di stampare, provate a selezionare questa opzione. Per esempio, selezionate questa opzione per stampare le font in giapponese in una stampante non-giapponese.

  Piú tempo viene richiesto per effettuare questa operazione. Non selezionatela a meno che non ci siano problemi nella stampa.

  Selezionate anche questa opzione se la stampante non puó sostenere Il level 3 di PostScript.
- **GhostScript pre-filtering** — vi permette di selezionare **No pre-filtering**, **Convertire a PS level 1**, oppure **Convertire a PS level 2** nel caso in cui la stampante non sostiene alcuni livelli. Questa opzione é solo disponibile se il driver PostScript viene usato con il sistema di stampa CUPS.

- **Converti il testo in postscript** viene selezionato per default. Se la stampante puó stampare documenti in plain text per diminuire il tempo richiesto per stampare. Si si usa il sistema di stampa CUPS, questa non é una opzione perché il testo viene sempre cambiato in postscript.
- **Misura della pagina** permette la selezione della misura della pagina. Le opzioni includono Lettere US, US Legal, A3, e A4.
- **Filtro locale in funzione** default a **C**. Se sono stati stampati i caratteri giapponesi, selezionare **ja_JP**. Altrimanti, accettare il default di **C**.
- **Media Source** default a **Stampante di default**. Cambia questa opzione per utilizzare carta da un vassoio diverso.

Per modificare le opzioni del driver, fare clic su **OK** per ritornare alla finestra principale. Fate clic su **Applica** per salvare i cambiamenti e riavviare il demone della stampante.

27.10. Salvare il file di configurazione

Una volta salvata la configurazione della stampante usando **Strumento di configurazione della stampante**, l'applicazione crea il proprio file di configurazione usato per creare i file nella directory `/etc/cups` (o il file `/etc/printcap` letto da `lpd`). Potete usare le opzioni della linea di comando per salvare o ripristinare il file **Strumento di configurazione della stampante**. Se la directory `/etc/cups` o il file `/etc/printcap` sono salvati e ripristinati nelle stesse posizioni, la configurazione della stampante non deve essere ripristinata in quanto ogni volta che il demone della stampante viene riavviato, crea un nuovo file `/etc/printcap` dal file di configurazione speciale **Strumento di configurazione della stampante**. Quando si crea un backup dei file di configurazione del sistema, usare il seguente metodo per salvare i file di configurazione della stampante. Se il sistema stá usando LPRng e sono state aggiunte le impostazioni personalizzate nel file `/etc/printcap.local`, dovrebbe essere salvato come parte del sistema di backup.

Per salvare la configurazione della vostra stampante, digitare questo comando come un utente root:

```
/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
```

La vostra configurazione é salvata nel file `settings.xml`.

Se questo file é salvato, puó essere usato per ripristinare le impostazioni della stampante. Ció é utile se la configurazione della stampante é stata cancellata, se Red Hat Linux é installato nuovamente, oppure se la stessa configurazione é necessaria su sistemi multipli. Il file dovrebbe essere salvato su di un sistema diverso prima della reinstallazione. Per creare la configurazione, digitare questo comando come un utente root:

```
/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
```

Se giá avete un file di configurazione (ne avete giá configurato uno o piú stampanti sul sistema) e cercate di importare un altro file di configurazione, il file di configurazione giá esistente, sará sovrascritto. Se volete mantenere la configurazione esistente e aggiungere la configurazione nel file salvato, potete unire i file, con il seguente comando (come utente root):

```
/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
```

La lista della vostra stampante consisterá nelle stampanti che avete configurato sul sistema e delle stampanti che sono state importate dal file di configurazione salvato. Se il suddetto file possiede una coda di stampa con lo stesso nome di un'altra coda nel sistema, la coda di stampa del file importato sovrascriverá quella della stampante giá esistente.

Dopo aver importato il file di configurazione (con o senza il comando `merge`), dovete avviare nuovamente il demone della stampante. Se state usando CUPS, emettete il comando:

```
/sbin/service cups restart
```

Se state usando LPRng, emettete il comando:

```
/sbin/service lpd restart
```

27.11. Configurazione della linea di comando

Se non avete il sistema X e desiderate usare una versione basata su testo, potete aggiungere una stampante tramite la linea di comando. Questo metodo é utile se volete aggiungere una stampante da uno script o nella sezione %post di una installazione di tipo Kickstart.

27.11.1. Aggiunta di una stampante locale

Per aggiungere una stampante:

```
redhat-config-printer-tui --Xadd-local options
```

Opzioni:

--device=*node*

(Richiesto) Il nodo del dispositivo da usare. Per esempio, `/dev/lp0`.

--make=*make*

(Necessario) La stringa IEEE 1284 MANUFACTURER oppure il nome della ditta produttrice della stampante inteso come database foomatic se la stringa della fabbrica stessa non é disponibile.

--model=*model*

(Necessario) La stringa IEEE 1284 MODEL oppure il modello della stampante riportato nel database foomatic se la stringa del modello stesso non é disponibile.

--name=*name*

(Facoltativo) Il nome da dare alla nuova coda. Se non é stato ancora dato, sará usato un nome basato sul nodo del dispositivo (come ad esempio “lp0”).

--as-default

(Facoltativo) Impostatelo come coda di default.

Se state usando come sistema di stampa CUPS (di default), dopo aver aggiunto la stampante, usare il seguente comando per iniziare/riavviare il demone della stampante:

```
service cups restart
```

Se state usando come sistema di stampa LPRng, dopo aver aggiunto la stampante, usare il seguente comando per iniziare/riavviare il demone della stampante:

```
service lpd restart
```

27.11.2. Rimuovere una stampante locale

La coda di una stampante puó essere rimossa anche tramite la linea di comando.

Come utente root, per rimuovere la coda di una stampante:

```
redhat-config-printer-tui --Xremove-local options
```

Opzioni:

--device=*node*

(Necessario) Il nodo del dispositivo usato come ad esempio `/dev/lp0`.

--make=*make*

(Necessario) La stringa IEEE 1284 MANUFACTURER, oppure (se non é disponibile) il nome della ditta produttrice inteso come database foomatic.

--model=*model*

(Necessario) La stringa IEEE 1284 MODEL, oppure (se non é disponibile) il modello della stampante come riportato nel database foomatic.

Se state usando come sistema di stampa CUPS (di default), dopo aver rimosso la stampante dalla configurazione di **Strumento di configurazione della stampante** riavviate il demone della stampante per confermare i cambiamenti:

```
service cups restart
```

Se state usando come sistema di stampa LPRng, dopo aver rimosso la stampante dalla configurazione di **Strumento di configurazione della stampante**, riavviare il demone della stampante per confermare i cambiamenti:

```
service lpd restart
```

Se state usando CUPS, rimosso tutte le stampanti e non volete piú eseguire il demone della stampante, eseguire il seguente comando:

```
service cups stop
```

Se state usando LPRng, rimosso tutte le stampanti e non desiderate piú eseguire il demone della stampante, eseguire il seguente comando:

```
service lpd stop
```

27.12. Gestione lavori di stampa

Quando inviate un lavoro di stampa al demone di una stampante, come ad esempio la stampa del file di testo da **Emacs** oppure la stampa d'immagine da **Il GIMP**, il suddetto lavoro viene aggiunto allo spool di coda di stampa. Lo spool di coda di stampa é una lista di lavori che viene inviata alla stampante e con essa vengono inviati anche informazioni inerenti ogni richiesta di stampa, come ad esempio la condizione di stampa, il nome dell'utente che ha inviato la richiesta, l'hostname del sistema che invia la richiesta, il numero di lavoro ecc.

Se state eseguendo un ambiente desktop grafico, fate clic sull'icona **Print manager** sul pannello per avviare il **Gnome Print Manager** come mostrato in Figura 27-13.

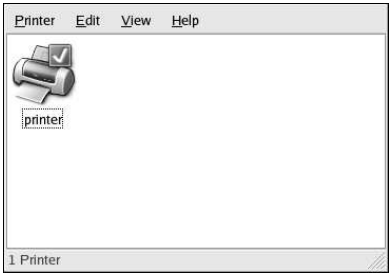

Figura 27-13. Gnome Print Manager

Puó essere avviato selezionando **Pulsante menu principale** (sul pannello) => **Tool del sistema** => **Print Manager**.

Per cambiare le impostazioni della stampante, fate clic col pulsante destro del mouse, sull'icona per la stampante e selezionare **Proprietá**. Il **Strumento di configurazione della stampante** viene avviato.

Fate un doppio clic su di una stampante configurata, per visualizzare lo spool della coda di stampa come mostrato in Figura 27-14.

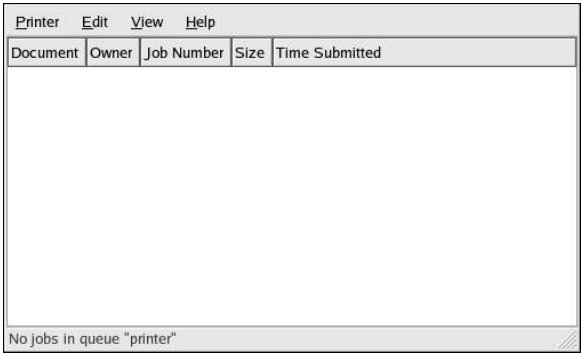

Figura 27-14. Lista dei lavori di stampa

Per cancellare un lavoro di stampa specifico riportato nel **Gnome Print Manager**, selezionarlo dalla lista e selezionare poi **Modifica** => **Cancella Documenti** dal menu a tendina.

Se ci sono lavori di stampa attivi nello spool di stampa, potrebbe apparire una icona di notifica nell'**Area di notifica del pannello** del pannello desktop come mostrato in Figura 27-15. Poiché vá alla ricerca ogni cinque secondi di lavori di stampa attivi, l'icona puó non essere visualizzata per lavori di stampa brevi.

Figura 27-15. Icona di notifica della stampante

Effettuando un clic sull'icona di notifica della stampante, si avvia il **Gnome Print Manager** a visualizzare una lista di lavori attuali.

Posizionato anche sul pannello vi é l'icona del **Print Manager**. Per stampare un file da **Nautilus**, effettuare una ricerca della posizione del file ed effettuare un drag e drop del file stesso sull'icona **Print Manager** sul pannello. Viene visualizzata una finestra, come mostrato in Figura 27-16. Fate clic su **OK** per iniziare la stampa del file.

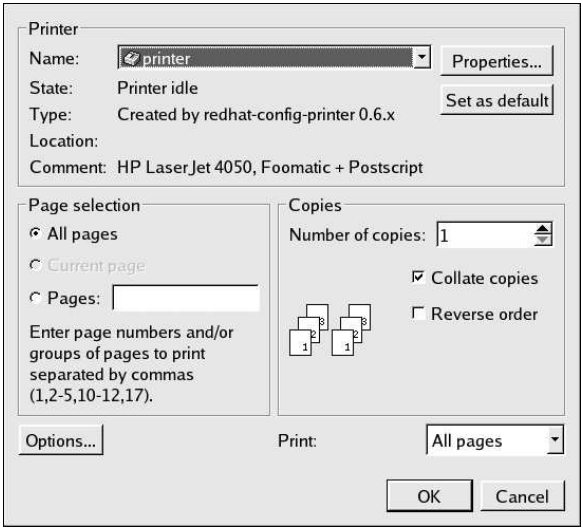

Figura 27-16. Finestra di verifica della stampa

Per visualizzare la lista dei lavori di stampa nella spool di stampa dal prompt della shell digitare il comando `lpq`. Le ultime righe saranno simili a quanto segue:

```
Rank    Owner/ID            Class  Job Files       Size Time
active user@localhost+902     A    902 sample.txt  2050 01:20:46
```

Esempio 27-1. Esempio di risposta `lpq`

Se volete annullare un lavoro di stampa, cercate il numero della richiesta con il comando `lpq` per poi usare il comando `lprm` *`job number`*. Per esempio, `lprm 902` cancellerá il lavoro di stampa in Esempio 27-1. Dovete avere dei permessi idonei per cancellare un lavoror di stampa. Non potete cancellare alcuna lavoro avviato da altri utenti a meno che non siate un utente root sulla macchina alla quale la stampante e collegata.

Potete anche stampare un file direttamente dal prompt della shell. Per esempio, il comando `lpr sample.txt` stamperá il file di testo `sample.txt`. Il filtro di stampa determina il tipo di file e lo converte in un formato comprensibile dalla stampante.

27.13. Condividere una stampante

L'abilitá dello **Strumento di configurazione della stampante** di condividere le opzioni di configurazione puó essere usata solo se usate un sistema di stampa CUPS. Per configurare la condivisione per LPRng, far riferimento a la Sezione 27.13.1.

Permettere agli utenti su di un computer diverso sulla rete, a stampare da una stampante configurata per il vostro sistema, viene chiamato *condividere* la stampante. Per default, le stamparti configurate con lo **Strumento di configurazione della stampante** non sono condivise.

Per condividere una stampante configurata, avviare lo **Strumento di configurazione della stampante** e selezionare una stampante dalla lista. Selezionare poi **Aziona => Condividere** dal menu a tendina.

Nota Bene

Se una stampante non viene selezionata, **Aziona** => **Condividere** mostra solo le opzioni di condivisione del sistema, normalmente mostrate sotto la scheda **Generale**

Sulla scheda della **Coda**, selezionare l'opzione per rendere la coda disponibile ad altri utenti.

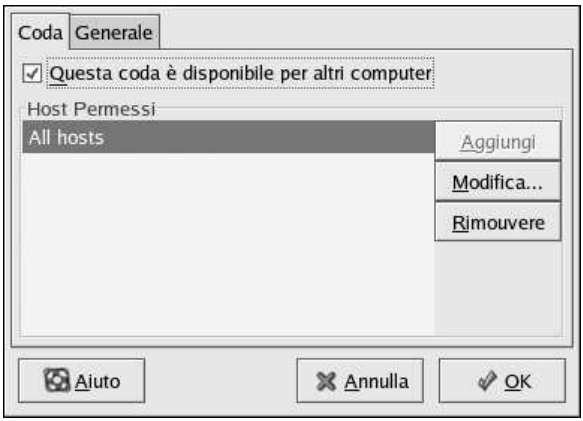

Figura 27-17. Opzioni della coda

Dopo aver selezionato di condividere la coda, di default, *tutti* gli host sono autorizzati a stampare dalla stampante condivisa. Permettendo tutti i sistemi sulla rete, puó essere pericoloso, specialmente se il sistema é direttamente collegato a Internet. É consigliato cambiare questa opzione selezionando la entry **Tutti gli host** e facendo clic sul pulsante **Modifica** per visualizzare la finestra mostrata in Figura 27-18.

Se avete configurato un firewall sul server di stampa, deve essere in grado di inviare e ricevere collegamenti sulla porta di ingresso UDP, 631. Se avete configurato un firewall sul client (il computer che invia una richiesta di stampa), esso deve essere abilitato a inviare e accettare connessioni sulla porta 631.

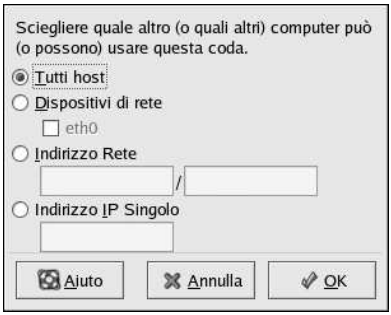

Figura 27-18. Host autorizzati

La scheda **Generale** configura le impostazioni per tutte le stampanti, incluse quelle non visibili con lo **Strumento di configurazione della stampante**. Ci sono due opzioni:

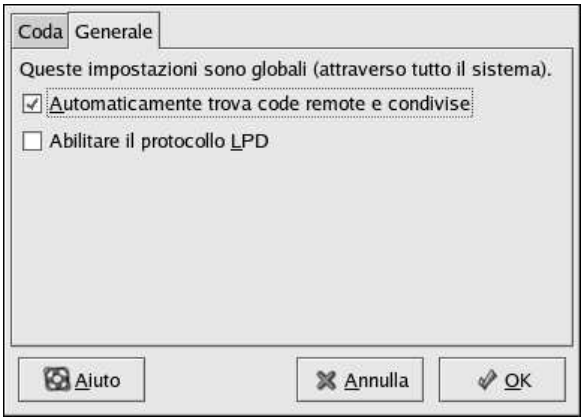

Figura 27-19. Opzioni di condivisione del sistema

- **Trova automaticamente le code remote di condivisione** — Selezionato per default, questa opzione permette il browsing IPP, ció significa che quando altre macchine sulla rete trasmettono le code da loro possedute, le code vengono aggiunte automaticamente alla lista di stampanti disponibili al sistema; non é richiesta alcuna configurazione aggiuntiva per una stampante trovata dal browsing IPP. Questa opzione non condivide automaticamente le stampanti configurate sul sistema locale.
- **Abilita il protocollo LPD** — Questa opzione permette ad una stampante di ricevere i lavori di stampa dai client configurati ad usare il protocollo LPD usando il servizio `cups-lpd`, il quale é un servizio `xinetd`.

Attenzione

Se questa opzione é abilitata, tutti i lavori di stampa sono accettati da tutti gli host, se ricevuti da un client LPD.

27.13.1. Condividere una stampante con LPRng

Se state eseguendo il sistema di stampa LPRng, la condivisione deve essere configurata manualmente. Per permettere ai sistemi sulla rete di stampare da una stampante configurata su di un sistema Red Hat Linux, seguire le seguenti fasi:

1. Creare il file `/etc/accepthost`. In questo file, aggiungere l'indirizzo IP o l'hostname del sistema sul quale desiderate permettere l'accesso per la stampa, con una linea per IP o hostname.
2. Non commentare "uncomment" in `/etc/lpd.perms`: la seguente riga
   `ACCEPT SERVICE=X REMOTEHOST=</etc/accepthost`
3. Riavviare il demone per confermare i cambiamenti:
   `service lpd restart`

27.14. Cambiare i sistemi di stampa

Per cambiare i sistemi di stampa, eseguite l'applicazione **Switcher del sistema di stampa**. Iniziatelo selezionando **Pulsante menu principale** (sul pannello) => **Impostazioni del sistema => Piú impostazioni del sistema => Switcher del sistema di stampa**, oppure digitare il comando `redhat-switch-printer` al prompt della shell (per esempio, in un XTerm o in un GNOME terminal).

Il programma rileva automaticamente se il sistema X Window é operativo. Se lo é il programma avvia la modalitá grafica come mostrato in Figura 27-20. Se X non viene rilevato, viene allora avviata la modalitá di testo. Per forzarlo ad operare come una applicazione di testo, usare il comando `redhat-switch-printer-nox`.

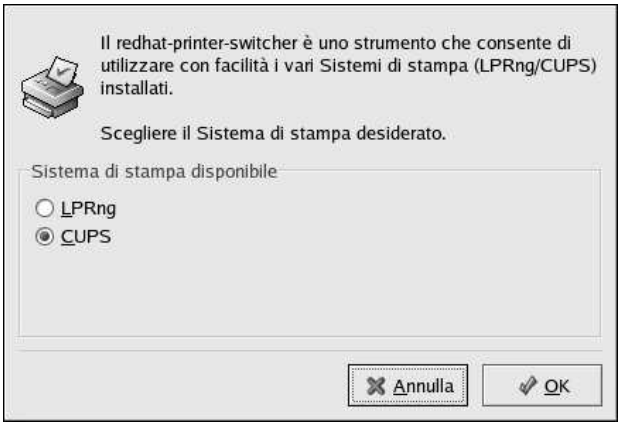

Figura 27-20. Switcher del sistema di stampa

Selezionare il sistema di stampa **LPRng** oppure **CUPS**. In Red Hat Linux 9, CUPS é il default. Se avete installato solo un sistema di stampa, é la sola opzione mostrata.

Se selezionate **OK** per cambiare il sistema di stampa, il demone selezionato é in grado di iniziare al momento dell'avvio "boot time", ed il demone che non é stato selezionato viene disabilitato in modo tale da non iniziare. Il demone selezionato dunque viene avviato, mentre l'altro resta inattivo, in modo tale i cambiamenti saranno effettivi da subito.

27.15. Risorse aggiuntive

Per saperne di piú sulla stampa con Red Hat Linux, fate riferimento alle seguenti risorse.

27.15.1. Documentazione installata

- `man printcap` — La pagina del manuale per il file di configurazione della stampante `/etc/printcap`.
- `map lpr` — La pagina del manuale per il comando `lpr` che vi permette di effettuare una stampa dalla linea di comando.
- `man lpd` — La pagina del manuale per il demone della stampante LPRng.
- `man lprm` — La pagina del manuale per la utility della linea di comando per rimuovere i lavori di stampa dalla spool di coda LPRng.
- `man mpage` — La pagina del manuale per la utility della linea di comando per la stampa multipla di pagine su di un foglio di carta.
- `man cupsd` — La pagina del manuale per il demone della stampante CUPS.
- `man cupsd.conf` — La pagina del manuale per il file di configurazione del demone della stampante CUPS.
- `man classes.conf` — La pagina del manuale per il file di configurazione della classe per CUPS.

27.15.2. Siti Web utili

- http://www.linuxprinting.org — *stampare con GNU/Linux* contiene una larga gamma d'informazioni sulla stampa con Linux.
- http://www.cups.org/ — Documentazione, FAQ, e newsgroup inerenti CUPS.

Capitolo 28.

Operazioni pianificate

Su Linux, è possibile configurare il sistema affinché alcune operazioni vengano eseguite in modo automatico entro un determinato periodo di tempo o in giorni stabiliti. Red Hat Linux è già preconfigurato per l'esecuzione di alcune operazioni di aggiornamento del sistema. Per esempio, il database slocate viene aggiornato quotidianamente tramite il comando `locate`. Un amministratore di sistema può utilizzare le operazioni pianificate per eseguire backup periodici, controllare il sistema, eseguire script personalizzati e altro.

Red Hat Linux è fornito con quattro utility per l'esecuzione automatica di operazioni: `cron`, `anacron`, `at` e `batch`.

28.1. Cron

Cron è un demone che può essere utilizzato per eseguire operazioni pianificate in base all'ora, al giorno del mese, al mese, al giorno della settimana e alla settimana.

Cron presuppone che il sistema sia sempre acceso. In caso contrario, quando è pianificata un'operazione, questa non viene eseguita. Per configurare le operazioni in base ai periodi anzichè all'ora esatta, consultate la Sezione 28.2. Per pianificare operazioni da eseguire una sola volta, consultate la Sezione 28.3.

Per usufruire dei servizi di cron, è necessario installare il pacchetto RPM `vixie-cron` e il servizio `crond` deve essere in esecuzione. Per stabilire se il pacchetto è già installato, digitate il comando `rpm -q vixie-cron`. Per determinare se il servizio è in esecuzione, digitate il comando `/sbin/service crond status`.

28.1.1. Come configurare le operazioni con Cron

Il file di configurazione più importante di cron, `/etc/crontab`, contiene le righe seguenti:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

Le prime quattro righe sono variabili utilizzate per configurare l'ambiente in cui vengono eseguite le operazioni di cron. Il valore della variabile `SHELL` indica al sistema quale ambiente shell utilizzare (bash shell, nell'esempio) e la variabile `PATH` definisce il percorso utilizzato per eseguire i comandi. L'output delle operazioni cron viene inviato tramite e-mail al nome utente definito con la variabile `MAILTO` Se in questa variabile non viene specificato nulla (`MAILTO` o viene definita come stringa vuota (`MAILTO=""`), non verrà inviata alcuna e-mail. La variabile `HOME` può essere utilizzata per impostare la directory home per l'esecuzione di comandi o script.

Ogni riga nel file `/etc/crontab` rappresenta un'operazione e ha il formato seguente:

```
minute   hour   day   month   dayofweek   command
```

- `minute` — qualsiasi numero intero da 0 a 59;
- `hour` — qualsiasi numero intero da 0 a 23;
- `day` — qualsiasi numero intero da 1 a 31 (deve essere un giorno valido per il mese specificato);
- `month` — qualsiasi numero intero da 1 a 12 (o abbreviazione del nome del mese, come gen, feb e così via);
- `dayofweek` — qualsiasi numero intero da 0 a 7 in cui 0 o 7 rappresenta la domenica (oppure l'abbreviazione del giorno come dom, lun e così via);
- `command` — è il comando da eseguire (può essere un comando come `ls /proc >> /tmp/proc` oppure un comando scritto da voi per eseguire uno script).

Per qualsiasi valore tra quelli sopra descritti, può essere utilizzato un asterisco (*) che rappresenta tutti i valori validi. Per esempio, un asterisco per il valore del mese indica di eseguire il comando ogni mese in base alle restrizioni degli altri valori.

Un trattino (-) tra numeri interi specifica un intervallo di numeri interi. Per esempio **`1-4`** indica un intervallo che comprende i numeri interi 1, 2, 3 e 4.

Una serie di valori separati da virgole (,) determina un elenco. Per esempio **`3, 4, 6, 8`** indica questi quattro numeri interi.

La barra (/) può essere usata per specificare valori che devono essere ignorati. Per omettere un numero entro un intervallo è necessario aggiungerlo alla fine dell'intervallo in questo modo: **`/`**<**`numero`**>. Per esempio **`0-59/2`** può essere usato per definire ogni minuto nel campo dei minuti. I valori da omettere possono essere usati anche con un asterisco. Per esempio, il valore **`*/3`** può essere usato nel campo dei mesi per eseguire l'operazione ogni tre mesi.

Le righe che iniziano con un carattere cancelletto (#) sono considerate commenti e, pertanto, non vengono elaborate.

Come potete notare, il file `/etc/crontab`, utilizza lo script `run-parts` per eseguire gli script nelle directory `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly`, rispettivamente su base oraria, giornaliera, settimanale o mensile. I file in queste directory dovrebbero essere script della shell.

Se un'operazione di cron deve essere eseguita con una programmazione diversa da quella oraria, giornaliera, settimanale o mensile, potete aggiungerla nella directory `/etc/cron.d`. Tutti i file in questa directory utilizzano la stessa sintassi di `/etc/crontab`. Per ulteriori esempi, consultate Esempio 28-1.

```
# record the memory usage of the system every monday
# at 3:30AM in the file /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# run custom script the first day of every month at 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

Esempio 28-1. Esempi di crontab

Gli utenti diversi da root possono configurare le operazioni di cron usando l'utility `crontab`. Tutti i crontab definiti dall'utente vengono salvati nella directory `/var/spool/cron` ed eseguiti usando il nome utente di chi li ha creati. Per creare un crontab con un determinato utente, connettetevi al sistema con il nome di questo utente e digitate il comando `crontab -e` per modificare il crontab utilizzando l'editor specificato nella variabile d'ambiente `VISUAL` o `EDITOR`. Il file utilizza lo stesso formato di `/etc/crontab`. Una volta salvate le modifiche al crontab, questo viene salvato in base al nome dell'utente e scritto nel file `/var/spool/cron/`*`nomeutente`*.

Il demone cron controlla il file `etc/crontab`, la directory `/etc/cron.d/` e la directory `/var/spool/cron` ogni minuto per rilevare eventuali modifiche. Se vengono rilevate delle

modifiche, il file e le directory vengono ricaricati in memoria. Tuttavia, se un file crontab viene modificato, non è necessario riavviare il demone cron.

28.1.2. Controllo dell'accesso al Cron

I file `/etc/cron.allow` e `/etc/cron.deny` consentono di limitare l'accesso a cron. Il formato di entrambi i file è costituito da un nome utente su ciascuna riga. Non possono essere lasciati spazi vuoti. Il demone cron (`crond`) non deve essere riavviato se i file di controllo dell'accesso vengono modificati. Questi file sono letti ogni volta che un utente cerca di aggiungere o eliminare un'operazione cron.

L'utente root può sempre usare cron, indipendentemente dai nomi degli utenti elencati nei file di controllo dell'accesso.

Se il file `cron.allow` esiste, solo gli utenti qui elencati possono usare cron e il file `cron.deny` viene ignorato.

Se `cron.allow` non esiste, tutti gli utenti elencati nel file `cron.deny` non sono autorizzati a usare cron.

28.1.3. Avvio e interruzione del servizio

Per avviare il servizio cron utilizzate il comando `/sbin/service crond start`, per interromperlo, utilizzate invece il comando `/sbin/service crond stop`. Si raccomanda di eseguire il servizio al momento dell'avvio. Per maggiori dettagli sull'esecuzione automatica del servizio cron all'avvio, consultate il Capitolo 14.

28.2. Anacron

Anacron è un'utility che consente di pianificare le operazioni, molto simile a cron salvo per il fatto che non richiede il funzionamento continuo del sistema. Può essere utilizzato per eseguire con cadenza giornaliera, settimanale e mensile i processi normalmente eseguiti da cron.

Per utilizzare il servizio Anacron, è necessario installare il pacchetto RPM `anacron` e il servizio `anacron` deve essere in esecuzione. Per determinare se il pacchetto è installato, utilizzate il comando `rpm -q anacron`. Per verificare se il servizio è in esecuzione, utilizzate il comando `/sbin/service anacron status`.

28.2.1. Configurazione delle operazioni di Anacron

Le operazioni di Anacron sono elencate nel file di configurazione `/etc/anacrontab`. Ogni riga nel file di configurazione corrisponde a un'operazione e ha il seguente formato:

```
period   delay   job-identifier  command
```

- `period` — frequenza (in giorni) per l'esecuzione del comando.
- `delay` — indica il ritardo in minuti.
- `job-identifier` — descrizione dell'operazione, è utilizzata nei messaggi Anacron e, come il file timestamp del processo, può contenere qualsiasi carattere (salvo il carattere barra).
- `command` — comando da eseguire.

Per ogni operazione, Anacron determina se deve essere eseguita entro il periodo specificato nel campo `period` del file di configurazione. Se l'operazione non è stata eseguita entro il periodo indicato, Anacron esegue il comando specificato nel campo `command` dopo aver atteso i minuti specificati nel campo `delay`.

Al termine dell'operazione, Anacron registra la data in un file timestamp nella directory `/var/spool/anacron`. Viene indicata solo la data (non l'ora) e il valore del `job-identifier` viene utilizzato come nome per il file timestamp.

Le variabili d'ambiente come `SHELL` e `PATH` possono essere definite all'inizio di `/etc/anacrontab` come per il file di configurazione di cron.

Il file di configurazione predefinito è simile al seguente:

```
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# These entries are useful for a Red Hat Linux system.
1       5       cron.daily              run-parts /etc/cron.daily
7       10      cron.weekly             run-parts /etc/cron.weekly
30      15      cron.monthly            run-parts /etc/cron.monthly
```

Figura 28-1. Anacrontab di default

Come potrete vedere nella Figura 28-1, anacron per Red Hat Linux è configurato per garantire che le operazioni di cron vengano eseguite con cadenza giornaliera, quotidiana o mensile.

28.2.2. Avvio e interruzione del servizio

Per avviare il servizio anacron, utilizzate il comando `/sbin/service anacron start`, per interromperlo, utilizzate il comando `/sbin/service anacron stop`. È consigliabile eseguire il servizio al momento dell'avvio. Per maggiori informazioni su come avviare anacron in modo automatico, consultate il Capitolo 14.

28.3. At e batch

Mentre cron e anacron consentono di pianificare operazioni ricorrenti, il comando `at` consente di pianificare un'operazione da eseguire una sola volta in un dato momento. Il comando `batch` consente di pianificare un'operazione da eseguire una sola volta quando il carico medio del sistema va al di sotto di 0.8.

Per usare `at` o `batch` il pacchetto RPM `at` deve essere installato e il servizio `atd` deve essere in esecuzione. Per determinare se il pacchetto è installato, usate il comando `rpm -q at`. Per determinare se il servizio è in esecuzione, usate il comando `/sbin/service atd status`.

28.3.1. Configurazione dei processi At

Per pianificare un processo da eseguire una sola volta in un dato momento, digitate il comando `at` *`tempo`*, dove *`tempo`* è il momento di di esecuzione del comando.

L'argomento *`tempo`* può essere uno dei seguenti:

- Formato HH:MM — Per esempio, 04:00 specifica le 4:00 del mattino. Se l'ora indicata è già passata, l'operazione verrà eseguita alla stessa ora del giorno successivo.
- midnight — Indica mezzanotte.
- noon — Indica mezzogiorno.
- teatime — Indica le 4:00 del pomeriggio.
- Formato nome mese-giorno-anno — Per esempio, gennaio 15 2002 specifica il quindicesimo giorno di gennaio dell'anno 2002. L'anno è opzionale.
- Formati MMGGAA (MMDDYY), MM/GG/AA (MM/DD/YY) o MM.GG.AA (MM.DD.YY) — Per esempio, 011502 specifica il quindicesimo giorno di gennaio dell'anno 2002.
- ora + tempo (now + time) — Il tempo è espresso in minuti, ore, giorni o settimane. Per esempio, ora + 5 giorni specifica che il comando deve essere eseguito alla stessa ora tra cinque giorni.

L'ora deve essere specificata per prima, seguita dalla data opzionale. Per maggiori informazioni sul formato, consultate il file di testo `/usr/share/doc/at-`*`versione`*`/timespec`.

Dopo avere digitato il comando `at` con il tempo, compare il prompt `at>`. Digitate il comando di esecuzione, premete [Invio], quindi digitate Ctrl-D. È possibile specificare più comandi premendo dopo ciascuno di essi il tasto [Invio]. Dopo aver digitato tutti i comandi, premete [Invio] per posizionarvi in una riga vuota, quindi digitate Ctrl-D. In alternativa, al prompt è possibile inserire uno script della shell, premendo [Invio] dopo ogni riga dello script, e digitando Ctrl-D su una riga vuota per uscire. Se inserite uno script, la shell usata è la stessa impostata nell'ambiente SHELL dell'utente, la shell di login dell'utente, o `/bin/sh` (l'elemento rilevato per primo).

Se la serie di comandi o script cerca di visualizzare le informazioni, l'output viene inviato via e-mail all'utente.

Utilizzate il comando `atq` per visualizzare i processi non ancora eseguiti. Per maggiori informazioni consultate la Sezione 28.3.3.

L'uso del comando `at` può essere limitato. Consultate la Sezione 28.3.5 per maggiori dettagli.

28.3.2. Configurazione dei processi batch

Per eseguire un'operazione una sola volta quando il carico medio del sistema va al di sotto di 0.8, usate il comando `batch`.

Dopo avere digitato il comando `batch`, il prompt `at>` viene visualizzato. Inserite il comando da eseguire, premete [Invio], quindi digitate Ctrl-D. È possibile specificare più comandi premendo dopo ciascuno di essi il tasto [Invio]. Dopo aver digitato tutti i comandi, premete [Invio] per posizionarvi in una riga vuota, quindi digitate Ctrl-D. In alternativa, al prompt è possibile inserire uno script della shell, premendo [Invio] dopo ogni riga dello script, e digitando Ctrl-D su una riga vuota per uscire. Se inserite uno script, la shell usata è la stessa impostata nell'ambiente SHELL, la shell di login dell'utente, o `/bin/sh` (l'elemento rilevato per primo). Non appena il carico medio va al di sotto di 0.8, la serie di comandi o di script viene eseguita.

Se la serie di comandi o script cerca di visualizzare le informazioni, l'output viene inviato via e-mail all'utente.

Utilizzate il comando `atq` per visualizzare i processi non ancora eseguiti. Per maggiori informazioni consultate la Sezione 28.3.3.

L'uso del comando `at` può essere limitato. Consultate la Sezione 28.3.5 per maggiori dettagli.

28.3.3. Visualizzazione dei processi da eseguire

Per visualizzare i processi `at` e `batch` non ancora eseguiti, utilizzate il comando `atq`. Verrà visualizzato l'elenco di tali processi, ognuno dei quali sarà su una riga. Ogni riga ha il formato "jobnumber, date, hour, job class, e username". Gli utenti possono solo visualizzare i propri processi. Se l'utente root esegue il comando `atq`, saranno visualizzati i processi di tutti gli utenti.

28.3.4. Opzioni da linea di comando aggiuntive

Le opzioni da linea di comando aggiuntive per `at` e `batch` includono:

Opzione	Descrizione
`-f`	Consente di leggere i comandi o lo script della shell da un file invece di specificarli al prompt.
`-m`	Consente di inviare messaggi di posta all'utente al termine del processo.
`-v`	Consente di visualizzare l'ora in cui il processo verrà eseguito.

Tabella 28-1. `at` e `batch` Opzioni da linea di comando

28.3.5. Controllo dell'accesso a at e batch

I file `/etc/at.allow` e `/etc/at.deny` possono essere usati per limitare l'accesso ai comandi `at` e `batch`. Il formato di entrambi i file di controllo dell'accesso è costituito da un nome utente su ciascuna riga. Non possono essere lasciati spazi vuoti. Il demone `at` (`atd`) non deve essere riavviato se i file di controllo dell'accesso vengono modificati. Questi file sono letti ogni volta che un utente cerca di eseguire i comandi `at` o `batch`.

L'utente root può sempre eseguire i comandi `at` e `batch`, indipendentemente dai file di controllo dell'accesso.

Se il file `at.allow` esiste, solo gli utenti qui elencati sono autorizzati a utilizzare `at` o `batch` e il file `at.deny` viene ignorato.

Se `at.allow` non esiste, tutti gli utenti elencati in `at.deny` non sono autorizzati a utilizzare `at` o `batch`.

28.3.6. Avvio e interruzione del servizio

Per avviare il servizio `at`, utilizzate il comando `/sbin/service atd start`. Per interrompere il servizio, utilizzate il comando `/sbin/service atd stop`. Si consiglia di eseguire il servizio all'avvio. Consultate il Capitolo 14 per ulteriori dettagli sull'esecuzione automatica del servizio cron all'avvio.

28.4. Risorse aggiuntive

Per maggiori informazioni sulla configurazione di operazioni automatiche, consultate le risorse elencate qui di seguito.

28.4.1. Documentazione installata

- Pagina man di `cron` — offre una panoramica di cron.
- Pagine man di `crontab` nelle sezioni 1 e 5 — la pagina man della sezione 1 contiene una panoramica del file `crontab`, mentre quella della sezione 5 contiene il formato del file e alcune voci esemplificative.
- `/usr/share/doc/at-`*<versione>*`/timespec` contiene informazioni dettagliate sui tempi che è possibile specificare per i processi cron.
- Pagina man di `anacron` — fornisce una descrizione di anacron e delle relative opzioni della linea di comando.
- Pagina man di `anacrontab` — offre una breve panoramica del file di configurazione di anacron.
- `/usr/share/doc/anacron-`*<version>*`/README` — describes Anacron and why it is useful.
- Pagina man di `at` — fornisce una descrizione di `at` e `batch` e delle relative opzioni della linea di comando.

Capitolo 29.

File di log

I *file di log* sono file che contengono messaggi relativi al sistema, compreso il kernel, i servizi e le applicazioni in funzione. Vi sono diversi tipi di file di log per le diverse informazioni. Per esempio, esiste un file di log predefinito per il sistema, un file di log solo per messaggi relativi alla sicurezza e un file di log per i task cron.

I file di log possono rivelarsi molto utili se state cercando di risolvere un problema concernete il sistema, per esempio se state tentando di caricare un driver del kernel o se state cercando un log non autorizzato per il sistema. Questo capitolo spiega dove reperire i file di log, come visualizzarli e che cosa cercare al loro interno.

Alcuni file di log sono controllati da un demone chiamato `syslogd`. Nel file di configurazione `/etc/syslog.conf` è possibile trovare un elenco dei messaggi di log gestiti da `syslogd`.

29.1. Individuazione dei file di log

La maggior parte dei file di log si trova nella directory `/var/log`. Alcune applicazioni, quali `httpd` e `samba` hanno una directory all'interno di `/var/log` riservata ai loro file di log.

Vi saranno molteplici file nella directory dei file di log seguiti da numeri. Tali file sono creati quando i file di log subiscono una rotazione; tale operazione viene eseguita per evitare che le loro dimensioni aumentino eccessivamente. Il pacchetto `logrotate` contiene un task cron che ruota automaticamente i file di log in base al file di configurazione e ai file di configurazione contenuti nella directory `/etc/logrotate.d`. Le impostazioni di default prevedono una rotazione ogni settimana e i file di log precedenti vengono conservati per quattro settimane.

29.2. Visualizzazione dei file di log

Quasi tutti i file di log sono in formato testo e potete visualizzarli con un qualsiasi editor di testo (per esempio **Vi** o **Emacs**). Alcuni file di log possono essere letti da tutti gli utenti registrati sul sistema, ma la maggior parte di essi sono riservati ai soli utenti con privilegi di root.

Per visualizzare i file di log tramite un'applicazione interattiva e in tempo reale, utilizzate il **Log Viewer**. Per lanciare questa applicazione, selezionate il **Pulsante menu principale** (sul pannello) => **Strumenti del sistema** => **Registrazione del sistema** oppure digitate il comando `redhat-logviewer` a un prompt della shell.

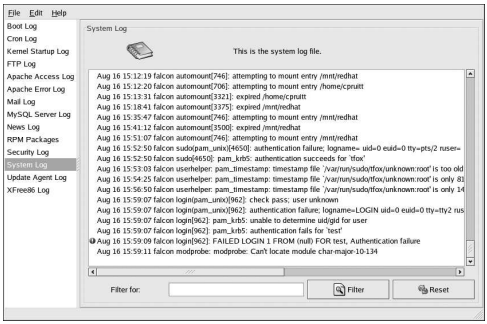

Figura 29-1. Log Viewer

L'applicazione visualizza soltanto i file di log esistenti, pertanto il vostro elenco potrebbe differire da quello mostranto nella Figura 29-1. Per ottenere l'elenco completo dei file di log visualizzabili, consultate il file di configurazione, `/etc/sysconfig/redhat-logviewer`.

Per default, il file di log attualmente visualizzabile viene ricaricato ogni 30 secondi. Per modificare la frequenza di ricaricamento, selezionate **Modifica => Preferenze** dal menu a tendina. Comparirà la finestra mostrata nella Figura 29-2. Nella linguetta **File di log**, fate clic sulle frecce che vanno in alto e in basso poste accanto alla frequenza di ricaricamento (refresh rate) per modificarla. Fate clic su **Chiudi** per tornare alla finestra principale. Le frequenza di ricaricamento viene cambiata all'istante. Per ricaricare manualmente il file attualmente visualizzabile, selezionate **File => Refresh Now** o premete la combinazione di tasti [Ctrl]-[R].

Per filtrare il contenuto del file di log per le parole-chiave, digitate la parola o le parole che state cercando per il campo di testo **Filter for** e fate clic su **Filter**. Infine, fate clic su **Resetta** per reimpostare il contenuto.

Potete anche cambiare il posto in cui l'applicazione ricerca i file di log dalla linguetta **File di log**. Selezionate il file di log desiderato dall'elenco e fate clic sul pulsante **Cambia posizione**. Digitate la nuova posizione del file di log oppure fate clic sul pulsante **Browse** per individuare la posizione del file mediante una finestra di dialogo per la selezione. Fate clic su **OK** per tornare alle preferenze e poi fate clic su **Chiudi** per tornare alla finestra principale.

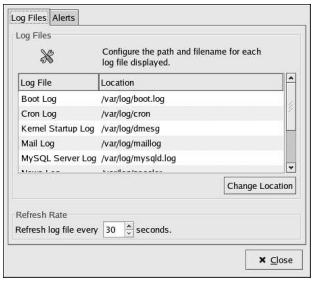

Figura 29-2. Posizione dei file di log

29.3. Esaminare i file di log

Il **Log Viewer** può essere impostato in modo che visualizzi una icona di avviso accanto alle righe

che contengono parole-chiave di avviso. Per aggiungere parole di avviso, selezionate **Modifica => Preferenze** dal menu a tendina e fate clic sulla linguetta **Alerts**. Fate clic sul pulsante **Aggiungi** per aggiungere la parola. Per cancellare una parola, invece, selezionatela dall'elenco e fate clic su **Cancella**.

Figura 29-3. Avvisi

Capitolo 30.

Aggiornamento del kernel

Il kernel fornito con Red Hat Linux è stato creato su misura dal team di esperti di Red Hat in modo da garantire la sua integrità e compatibilità con l'hardware supportato. Prima che venga lanciato da Red Hat, il kernel deve superare un insieme di test di qualità.

I kernel ufficiali di Red Hat Linux sono disponibili nel formato RPM per facilitare aggiornamenti e verifiche. Per esempio, il pacchetto RPM del `kernel` RPM crea l'immagine `initrd`. Adesso non è più necessario usare il comando `mkinitrd` dopo avere installato un kernel diverso se il kernel è stato installato dal pacchetto RPM di Red Hat. Se è installato GRUB oppure LILO, viene inoltre modificato il file di configurazione del boot loader per includere il nuovo kernel.

Il capitolo spiega la procedura da seguire per aggiornare il kernel unicamente su sistemi x86.

Avvertenza

I kernel creati dall'utente non sono supportati dal Team di assistenza all'installazione di Red Hat Linux. Per maggiori informazioni sulla creazione di un kernel personalizzato usando il codice sorgente, consultate il Appendice A.

30.1. Il kernel 2.4

Red Hat Linux viene ora fornito con il kernel 2.4, le cui caratteristiche sono di seguito elencate:

- La directory in cui si trovano i sorgenti del kernel è `/usr/src/linux-2.4` mentre prima era `/usr/src/linux`.
- Supporto per il filesystem ext3.
- Supporto multi-processore (SMP).
- Supporto USB.
- Supporto per lo standard IEEE 1394, conosciuto anche come FireWire™.

30.2. Prima dell'aggiornamento

Prima di migliorare il kernel, prendere delle precauzioni. Il primo step é di assicurarsi dell'esistenza di un dischetto di avvio per il sistema nel caso in cui si verifichi un problema. Se il boot loader non é configurato in modo corretto per avviare il nuovo kernel, il sistema non potrá essere avviato nel Red Hat Linux senza un dischetto di avvio funzionante.

Per creare un dischetto di avvio, dovete determinare quale versione del kernel è attualmente in esecuzione. Per farlo, digitate il seguente comando:

```
/sbin/mkbootdisk `uname -r`
```

Suggerimento

Per conoscere le altre opzioni disponibili, consultate la pagina man di `mkbootdisk`.

Riavviate la macchina con il dischetto di avvio e verificate che funzioni prima di continuare.

Vi auguriamo di non dover più utilizzare il dischetto, ma conservatelo comunque in un posto sicuro in caso di problemi.

Per determinare quali pacchetti del kernel avete installato, digitate il seguente commando al prompt della shell:

```
rpm -qa | grep kernel
```

L'output del comando contiene alcuni o tutti i seguenti pacchetti, in funzione del tipo di installazione eseguita (i numeri di versione e i pacchetti potrebbero essere diversi):

```
kernel-2.4.20-2.47.1
kernel-debug-2.4.20-2.47.1
kernel-source-2.4.20-2.47.1
kernel-doc-2.4.20-2.47.1
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.20-2.47.1
```

Dall'output è possibile determinare quali pacchetti devono essere scaricati per l'aggiornamento del kernel. L'unico pacchetto indispensabile è il pacchetto `kernel`.

Se disponete di più processori, avrete bisogno del pacchetto `kernel-smp` che fornisce il supporto relativo. È consigliabile installare anche il pacchetto `kernel` nel caso in cui il kernel multi-processore non funzioni correttamente.

Se disponete di un computer con oltre quattro gigabyte di memoria, vi serve il pacchetto `kernel-bigmem`. Anche in questo caso, è consigliabile installare il pacchetto `kernel` per il debug. `kernel-bigmem` è fornito solo per l'architettura i686.

Se eseguite l'aggiornamento del kernel su un computer portatile o usate un dispositivo PCMCIA, dovete scaricare anche il pacchetto `kernel-pcmcia-cs`.

Il pacchetto `kernel-source` è necessario unicamente se decidete di ricompilare il kernel o di eseguire uno sviluppo del kernel.

Il pacchetto `kernel-doc` contiene una documentazione sullo sviluppo del kernel e non è indispensabile. É raccomandabile il suo uso se il sistema é usato per lo sviluppo del kernel.

Il pacchetto `kernel-util` contiene alcune utility che possono essere utilizzate per controllare il kernel o l'hardware del sistema. Anch'esso non è indispensabile.

Red Hat fornisce i kernel ottimizzati per diverse versioni x86. Potete scegliere `athlon` per sistemi AMD Athlon™ e AMD Duron™, `i686` per Intel® Pentium® II, Intel® Pentium® III, Intel® Pentium® 4 e `i586` per Intel® Pentium® e AMD K6™. Se non conoscete la versione del vostro sistema x86, usate il kernel fornito per la versione `i386`, compatibile con tutti i sistemi x86.

La versione x86 del sistema RPM è inclusa nel nome del file. Per esempio, `kernel-2.4.20-2.47.1.athlon.rpm` è ottimizzato per sistemi AMD Athlon™ e AMD Duron™ mentre `kernel-2.4.20-2.47.1.i686.rpm` è ottimizzato per sistemi Intel® Pentium® II, Intel® Pentium® III e Intel® Pentium® 4. Una volta stabilito quali pacchetti utilizzare per aggiornare il kernel, selezionate l'architettura appropriata per i pacchetti `kernel`, `kernel-smp` e `kernel-bigmem`. Usate le versioni `i386` degli altri pacchetti.

30.3. Download del kernel aggiornato

Esistono diversi modi per stabilire se esiste un kernel aggiornato per il proprio sistema.

- Collegatevi al sito http://www.redhat.com/apps/support/errata/, scegliete la versione di Red Hat Linux che state usando e visualizzate l'aggiornamento corrispondente. Solitamente gli aggiornamenti del kernel sono contenuti nella sezione **Security Advisories**. Per visualizzare il report degli aggiornamenti, fate clic sull'aggiornamento desiderato. Il report contiene un elenco dei pacchetti RPM richiesti e un link per scaricarli dal sito FTP di Red Hat. Potete scaricarli anche da un sito mirror FTP Red Hat. Per un elenco dei siti mirror, visitate il sito http://www.redhat.com/download/mirror.html.
- Potete usare Red Hat Network per scaricare i pacchetti RPM del kernel e installare i pacchetti. Red Hat Network può, scaricare il kernel più recente, aggiornarlo sul vostro sistema, creare, se necessario, un RAM disk iniziale e configurare il boot loader perché avvii il nuovo kernel. Vi basterà poi avviare il sistema sul nuovo kernel. Per maggiori informazioni consultate la *Red Hat Network User Reference Guide* disponibile all'indirizzo http://www.redhat.com/docs/manuals/RHNetwork/.

Se i pacchetti RPM sono stati installati dalla pagina errata di Red Hat Linux o Red Hat Network é stato usato solo per scaricare i pacchetti, controllare la Sezione 30.4. Se Red Hat Network é stato usato per scaricare e installare il kernel aggiornato, seguire le istruzioni in la Sezione 30.5 e la Sezione 30.6, ma non cambiate il kernel in modo tale da avviarsi per default, perché Red Hat Network automaticamente cambia il kernel di default nella ultimissima versione.

30.4. Esecuzione dell'aggiornamento

Adesso che avete i pacchetti RPM del kernel, potete procedere al miglioramento del kernel esistente. Collegatevi come root da una shell, entrate nella directory contenente i pacchetti RPM del kernel ed eseguite le operazioni seguenti.

Importante

È consigliabile conservare il vecchio kernel nel caso si verifichino problemi con quello nuovo.

Utilizzate l'argomento `-i` con il comando `rpm` se desiderate conservare il vecchio kernel. Se utilizzate l'opzione `-U` per aggiornare il pacchetto `kernel`, verrà sovrascritta la versione del kernel correntemente installato (la versione del kernel e la versione x86 potrebbero variare):

```
rpm -ivh kernel-2.4.20-2.47.1.i386.rpm
```

Se disponete di un sistema multi-processore, installate anche i pacchetti `kernel-smp` (la versione x86 e la versione del kernel potrebbero variare):

```
rpm -ivh kernel-smp-2.4.20-2.47.1.i386.rpm
```

Se il sistema utilizza `i686` e dispone di oltre 4 gigabyte di RAM, installate anche il pacchetto `kernel-bigmem` appositamente creato per l'architettura `i686` (la versione del kernel potrebbe variare):

```
rpm -ivh kernel-bigmem-2.4.20-2.47.1.i686.rpm
```

Se intendete migliorare i pacchetti `kernel-source`, `kernel-docs` o `kernel-utils`, con molta probabilità non dovrete conservare le versioni precedenti. Per l'aggiornamento di questi pacchetti (le versioni potrebbero variare), usate i comandi di seguito riportati:

```
rpm -Uvh kernel-source-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-docs-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-utils-2.4.20-2.47.1.i386.rpm
```

Se usate un dispositivo PCMCIA (per esempio, un computer portatile), dovete installare anche il pacchetto `kernel-pcmcia-cs` e conservarne la versione precedente. Se usate l'opzione `-i`, si verificherà un conflitto perché il vecchio kernel necessita di questo pacchetto per avviarsi con il supporto PCMCIA. Per risolvere il conflitto, usate `--force` (la versione potrebbe variare):

```
rpm -ivh --force kernel-pcmcia-cs-3.1.24-2.i386.rpm
```

La fase successiva é quella di controllare che l'immagine iniziale del RAM disk é stato creato. Consultate la Sezione 30.5 per maggiori informazioni.

30.5. Verifica dell'immagine iniziale del RAM disk

Se usate il filesystem ext3 oppure un controller SCSI, vi serve un RAM disk iniziale, che permette a un kernel modulare di accedere ai moduli di cui ha bisogno per avviarsi prima di accedere al dispositivo contenente i moduli.

Il RAM disk iniziale viene creato usando il comando `mkinitrd`. Tuttavia, questa fase viene effettuata automaticamente dal kernel e i suoi pacchetti associati sono installati o migliorati dai pacchetti RPM distribuiti da Red Hat, Inc.; in modo tale da non aver bisogno di effettuare questa operazione manualmente. Per assicurarsi di quanto detto, usare il comando `ls -l /boot` e controllare se il file `initrd-2.4.20-2.47.1.img` é stato creato (la versione dovrebbe corrispondere alla versione del kernel appena installato).

Adesso che avete installato il nuovo kernel, dovete configurare il boot loader affinché avvii il nuovo kernel. Per maggiori dettagli, consultate la la Sezione 30.6.

30.6. Configurazione del boot loader

Il pacchetto RPM del `kernel` configura il boot loader GRUB o LILO affinché avvii il nuovo kernel installato, ma non lo configura perchè avvii il nuovo kernel di default.

È sempre utile confermare che il boot loader è stato configurato correttamente. L'operazione è cruciale. Se la eseguite in modo sbagliato, non potrete avviare il sistema. Se dovesse accadere, avviate il sistema usando il dischetto di avvio e riprovate a configurare il boot loader.

30.6.1. GRUB

Se avete scelto il boot loader GRUB, confermate che il file `/boot/grub/grub.conf` contenga una sezione `title` con la stessa versione del `kernel` installato (disporrete di una sezione anche se avete installato `kernel-smp` e/o `kernel-bigmem`):

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=3
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-2.47.1)
        root (hd0,0)
```

```
        kernel /vmlinuz-2.4.20-2.47.1 ro root=LABEL=/
        initrd /initrd-2.4.20-2.47.1.img
title Red Hat Linux (2.4.20-2.30)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.30 ro root=LABEL=/
        initrd /initrd-2.4.20-2.30.img
```

Se avete creato una partizione `/boot` separata, i percorsi del kernel e dell'immagine initrd si riferiscono alla partizione `/boot`.

Per configurare GRUB perché avvii il nuovo kernel per default, modificate il valore della variabile `default` utilizzando il numero per la sezione del titolo che contiene il nuovo kernel. Il conteggio inizia da 0. Se, per esempio, il nuovo kernel è rappresentato dalla seconda sezione del titolo, impostate `default` a **`1`**.

Potete iniziare a eseguire una verifica del kernel riavviando il computer e osservando i messaggi che compaiono a video. In questo modo potete controllare che l'hardware venga rilevato correttamente.

30.6.2. LILO

Se avete scelto il boot loader LILO, confermate che il file `/etc/lilo.conf` contenga una sezione `image` con la stessa versione del pacchetto `kernel` installato (se il pacchetto `kernel-smp` o `kernel-bigmem` é stato installato, esisterá una sua sezione):

```
prompt
timeout=50
default=2.4.20-2.30
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear

image=/boot/vmlinuz-2.4.20-2.47.1
        label=2.4.20-2.47.1
        initrd=/boot/initrd-2.4.20-2.47.1.img
        read-only
        append="root=LABEL=/"

image=/boot/vmlinuz-2.4.20-2.30
        label=2.4.20-2.30
        initrd=/boot/initrd-2.4.20-2.30.img
        read-only
        append="root=LABEL=/"
```

Notare che il default non é impostato per il nuovo kernel. Per configurare LILO perchè avvii il nuovo kernel per default, impostate la variabile `default` al valore di `label` nella sezione `image` per il nuovo kernel. È necessario eseguire il comando `/sbin/lilo` come root per abilitare le modifiche. Eseguita quest'operazione, verrà visualizzato un output simile al seguente:

```
Added 2.4.20-2.47.1 *
Added linux
```

Il carattere `*` dopo `2.4.20-2.47.1` significa che il kernel in quella sezione é quello di default che LILO avvierá.

Potete iniziare a eseguire una verifica del kernel riavviando il computer e osservando i messaggi che compaiono a video. In questo modo potete controllare che l'hardware venga rilevato correttamente.

Capitolo 31.

Moduli del kernel

Il kernel di Linux ha un design modulare. All'avvio, viene caricata in memoria solo una minima parte del kernel. Dunque, quando un utente desidera utilizzare una periferica il cui supporto non è presente nel kernel attualmente attivo, viene caricato dinamicamente un *module del kernel*, talvolta riferito come *driver*.

Durante l'installazione di Red Hat Linux, l'hardware del vostro sistema viene analizzato. Sulla base del rilevamento e delle informazioni da voi fornite, il programma di installazione decide quali moduli caricare all'avvio del sistema. Il programma di installazione configura il meccanismo di caricamento dinamico in modo che funzioni in maniera trasparente.

Se dopo l'installazione aggiungete nuovo hardware che richiede un particolare modulo del kernel, dovete configurare il sistema in modo tale da caricare il modulo del kernel corretto per il nuovo hardware. **Kudzu** viene eseguita all'avvio del sistema e di norma è in grado di rilevare il nuovo hardware. Potete anche aggiungere un nuovo driver modificando il file di configurazione del modulo, `/etc/modules.conf`.

Nota bene

I moduli della scheda video usati per visualizzare l'interfaccia del Sistema X Window, fanno parte del pacchetto `XFree86`, non del kernel; di conseguenza, questo capitolo non viene applicato ai suddetti moduli.

Per esempio, se il vostro sistema ha una scheda di rete PCI SMC EtherPower 10 al momento dell'installazione, il file di configurazione del modulo conterrà la seguente linea:

```
alias eth0 tulip
```

Dopo l'istallazione, se installate un'altra scheda di rete identica nel vostro sistema, aggiungete la seguente linea nel file `/etc/modules.conf`:

```
alias eth1 tulip
```

Per ottenere un elenco alfabetico dei moduli del kernel e dei dispositivi hardware che supportano, consultate la *Red Hat Linux Reference Guide*.

31.1. Utility dei moduli del kernel

Potete anche utilizzare un gruppo di comandi per gestire i moduli del kernel se il pacchetto `modutils` é installato. Questi comandi sono utili se volete provare diversi moduli o se desiderate verificare che un determinato modulo sia stato caricato correttamente.

Il comando `/sbin/lsmod` visualizza un elenco dei moduli attualmente caricati. Per esempio:

```
Module                  Size  Used by    Not tainted
iptable_filter          2412   0 (autoclean) (unused)
ip_tables              15864   1 [iptable_filter]
nfs                    84632   1 (autoclean)
lockd                  59536   1 (autoclean) [nfs]
sunrpc                 87452   1 (autoclean) [nfs lockd]
```

```
soundcore               7044   0 (autoclean)
ide-cd                 35836   0 (autoclean)
cdrom                  34144   0 (autoclean) [ide-cd]
parport_pc             19204   1 (autoclean)
lp                      9188   0 (autoclean)
parport                39072   1 (autoclean) [parport_pc lp]
autofs                 13692   0 (autoclean) (unused)
e100                   62148   1
microcode               5184   0 (autoclean)
keybdev                 2976   0 (unused)
mousedev                5656   1
hid                    22308   0 (unused)
input                   6208   0 [keybdev mousedev hid]
usb-uhci               27468   0 (unused)
usbcore                82752   1 [hid usb-uhci]
ext3                   91464   2
jbd                    56336   2 [ext3]
```

Per ogni riga, la prima colonna é il nome del modulo, la seconda colonna é la misura del modulo, e la terza colonna rappresenta il conteggio dell'utilizzo.

L'informazione dopo il conteggio dell'utilizzo varia di poco a seconda del modulo. Se `(unused)` é elencato sulla riga del modulo, lo stesso modulo correntemente non é stato usato. Se `(autoclean)` é sulla riga per il modulo, lo stesso puó essere cancellato automaticamente dal comando `rmmod -a`. Quando questo comando viene eseguito, qualsiasi modello che é stato etichettato "tagged" con autoclean, e che non é stato usato dall'ultima azione di autoclean, viene scaricato. Red Hat Linux non effettua questa azione per default.

Se il nome di un modulo é elencato alla fine della riga tra parentesi, tale modulo dipende dal modulo elencato nella prima colonna della riga. Per esempio, nella riga

```
usbcore                82752   1 [hid usb-uhci]
```

i moduli del kernel hid e usb-uhci dipendono dal modulo usbcore.

L'output `/sbin/lsmod` é lo stesso output visualizzando `/proc/modules`.

Per caricare un modulo del kernel, potete utilizzare il comando `/sbin/modprobe` seguito dal nome del modulo. Per default, `modprobe` cerca di caricare il modulo dalle sottodirectory `/lib/modules/<kernel-version>/kernel/drivers`. Esiste una sottodirectory per ciascun tipo di modulo (per esempio, la sottodirectory `net` per i driver dell'interfaccia di rete. Alcuni moduli del kernel hanno delle dipendenze — per poterli caricare, occorre averne prima caricati degli altri. Per ovviare a questo problema, potete caricare le dipendenze del modulo desiderato e poi il modulo stesso, oppure potete utilizzare il comando `/sbin/modprobe` seguito dal nome del modulo per caricarlo insieme alle sue dipendenze.

Per esempio, il comando

```
/sbin/modprobe hid
```

carica ogni dipendenza del modulo e anche il modulo `hid`.

Per far comparire sulla schermata tutti i comandi come `/sbin/modprobe`, usare l'opzione `-v`. Per esempio:

```
/sbin/modprobe -v hid
```

Viene visualizzato un output simile al seguente:

```
/sbin/insmod /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
```

```
Using /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'
```

Esiste anche il comando `/sbin/insmod` per caricare i moduli del kernel; tuttavia, non risolve le dipendenze. É consigliato usare il comando `/sbin/modprobe`.

Per rimuovere dalla memoria un modulo del kernel, usate il comando `/sbin/rmmod` seguito dal nome del modulo. L'utility `rmmod` rimuoverà soltanto i moduli non utilizzati e non necessari per altri moduli in uso.

Per esempio, il comando

```
/sbin/rmmod hid
```

rimuove il modulo del kernel `hid`.

Un'altra importante utility per i moduli del kernel è `modinfo`. Potete usare il comando `/sbin/modinfo` per visualizzare informazioni relative a un modulo del kernel. La sintassi generale è:

```
/sbin/modinfo [options] <module>
```

Tra le opzioni è incluso il comando `-d`, che visualizza una breve descrizione del modulo, e il comando `-p` che fornisce un elenco dei parametri supportati dal modulo. Per un elenco completo delle opzioni, consultate la pagina man di `modinfo` (`man modinfo`).

31.2. Risorse aggiuntive

Per maggiori informazioni sui moduli del kernel e le loro utility, consultate le risorse seguenti.

31.2.1. Documentazione installata

- pagina man di `lsmod` — descrizione e spiegazione dell'output.
- pagina man di `insmod` — descrizione ed elenco di opzioni da linea di comando.
- pagina man di `modprobe` — descrizione ed elenco di opzioni da linea di comando.
- pagina man di `rmmod` — descrizione ed elenco di opzioni da linea di comando.
- pagina man di `modinfo` — descrizione ed elenco di opzioni da linea di comando.
- `/usr/src/linux-2.4/Documentation/modules.txt` — spiegazione su come compilare e utilizzare moduli del kernel.

31.2.2. Useful Websites

- http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html — *Linux Loadable Kernel Module HOWTO* da Linux Documentation Project.

V. Gestione del pacchetto

Il software su di un sistema Red Hat Linux é diviso in pacchetti RPM i quali possono essere installati, migliorati o rimossi. Questa sezione descrive come gestire i pacchetti RPM su di un sistema Red Hat Linux usando strumenti grafici e della linea di comando.

Sommario

Capitolo 32.

Gestione dei pacchetti con RPM

L'applicazione RPM (RPM Package Manager) è un sistema di packaging aperto, disponibile per tutti, che gira su Red Hat Linux e su altri sistemi Linux e UNIX. Red Hat, Inc. incoraggia altri distributori a usare RPM per i propri prodotti. RPM è distribuito secondo i termini della General Public Licence.

Per l'utente finale, RPM crea aggiornamenti di sistema semplici. L'installazione, la disinstallazione e l'aggiornamento dei pacchetti RPM si possono effettuare con comandi brevi. RPM contiene un database dei pacchetti installati e dei loro file, in modo che l'utente possa effettuare ricerche e verifiche sul sistema. Se preferite un'interfaccia grafica, potete usare **Strumento di gestione dei pacchetti** per eseguire molti comandi RPM. Per ulteriori informazioni, consultate il Capitolo 33.

Durante gli aggiornamenti, RPM gestisce i file di configurazione con molta cautela, in modo che l'utente non perda mai le sue personalizzazioni — cosa impossibile con i file `.tar.gz` normali.

RPM permette agli sviluppatori di prendere il codice sorgente e di inglobarlo in pacchetti sorgenti binari per l'utente finale. Il processo è abbastanza semplice ed è effettuato a partire da un file singolo e da aggiornamenti opzionali creati dall'utente. Questa chiara delineazione dei sorgenti di origine, degli aggiornamenti e delle istruzioni semplifica la conservazione del pacchetto man mano che vengono create nuove versioni del software.

Nota Bene

Poiché RPM apporta delle modifiche al sistema, dovete essere collegati come root per installare, rimuovere o aggiornare un pacchetto RPM.

32.1. Concetti di base relativi a RPM

Per comprendere il funzionamento di RPM, può essere utile capirne i concetti di base:

Aggiornabilità

Usando RPM potete aggiornare singoli componenti del sistema senza reinstallarli completamente. Quando installate una nuova versione di un sistema operativo basato su RPM (come Red Hat Linux), non dovete reinstallare tutto il sistema (come avete fatto con i sistemi operativi basati su altri sistemi di pacchetti). RPM permette di aggiornare il sistema in modo intelligente e completamente automatico. I file di configurazione contenuti nei pacchetti sono protetti dagli aggiornamenti perché le personalizzazioni dell'utente non vengano perse. L'aggiornamento di un pacchetto non necessita di particolari file di aggiornamento poiché lo stesso file RPM viene utilizzato per l'installazione e l'aggiornamento del pacchetto.

Opzioni di interrogazione

RPM fornisce potenti opzioni di interrogazione del sistema. Nel vostro database potete effettuare ricerche di pacchetti o di semplici file, nonché sapere a quale pacchetto appartiene un certo file e risalire alle origini del pacchetto. I file contenuti in un pacchetto RPM sono in un archivio compresso, con un header binario personalizzato che racchiude informazioni utili sul pacchetto e sul suo contenuto. Questo vi permette di interrogare singoli pacchetti in modo semplice e veloce.

Verifica del sistema

Un'altra funzione molto utile è la capacità di verificare pacchetti. Se avete cancellato un file importante per alcuni pacchetti, verificate il pacchetto stesso. Durante la verifica vi viene indicata qualsiasi anomalia. A questo punto, potete reinstallare il pacchetto, se necessario. Tutti i file di configurazione che avete modificato vengono conservati durante la reinstallazione.

Sorgenti inalterate

Uno degli obiettivi principali era quello di permettere l'utilizzo delle sorgenti inalterate del software, come distribuite dall'autore stesso. In RPM sono contenuti i sorgenti originali e tutte le modifiche che sono state apportate, nonché tutte le istruzioni per la ricompilazione. Questo è un vantaggio importante per vari motivi. Per esempio, se esce una nuova versione di un programma, non bisogna partire da zero per ricompilarlo. Potete guardare il patch per vedere cosa *potreste* dover fare. Tutti i parametri di default e tutte le modifiche apportate al software sono facilmente identificabili con questa tecnica.

La conservazione delle sorgenti originali inalterate può sembrare importante solo per gli sviluppatori, ma lo è anche per la qualità del software finale. Ringraziamo l'équipe di BOGUS per avere creato il concetto delle fonti di origine.

32.2. Utilizzo di RPM

RPM ha cinque modalità di funzionamento: installazione, disinstallazione, aggiornamento, interrogazione e verifica. Questa sezione contiene una panoramica di ogni modalità. Per maggiori dettagli e opzioni, digitate il comando `rpm --help` o consultate la Sezione 32.5.

32.2.1. Ricerca dei pacchetti RPM

Prima di usare un RPM, dovete sapere dove cercarlo. Su Internet troverete molti RPM diversi, ma se state cercando i pacchetti RPM di Red Hat, consultate quanto segue:

- I CD-ROM Red Hat Linux ufficiali
- La pagina degli Errata disponibile all'indirizzo http://www.redhat.com/apps/support/errata/
- Un sito mirror FTP di Red Hat disponibile all'indirizzo http://www.redhat.com/download/mirror.html
- Red Hat Network — Consultate il Capitolo 34 per ulteriori dettagli su Red Hat Network

32.2.2. Installazione

Solitamente i nomi dei file dei pacchetti RPM sono simili a `foo-1.0-1.i386.rpm`. Il nome del file include il nome del pacchetto (`foo`), la versione (`1.0`), la release (`1`) e l'architettura (`i386`). Per installare un pacchetto basta digitare, al prompt della shell, il comando seguente:

```
rpm -Uvh foo-1.0-1.i386.rpm
```

Se l'installazione ha successo, potrete visualizzare quanto riportato di seguito:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [100%]
```

Come potete vedere, RPM stampa il nome del pacchetto e una serie di riferimenti che servono per seguire l'installazione del pacchetto.

A partire dalla versione 4.1 di RPM, la firma di un pacchetto viene verificata durante l'installazione o l'aggiornamento di un pacchetto. Se la verifica della firma non riesce, verrà visualizzato un messaggio di errore come il seguente:

```
error: V3 DSA signature: BAD, key ID 0352860f
```

Se si tratta di una nuova firma, costituita solo dall'intestazione, verrà visualizzato un messaggio di errore simile al seguente:

```
error: Header V3 DSA signature: BAD, key ID 0352860f
```

Se non disponete della chiave appropriata installata per la verifica della firma, il messaggio conterrà `NOKEY` come:

```
warning: V3 DSA signature: NOKEY, key ID 0352860f
```

Per ulteriori informazioni sulla verifica di una firma del pacchetto, consultate la Sezione 32.3.

Nota Bene

Se state installato un pacchetto del kernel, dovreste utilizzare `rpm -ivh`. Per ulteriori informazioni consultate il Capitolo 30.

L'installazione dei pacchetti è un'operazione semplice, ma vi può capitare di trovare degli errori.

32.2.2.1. Pacchetti già installati

Se sul sistema è già installata la stessa versione di pacchetto, compare il messaggio seguente:

```
Preparing...                ########################################### [100%]
package foo-1.0-1 is already installed
```

Se volete installare ugualmente il pacchetto, e la stessa versione è già presente sul sistema, usate l'opzione `--replacepkgs` che indica a RPM di ignorare l'errore:

```
rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
```

L'opzione è utile se sono stati cancellati dei file RPM oppure se volete installare i file di configurazione originali di RPM.

32.2.2.2. File in conflitto

Se provate a installare un pacchetto contenente un file che è già stato installato da un altro pacchetto o da una versione precedente dello stesso pacchetto, compare a video il messaggio seguente:

```
Preparing...                ########################################### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package bar-2.0.20
```

Perché RPM ignori questo errore, usate l'opzione `--replacefiles`:

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

32.2.2.3. Dipendenze non risolte

I pacchetti RPM possono "dipendere" da altri pacchetti, il che significa che la loro installazione è subordinata alla presenza di altri pacchetti. Se provate a installare un pacchetto che ha delle dipendenze non risolte, compare a video il messaggio seguente:

```
Preparing...                ########################################### [100%]
error: Failed dependencies:
        bar.so.2 is needed by foo-1.0-1
    Suggested resolutions:
        bar-2.0.20-3.i386.rpm
```

Se state installando un Red Hat ufficiale, suggerirà in genere che i pacchetti devono risolvere la dipendenza. Questi pacchetti sono disponibili nei CD-ROM di Red Hat Linux o nel sito FTP o mirror di Red Hat e potete aggiungerli al comando:

```
rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
```

Se l'installazione di entrambi i pacchetti riesce, potrete visualizzare quanto segue:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [ 50%]
   2:bar                    ########################################### [100%]
```

Se non viene suggerito un pacchetto per risolvere la dipendenza, potete tentare di utilizzare l'opzione `--redhatprovides` per determinare quale pacchetto contiene il file richiesto. È necessario che il pacchetto `rpmdb-redhat` sia installato per utilizzare queste opzioni.

```
rpm -q --redhatprovides bar.so.2
```

Se il pacchetto che contiene `bar.so.2` si trova nel database installato dal pacchetto `rpmdb-redhat`, verrà visualizzato il nome del pacchetto:

```
bar-2.0.20-3.i386.rpm
```

Se volete procedere all'installazione senza risolvere il problema (scelta sconsigliabile visto che probabilmente il pacchetto non funzionerà correttamente), usate l'opzione `--nodeps`.

32.2.3. Rimozione dell'installazione

L'operazione di rimozione è semplice quanto quella di installazione. Al prompt della shell digitate il comando seguente:

```
rpm -e foo
```

Nota Bene

È stato usato il *nome* di pacchetto `foo`, non quello del *file* originale `foo-1.0-1.i386.rpm`. Per disinstallare un pacchetto, sostituite `foo` con il nome del pacchetto di origine.

Potete incontrare un errore di dipendenza durante la rimozione di un pacchetto se un altro pacchetto installato dipende da quello che state cercando di rimuovere. Per esempio:

```
Preparing...                ########################################### [100%]
error: removing these packages would break dependencies:
        foo is needed by  bar-2.0.20-3.i386.rpm
```

Perché RPM ignori questo errore e disinstalli il pacchetto (anche questa operazione è sconsigliabile poiché il pacchetto dipendente non potrà funzionare correttamente), usate l'opzione `--nodeps`.

32.2.4. Aggiornamento

L'operazione di aggiornamento è simile a quella di installazione. Nella shell digitate quanto segue:

```
rpm -Uvh foo-2.0-1.i386.rpm
```

Ciò che non vedete sopra è che RPM ha automaticamente disinstallato tutte le versioni precedenti del pacchetto `foo`. È consigliabile usare sempre il comando `-U` per installare i pacchetti, poiché funziona anche quando non ci sono versioni precedenti del pacchetto installato.

Dato che RPM esegue un aggiornamento intelligente dei pacchetti con i file di configurazione, può comparire a video un messaggio simile a:

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

Il messaggio indica che le modifiche apportate al file di configurazione possono non essere "forward compatible" con il nuovo file di configurazione del pacchetto, perciò RPM ha salvato il vostro file originale e ne ha installato uno nuovo. Dovete cercare le differenza fra i due file di configurazione e risolverle appena possibile in modo che il sistema possa continuare a funzionare correttamente.

L'aggiornamento è una combinazione dell'installazione e della disinstallazione perciò, durante un aggiornamento di RPM, potete trovare errori di installazione e disinstallazione più un altro errore. Se RPM crede che state cercando di aggiornare un pacchetto con una versione *precedente*, compare a video il messaggio seguente:

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

Perché RPM si aggiorni ugualmente, usate l'opzione `--oldpackage`:

```
rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
```

32.2.5. Refresh

L'operazione di refresh è simile all'operazione di aggiornamento. Al prompt della shell digitate il comando seguente:

```
rpm -Fvh foo-1.2-1.i386.rpm
```

L'opzione di refresh di RPM controlla le versioni dei pacchetti specificati nella linea di comando e quelli già installati sul sistema. Quando una versione di un pacchetto già installato viene elaborata dall'opzione di refresh, il pacchetto viene aggiornato alla nuova versione. Tuttavia, l'opzione di refresh di RPM non installa un pacchetto se sul sistema non è presente alcuna versione precedente di questo pacchetto. Questo è ciò che differenzia l'opzione di refresh dall'opzione di aggiornamento. Infatti, l'operazione di aggiornamento *installa* pacchetti, a prescindere dalla presenza sul sistema di versioni precedenti dei pacchetti.

L'opzione di refresh di RPM funziona sia per singoli pacchetti che per gruppi di pacchetti. Se avete appena scaricato numerosi pacchetti diversi e volete aggiornare quelli presenti sul sistema, scegliete l'opzione di refresh. Con quest'opzione, prima di usare RPM non dovete rimuovere i pacchetti non desiderati dal gruppo scaricato.

In questo caso, potete semplicemente digitare il comando che segue:

```
rpm -Fvh *.rpm
```

RPM aggiorna automaticamente solo i pacchetti che sono già installati.

32.2.6. Interrogazione

Usate il comando `rpm -q` per interrogare il database dei pacchetti installati. Il comando `rpm -q foo` stampa il nome, la versione e la release del pacchetto foo installato:

```
foo-2.0-1
```

Nota Bene

È stato usato il *nome* di pacchetto `foo`. Per interrogare un pacchetto, sostituite `foo` con il nome del pacchetto da interrogare.

Anziché specificare il nome del pacchetto, potete usare le seguenti opzioni con `-q` per specificare i pacchetti che volete interrogare. Queste sono chiamate *Opzioni di specifica del pacchetto*.

- `-a` interroga tutti i pacchetti installati.
- `-f` <*`file`*> interroga il pacchetto contenente il <*`file`*>. Quando specificate un file, dovete indicare il percorso del file (per esempio, `/usr/bin/ls`).
- `-p` <*`filepacchetto`*> interroga il pacchetto <*`filepacchetto`*>.

Ci sono molti modi per specificare quali informazioni devono essere visualizzate sul pacchetto interrogato. Le opzioni seguenti vengono usate per selezionare le informazioni che state cercando. Queste sono chiamate *Opzioni di selezione delle informazioni*.

- `-i` mostra informazioni sul pacchetto, quali il nome, la descrizione, la release, le dimensioni, la data di installazione, il distributore e altro ancora.
- `-l` mostra l'elenco dei file contenuti nel pacchetto.
- `-s` mostra lo stato di tutti i file nel pacchetto.
- `-d` mostra un elenco dei file di documentazione (pagine man, pagine info, file README e così via).
- `-c` mostra un elenco dei file di configurazione. Questi sono i file che potete modificare dopo l'installazione per configurare il pacchetto nel vostro sistema (per esempio `sendmail.cf`, `passwd`, `inittab` e così via).

Per le opzioni che visualizzano elenchi di file, potete aggiungere `-v` al comando perché la visualizzazione degli elenchi sia simile a quella del comando `ls -l`.

32.2.7. Verifica

Il processo di verifica di un pacchetto confronta le informazioni dei file installati da un pacchetto con le informazioni del pacchetto originale. Tra le altre cose, la verifica confronta le dimensioni, MD5, i permessi, il tipo, il proprietario e il gruppo di ogni file.

`rpm -V` verifica un pacchetto. Potete usare un elenco qualsiasi di *opzioni di selezione dei pacchetti* per interrogare i pacchetti specifici che volete verificare. Un uso semplice è `rpm -V foo` che verifica che tutti i file nel pacchetto foo siano identici a quelli installati originariamente. Per esempio:

- Per verificare un pacchetto contenente un file particolare:
  `rpm -Vf /bin/vi`
- Per verificare TUTTI i pacchetti installati:
  `rpm -Va`
- Per verificare i pacchetti installati di un pacchetto RPM:
  `rpm -Vp foo-1.0-1.i386.rpm`

  Può essere utile se sospettate che i vostri database RPM siano danneggiati.

Se tutto è stato verificato correttamente non compare alcun output, mentre le eventuali discrepanze rilevate vengono visualizzate. Il formato dell'output è una stringa di 8 caratteri (una possibile, `c` denota un file di configurazione) e il nome del file. Ogni singolo carattere è il risultato di una comparazione di un attributo del file con il valore dell'attributo in memoria nel database RPM. Un singolo `.` (un punto) significa che la verifica è risultata corretta. I seguenti caratteri indicano errori in alcune verifiche:

- `5` — MD5 checksum
- `S` — dimensioni del file
- `L` — link simbolico
- `T` — ora di modifica del file
- `D` — dispositivo
- `U` — utente
- `G` — gruppo
- `M` — modalità (include permessi e tipo di file)
- `?` — file non leggibile

Se vedete un output, usate il vostro intuito per determinare se è necessario rimuovere o reinstallare il pacchetto oppure risolvere il problema in qualche altro modo.

32.3. Verifica della "firma" di un pacchetto

Per verificare se un pacchetto è stato danneggiato, esaminate l'md5sum digitando il comando seguente al prompt della shell (sostituite <*file-rpm*> con il nome del file del pacchetto RPM):

```
rpm -K --nogpg <rpm-file>
```

Compare a video il messaggio <*file-rpm*>`: md5 OK`. Questo breve messaggio indica che il file non è stato danneggiato durante il trasferimento. Per un messaggio più dettagliato, sostituite `-K` con `-Kvv` nel comando.

Ci si può però fidare dello sviluppatore del pacchetto? Se il pacchetto è *firmato* dalla *chiave* GnuPG dello sviluppatore, allora quest'ultimo è veramente chi dice di essere.

I pacchetti RPM possono essere firmati tramite la Gnu Privacy Guard (o GnuPG) che consente di capire se il pacchetto che avete scaricato è sicuro.

GnuPG, un tool libero per la comunicazione sicura, sostituisce la tecnologia di cifratura PGP, un programma elettronico privato. Grazie a GnuPG, potete autenticare la validità di documenti e cifra-

re/decifrare dati da e verso altri destinatari. GnuPG è in grado di decifrare e verificare anche i file PGP 5.*x*.

Poiché, durante l'installazione di Red Hat Linux, GnuPG viene installato per default, potete subito iniziare a utilizzarlo per verificare i pacchetti che ricevete da Red Hat. Per prima cosa, dovete importare la chiave pubblica di Red Hat.

32.3.1. Importazione delle chiavi

Per verificare i pacchetti di Red Hat ufficiali, è necessario importare la chiave GPG di Red Hat. Per effettuare questa operazione, eseguite il comando riportato di seguito al prompt della shell:

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

Per visualizzare un elenco di tutte le chiavi installate per la verifica RPM, eseguite il comando:

```
rpm -qa gpg-pubkey*
```

Per la chiave di Red Hat l'output comprenderà:

```
gpg-pubkey-db42a60e-37ea5438
```

Per visualizzare i dettagli su una chiave specifica, utilizzate `rpm-qi`, seguito dall'output del comando precedente:

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

32.3.2. Verifica della firma dei pacchetti

Per verificare la firma GnuPG di un file RPM dopo avere importato la chiave GnuPG del costruttore, digitate il comando seguente (sostituite <*file-rpm*> con il nome di file del vostro pacchetto RPM):

```
rpm -K <rpm-file>
```

Se l'operazione va a buon fine, compare a video il messaggio: `md5 gpg OK`, che indica che la firma del pacchetto è stata verificata e che non è danneggiato.

Suggerimento

Per altre informazioni su GnuPG, consultate il Appendice B.

32.4. Sorprendete i vostri amici con RPM

RPM è un tool utile sia per la gestione del sistema sia per la diagnosi e la risoluzione dei problemi. Ecco alcuni esempi delle opzioni di RPM.

- Potreste aver cancellato inavvertitamente alcuni file, ma non sapete esattamente quali. Per controllare l'intero sistema e capire quali file mancano, digitate il comando seguente:
  `rpm -Va`

Se alcuni file sono mancanti o sembrano danneggiati, dovete reinstallare il pacchetto oppure disinstallare e reinstallare il pacchetto.

- Se non riconoscete un file, cercate a quale pacchetto appartiene digitando il comando seguente:
  `rpm -qf /usr/X11R6/bin/ghostview`

  L'output è simile a:
  `gv-3.5.8-22`

- Potete integrare gli esempi sopra citati nella situazione seguente. Supponete di avere dei problemi con `/usr/bin/paste`. Verificate il pacchetto che contiene il programma, però non sapete quale pacchetto contiene `paste`. Eseguite il comando:
  `rpm -Vf /usr/bin/paste`

  e il pacchetto corrispondente verrà verificato.

- Volete ottenere maggiori informazioni su un programma in particolare? Usate il comando seguente per localizzare la documentazione fornita con il pacchetto che contiene tale programma:
  `rpm -qdf /usr/bin/free`

  L'output che ottenete è il seguente:
  ```
  /usr/share/doc/procps-2.0.11/BUGS
  /usr/share/doc/procps-2.0.11/NEWS
  /usr/share/doc/procps-2.0.11/TODO
  /usr/share/man/man1/free.1.gz
  /usr/share/man/man1/oldps.1.gz
  /usr/share/man/man1/pgrep.1.gz
  /usr/share/man/man1/pkill.1.gz
  /usr/share/man/man1/ps.1.gz
  /usr/share/man/man1/skill.1.gz
  /usr/share/man/man1/snice.1.gz
  /usr/share/man/man1/tload.1.gz
  /usr/share/man/man1/top.1.gz
  /usr/share/man/man1/uptime.1.gz
  /usr/share/man/man1/w.1.gz
  /usr/share/man/man1/watch.1.gz
  /usr/share/man/man5/sysctl.conf.5.gz
  /usr/share/man/man8/sysctl.8.gz
  /usr/share/man/man8/vmstat.8.gz
  ```

- Se trovate un nuovo RPM, ma non sapete quali sono le sue funzioni, digitate il comando seguente:
  `rpm -qip crontabs-1.10-5.noarch.rpm`

  L'output è simile a:
  ```
  Name        : crontabs                     Relocations: (not relocateable)
  Version     : 1.10                              Vendor: Red Hat, Inc.
  Release     : 5                             Build Date: Fri 07 Feb 2003 04:07:32 PM EST
  Install date: (not installed)               Build Host: porky.devel.redhat.com
  Group       : System Environment/Base       Source RPM: crontabs-1.10-5.src.rpm
  Size        : 1004                             License: Public Domain
  Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
  Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
  Summary     : Root crontab files used to schedule the execution of programs.
  Description :
  The crontabs package contains root crontab files. Crontab is the
  program used to install, uninstall, or list the tables used to drive the
  cron daemon. The cron daemon checks the crontab files to see when
  particular commands are scheduled to be executed. If commands are
  scheduled, then it executes them.
  ```

- Se volete controllare quali file `crontabs` RPM installa. Potete inserire quanto segue:
  `rpm -qlp crontabs-1.10-5.noarch.rpm`

  L'output che compare a video è simile a:

```
Name        : crontabs                      Relocations: (not relocateable)
Version     : 1.10                              Vendor: Red Hat, Inc.
Release     : 5                             Build Date: Fri 07 Feb 2003 04:07:32 PM EST
Install date: (not installed)               Build Host: porky.devel.redhat.com
Group       : System Environment/Base       Source RPM: crontabs-1.10-5.src.rpm
Size        : 1004                             License: Public Domain
Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : Root crontab files used to schedule the execution of programs.
Description :
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

Questi sono solo alcuni esempi di ciò che RPM può fare. Usandolo ne scoprirete tanti altri.

32.5. Risorse aggiuntive

RPM è un'utilità estremamente complessa con molte opzioni e metodi di interrogazione, installazione, aggiornamento e rimozione di pacchetti. Per maggiori informazioni, consultate le risorse di seguito elencate.

32.5.1. Documentazione installata

- `rpm --help` — il comando visualizza un breve elenco dei parametri di RPM.
- `man rpm` — la pagina man di RPM fornisce maggiori dettagli sui parametri di RPM del comando `rpm --help`.

32.5.2. Siti Web utili

- http://www.rpm.org/ — il sito Web di RPM.
- http://www.redhat.com/mailing-lists/rpm-list/ — contiene la mailing list di RPM. Per iscrivervi, inviate un'e-mail all'indirizzo <`rpm-list-request@redhat.com`> menzionando la parola `subscribe` nell'oggetto.

32.5.3. Libri correlati

- *Maximum RPM* di Ed Bailey; Red Hat Press — una versione online del libro è disponibile all'indirizzo http://www.rpm.org/ e http://www.redhat.com/docs/books/.

Capitolo 33.

Strumento di gestione dei pacchetti

Durante il processo di installazione, gli utenti selezionano un tipo di installazione, come per esempio **Workstation** o **Server**. I pacchetti software vengono installati sulla base di tale scelta. Poiché la gente utilizza il computer in modi differenti a seconda delle proprie esigenze, gli utenti potrebbero voler installare o rimuovere pacchetti anche a installazione ultimata. Il **Strumento di gestione dei pacchetti** consente agli utenti di eseguire tali azioni.

Il Sistema X Windows é necessario per eseguire il **Strumento di gestione dei pacchetti**. Per lanciare l'applicazione, selezionate il **Pulsante menu principale** (sul pannello) => **Impostazioni del sistema** => **Pacchetti** o digitate il comando `redhat-config-packages` al prompt della shell.

La stessa interfaccia appare se inserite il CD-ROM #1 di Red Hat Linux nel vostro computer.

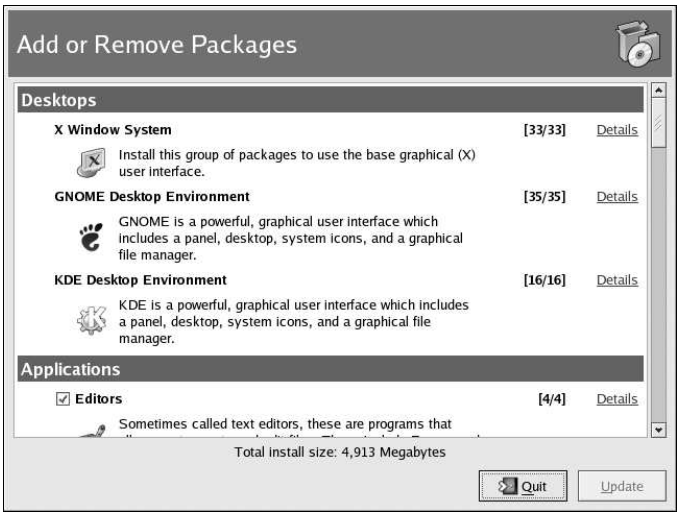

Figura 33-1. Strumento di gestione dei pacchetti

L'interfaccia per questa applicazione è simile a quella utilizzata durante il processo di installazione. I pacchetti si dividono in gruppi di pacchetti, che contengono un elenco di *pacchetti standard* e *pacchetti extra* che condividono alcune funzionalità comuni. Per esempio, il gruppo **Graphical Internet** contiene un browser Web, un client di posta elettronica e altri programmi grafici utilizzati per connettersi a Internet. I pacchetti standard possono essere rimossi solo eliminando l'intero gruppo di pacchetti. I pacchetti extra sono pacchetti opzionali che possono essere installati o rimossi se viene selezionato il gruppo di pacchetti.

La finestra principale mostra un elenco di gruppi di pacchetti. Se la casellina posta accanto a un determinato gruppo di pacchetti è spuntata significa che alcuni pacchetti appartenenti a quel gruppo sono attualmente installati. Per visualizzare l'elenco dei singoli pacchetti installati per un gruppo, fate clic sul pulsante **Dettagli** posto accanto a esso. I singoli pacchetti che presentano una spunta sono quelli attualmente installati.

33.1. Installazione dei pacchetti

Per installare i pacchetti standard in un gruppo di pacchetti attualmente non installato, mettete una spunta nella casellina corrispondente. Per personalizzare i pacchetti da installare all'interno del gruppo, fate clic sul pulsante **Dettagli**. Viene visualizzato l'elenco dei pacchetti standard ed extra, come mostrato nella Figura 33-2. Facendo clic sul nome del pacchetto, in fondo alla finestra viene visualizzato lo spazio disco necessario per installare il pacchetto. Per marcare il pacchetto da installare, basta spuntare la casellina corrispondente.

Potete anche selezionare pacchetti singoli da gruppi di pacchetti già installati facendo clic sul pulsante **Dettagli** e spuntando i pacchetti extra che risultano non ancora installati.

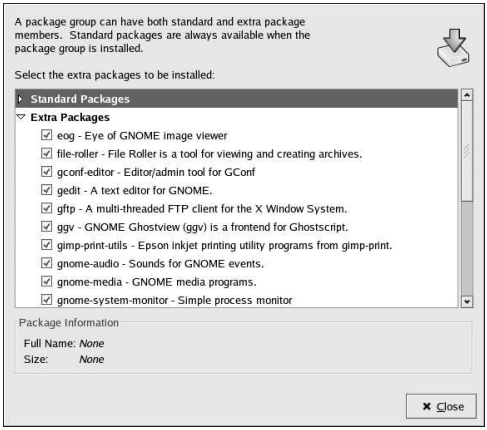

Figura 33-2. Selezione di pacchetti individuali

Dopo aver selezionato i gruppi di pacchetti e i pacchetti singoli da installare, fate clic sul pulsante **Update** posto sulla finestra principale. L'applicazione procederà, quindi, a calcolare la quantità di spazio necessaria per installare i pacchetti, a rilevare eventuali dipendenze e a visualizzare una finestra riassuntiva. Qualora esistessero delle dipendenze, esse verrebbero automaticamente aggiunte all'elenco dei pacchetti da installare. Fate clic sul pulsante **Show Details** per visualizzare l'elenco completo dei pacchetti da installare.

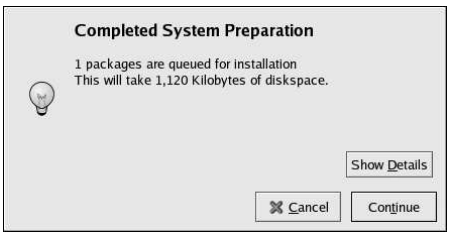

Figura 33-3. Riassunto dell'installazione dei pacchetti

Fate clic su **Continua** per avviare l'installazione. Al termine del processo, compare il messaggio **Update Complete**.

Suggerimento

Se vi servite di **Nautilus** come browser per passare in rassegna i file e le directory presenti sul vostro computer, potete utilizzarlo anche per installare i pacchetti. All'interno di **Nautilus**, andate alla directory che contiene un pacchetto RPM (generalmente hanno estensione `.rpm`) e fate doppio clic sull'icona dell'RPM.

33.2. Rimozione di pacchetti

Per rimuovere tutti i pacchetti installati all'interno di un gruppo di pacchetti, togliete la spunta dalla casellina corrispondente al pacchetto. Per rimuovere singoli pacchetti, fate clic sul pulsante **Dettagli** posto accanto al gruppo di pacchetti in questione e togliete la spunta dai singoli pacchetti.

Quando avete terminato di selezionare i pacchetti da rimuovere, fate clic sul pulsante **Update** posto nella finestra principale. L'applicazione calcola la quantità di spazio disco che verrà liberato e rileva la presenza di eventuali dipendenze relative al software. Se esistono pacchetti che dipendono dal pacchetto che avete selezionato per la rimozione, essi verranno automaticamente aggiunti all'elenco dei pacchetti da rimuovere. Per visualizzarne l'elenco, fate clic sul pulsante **Show Details**.

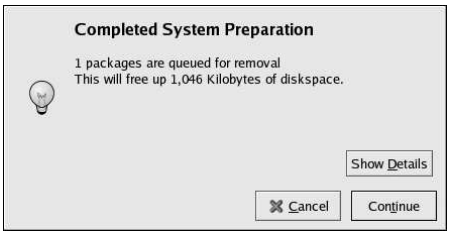

Figura 33-4. Riassunto dei pacchetti da rimuovere

Fate clic su **Continua** per avviare la rimozione. Al termine del processo, compare il messaggio **Update Complete**.

Suggerimento

Potete combinare l'installazione e la rimozione di pacchetti selezionando i gruppi di pacchetti o i singoli pacchetti da installare/rimuovere e facendo poi clic su **Update**. La finestra **Completed System Preparation** visualizzerà il numero dei paccheti da installare e da rimuovere.

Capitolo 34.

Red Hat Network

Red Hat Network è una soluzione Internet per la gestione del sistema Red Hat Linux o di una rete di sistemi Red Hat Linux. Tutti gli avvisi riguardanti la sicurezza, la risoluzione di bug e l'ottimizzazione (collettivamente conosciuti come Avvisi di Errata) possono essere scaricati direttamente da Red Hat usando l'applicazione indipendente **Red Hat Update Agent** oppure tramite il sito Web di RHN all'indirizzo http://rhn.redhat.com/.

Figura 34-1. Il vostro RHN

Red Hat Network permette agli utenti di risparmiare tempo poiché invia un messaggio di posta elettronica che informa della disponibilità di pacchetti aggiornati. Gli utenti non devono navigare sull'Internet alla ricerca di pacchetti aggiornati o avvisi di sicurezza. Di default, Red Hat Network procede anche all'installazione dei pacchetti. Gli utenti non hanno bisogno di imparare a usare RPM o preoccuparsi di risolvere le dipendenze dei pacchetti. RHN fa tutto da solo.

Ogni account di Red Hat Network offre:

- Avvisi Errata — gli avvisi di sicurezza, di risoluzione di bug e di ottimizzazione saranno creati per tutti i sistemi della vostra rete attraverso l'interfaccia Basic

Figura 34-2. Errata Relativa

- Notifica automatica via email — ricevete una notifica via email quando un avviso Errata viene creato per il vostro sistema.
- Aggiornamento programmato degli Errata — programmate l'invio degli aggiornamenti Errata
- Installazione dei pacchetti — programmate l'installazione dei pacchetti su uno o più sistemi con un semplice clic.
- **Red Hat Update Agent** —usate **Red Hat Update Agent** per scaricare gli ultimi pacchetti software adatti al vostro sistema e scegliete se installarli automaticamente.
- Sito Web di Red Hat Network — permette di gestire più sistemi, scaricare singoli pacchetti e programmare azioni quali gli aggiornamenti Errata mediante una connezionesicura di Web browser dal vostro computer.

Per iniziare a usare Red Hat Network, seguite queste tre semplici procedure:

1. Create un profilo di sistema usando uno dei metodi seguenti:
   - Registrate il sistema con RHN durante il **Agent Setup** al primo avvio del sistema dopo l'installazione.
   - Selezionate **Pulsante del Menu Principale => Strumenti di sistema => Red Hat Network** sul vostro desktop.
   - Eseguite il comando `up2date` da un prompt della shell.

2. Collegatevi a RHN all'indirizzo http://rhn.redhat.com/ e abilitare il sistema ai servizi offerti. A ogni utente viene fornito un abbonamento gratuito a Red Hat Network valido per un sistema. Se l'utente lo desidera abbonamenti addizionali possono essere acquistati.

3. Cominciate a programmare gli aggiornamenti tramite il sito Web di RHN oppure scaricate e installate gli aggiornamenti Errata con **Red Hat Update Agent**.

Per informazioni più dettagliate, consultate la *Guida di Referimento per l'utente diRed Hat Network* disponibile all'indirizzo http://www.redhat.com/docs/manuals/RHNetwork/.

Suggerimento

Red Hat Linux include l'applicazione **Red Hat Network Notification Tool**, un pannelo utile di icon che visualizza avvisi visibili quando ci sono aggiornamenti per il vostro sistema Red Hat Linux. Consultate la seguente URL per ulteriori informazioni su applet: http://rhn.redhat.com/help/basic/applet.html

VI. Appendici

Questa sezione contiene le istruzioni per la costruzioni del kernel personale dai file della fonte forniti da Red Hat, Inc.. Esso contiene altresí un capitolo su Gnu Privacy Guard, uno strumento puó essere usato per comunicazioni sicure.

Sommario

Appendice A.

Creazione di un kernel personalizzato

Molti tra i nuovi utenti di Linux si domandano: "per quale motivo dovrei creare il kernel da solo?". Considerando i grandi progressi compiuti nell'utilizzo dei moduli del kernel, la risposta più corretta a questa domanda è: "A meno che tu non conosca già il motivo, probabilmente non ti serve saperlo".

Il kernel fornito con Red Hat Linux e tramite il sistema Errata di Red Hat Linux fornisce supporto per molti hardware di nuova concezione e per contenuti del kernel. Per molti utenti, non c'é bisogno di ricompilarlo. Questa appendice rappresenta una guida per gli utenti che vogliono ricompilare il loro kernel, per gli utenti che vogliono compilare un contenuto sperimentale nel kernel e cosí via.

Per migliorare il kernel usando i pacchetti del kernel distribuiti da Red Hat, Inc., consultare Capitolo 30.

Avviso

La configurazione di un kernel personale non é supportata dal team di supporto d'installazione di Red Hat Linux. Per maggiori informazioni sul miglioramento del kernel usando i pacchetti RPM distribuiti da Red Hat, Inc., consultare Capitolo 30.

A.1. Preparazione alla configurazione

Prima di configurare un kernel personale, é molto importante assicurarsi che esista un dischetto di avvio di emergenza, nel caso in cui si verifica un errore. Per fare un dischetto abilitato all'avvio usando il kernel attuale, eseguire il seguente comando:

```
/sbin/mkbootdisk 'uname -r'
```

Dopo aver fatto il dischetto, provatelo e assicuratevi che sia in grado di avviare il sistema.

Per ricompilare il kernel, deve essere installato il pacchetto `kernel-source`. Emettere il comando

```
rpm -q kernel-source
```

per determinare se é stato installato. Se non é presente, installatelo dai CD-ROM di Red Hat Linux, dal sito FTP di Red Hat ftp://ftp.redhat.com (un elenco dei mirror é disponibile su http://www.redhat.com/mirrors.html), o Red Hat Network. For more information on installing RPM packages, refer to Parte V.

A.2. Configurazione del Kernel

Le istruzioni contenute in questa sezione si riferiscono alla creazione di un kernel modulare. Se invece siete intenzionati a creare e installare un kernel monolitico, per informazioni sui diversi aspetti della sua creazione e installazione, consultate la la Sezione A.3.

Nota Bene

In questo esempio utilizzeremo la versione di kernel 2.4.20-2.47.1, ma la vostra versione può risultare differente. Per determinare la versione del vostro kernel, digitate il comando `uname -r`, sostituite 2.4.20-2.47.1 con la vostra attuale versione di kernel.

Per configurare un kernel personale per l'architettura x86 (effettuare tutte le seguenti fasi):

1. Aprite la shell e spostatevi nella directory `/usr/src/linux-2.4`. Tutti i comandi che andrete a digitare da questo punto in avanti devono essere eseguiti da questa directory.
2. Per iniziare la creazione del kernel, è importante che l'albero sorgente sia "pulito". Pertanto, è consigliabile eseguire prima di tutto il comando `make mrproper`, per rimuovere dal suo interno tutti i file di configurazione e qualsiasi traccia di precedenti compilazioni. Se disponete già di un file di configurazione funzionante (`/usr/src/linux-2.4/.config`) e volete utilizzarlo, salvatelo all'interno di un'altra directory prima di eseguire questo comando e, dopo, copiatelo di nuovo dove si trovava.
3. É consigliabile che la configurazione del kernel di default di Red Hat Linux venga usato come punto di partenza. Per fare questo, copiare il file di configurazione per l'architettura del sistema dalla directory `/usr/src/linux-2.4/configs/` alla directory `/usr/src/linux-2.4/.config`. Se il sistema ha piú di quattro gigabyte di memoria, copiare il file che contiene la keyword `bigmem`.
4. Successivamente, personalizzare le impostazioni. Se il sistema X Window é disponibile, il metodo consigliato é quello di usare il comando `make xconfig` per eseguire **Configurazione del kernel di Linux**.

Nota Bene

Per usare un tool grafico avviato con il comando `make xconfig`, il pacchetto `tk` il quale fornisce il comando `wish`, deve essere installato. For more information on installing RPM packages, refer to Parte V.

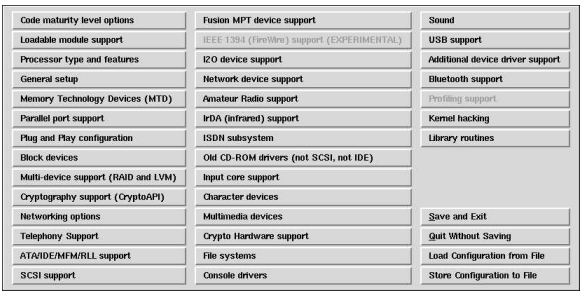

Figura A-1. Configurazione delle categorie del componente del Kernel

Come mostrato in Figura A-1, selezionare una categoria, cliccandoci sopra, da configurare. Tra ogni categoria ci sono i componenti. Selezionare **y** (si), **m** (modulo), o **n** (no) vicino al componente da compilare nel kernel, compilarlo come se fosse un modulo del kernel, oppure non compilarlo. Per saperne di piú sui componenti, fate clic sul pulsante **Aiuto**.

Fate clic sul **Menu principale** per tornare all'elenco delle categorie.

Dopo aver completato la configurazione, fate clic sul **pulsante salva ed esci** nella finestra del menu principale, per creare il file di configurazione `/usr/src/linux-2.4/.config` ed uscire dal programma **Configurazione del Kernel di Linux**.

Anche se nessun cambiamento é stato apportato alle impostazioni, eseguite il comando `make xconfig` (o uno degli altri metodi per la configurazione del kernel) prima di continuare.

Altri metodi disponibili per la configurazione del kernel includono:

- `make config` — un programma di testo interattivo. I componenti da includere nel kernel sono presentati in formato lineare e dovete trattarli uno per volta. Questo metodo non richiede il sistema X Window e non consente di modificare le risposte alle domande precedenti.
- `make menuconfig` — un programma in modalità testo che funziona tramite menu. I componenti sono presentati in un menu ordinato per categorie; i componenti desiderati si selezionano come nel programma di installazione in modalità testo di Red Hat Linux. Selezionate gli elementi corrispondenti digitando: **[*]** (integrato), **[ ]** (escludi), <**M**> (modulo) o < > (supporto per i moduli). Questo metodo non richiede il sistema X Window.
- `make oldconfig` — uno script non interattivo che crea i file di configurazione contenenti le impostazioni di default. Se state usando il kernel predefinito di Red Hat Linux, crea un file di configurazione per il kernel distribuito con Red Hat Linux per la vostra architettura. Questo è utile per configurare il vostro kernel in base a parametri di default funzionanti, scartando poi le caratteristiche che non vi interessano.

Nota Bene

Per utilizzare `kmod` e i moduli del kernel, dovete rispondere **`Sì`** a `kmod support` e `module version (CONFIG_MODVERSIONS) support` nel corso della configurazione.

5. Dopo aver creato il file `/usr/src/linux-2.4/.config`, lanciate il comando `make dep` per configurare correttamente tutte le dipendenze.
6. Lanciate il comando `make clean` per preparare l'albero sorgente per la compilazione.
7. È consigliabile che attribuiate al kernel che state creando un numero di versione modificato, in modo da non sovrascrivere il kernel preesistente. Il metodo qui descritto è il più facile per ovviare a eventuali contrattempi. Se desiderate conoscere altre alternative, andate all'indirizzo http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html oppure nel `Makefile` in `/usr/src/linux-2.4`.

   Per default, `/usr/src/linux-2.4/Makefile` presenta la parola `custom` al termine della linea che inizia con `EXTRAVERSION`. Aggiungendo la stringa potrete avere sul vostro sistema sia il vecchio kernel sia quello nuovo (versione 2.4.20-2.47.1custom), entrambi funzionanti.

   Se il sistema contiene piú di un kernel personale, potete aggiungere la data al termine della stringa (oppure un altro identificatore).
8. Generate il kernel con il comando `make bzImage`.
9. Create gli eventuali moduli che avete configurato con il comando `make modules`.
10. Installate i moduli del kernel (anche se non ne avete creato nessuno) con il comando `make modules_install`. Assicuratevi di digitare l'underscore (_), che farà in modo di installare i moduli del kernel nella directory `/lib/modules/<`*`KERNELVERSION`*`>/kernel/drivers` (dove *`KERNELVERSION`* sta per la versione specificata nel `Makefile`). Nel nostro esempio risulterebbe, dunque, `/lib/modules/2.4.20-2.47.1custom/kernel/drivers/`.
11. Digitate il comando `make install` per copiare il vostro kernel e i file a esso associati nelle rispettive directory.

    Oltre a consentire l'installazione dei file del kernel all'interno della directory `/boot`, questo comando esegue lo script `/sbin/new-kernel-pkg`, che crea una nuova immagine `initrd` e aggiunge nuove voci al file di configurazione del boot loader.

    Se possedete un adattatore SCSI e avete ricompilato il driver SCSI come modulo o avete compilato il kernel con supporto ext3 come modulo (quello predefinito in Red Hat Linux), vi occorre l'immagine `initrd`.

12. Anche se l'immagine `initrd` e le modifiche al boot loader sono fatte su misura per voi, è bene verificare che siano state fatte correttamente e che sia stato usato la versione del kernel personale invece di 2.4.20-2.47.1. Per i dettagli, consultate la la Sezione 30.5 e la la Sezione 30.6.

A.3. Creazione di un kernel monolitico

Per creare un kernel monolitico si segue lo stesso procedimento necessario per compilare un kernel modulare, con qualche eccezione.

- Quando configurate il kernel, non compilate niente come modulo. In altre parole, rispondete solo **`Si`** e **`No`** alle domande. Inoltre, dovete rispondere **`No`** a `kmod support` e a `module version (CONFIG_MODVERSIONS) support`.
- Tralasciate i seguenti punti:
  ```
  make modules
  make modules_install
  ```
- Aggiungere alla riga `kernel` in `grub.conf` con `nomodules` o modificare `lilo.conf` per includere la riga `append=nomodules`

A.4. Risorse aggiuntive

For more information on the Linux kernel, refer to the following resources.

A.4.1. Documentazione installata

- `/usr/src/linux-2.4/Documentation` — documentazione avanzata sul kernel di Linux e sui suoi moduli. Tali documenti sono rivolti a persone interessate a contribuire al codice sorgente del kernel e a capire il funzionamento del kernel.

A.4.2. Siti Web utili

- http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html — *The Linux Kernel HOWTO* tratto dal progetto di documentazione di Linux.
- http://www.kernel.org/pub/linux/docs/lkml/ — la mailing list del kernel di Linux.

Appendice B.

Uso di Gnu Privacy Guard

B.1. Introduzione all'uso di GnuPG

Vi siete mai chiesti se i vostri messaggi di posta elettronica possono essere intercettati durante la trasmissione al (o dal) vostro computer? Ebbene, la vostra posta può essere intercettata o manipolata da perfetti estranei.

Con la posta tradizionale le lettere vengono chiuse in buste sigillate, affrancate e smistate presso l'ufficio postale per essere inviate alla destinazione indicata. L'invio di posta tramite Internet, invece, non è altrettanto sicuro. La posta elettronica viene trasmessa da server a server in chiaro e di solito non vengono prese misure di protezione per evitare che la corrispondenza venga letta o manipolata da persone estranee.

Per tutelare la vostra privacy, Red Hat Linux 9 fornisce GnuPG, il programma *GNU Privacy Guard* che viene installato per default durante un'installazione standard di Red Hat Linux. È conosciuto anche come *GPG*.

GnuPG è un tool che assicura comunicazioni sicure. Si tratta di un sostituto valido e gratuito della tecnologia di cifratura PGP (Pretty Good Privacy, un'applicazione di cifratura molto diffusa). Usando GnuPG, potete cifrare i vostri dati e la corrispondenza e inoltre potete autenticare i vostri messaggi e-mail con la *firma digitale*. GnuPG è inoltre in grado di decifrare e verificare PGP 5.*x*.

Dal momento che GnuPG è compatibile con altri standard di cifratura, la vostra corrispondenza sicura sarà probabilmente compatibile con applicazioni di posta elettronica di altri sistemi operativi, come Windows e Macintosh.

GnuPG usa *una cifratura a chiave pubblica* in modo da consentire lo scambio sicuro di dati. In uno schema di crittografia a chiave pubblica vengono generate due chiavi: una chiave pubblica e una privata. La chiave pubblica viene scambiata con gli altri destinatari o con un server delle chiavi. Non dovreste mai rivelare la vostra chiave privata.

La cifratura dipende dall'uso delle chiavi. Nella cifratura convenzionale o simmetrica, entrambe le estremità della transazione possiedono la stessa chiave, usata per decodificare le trasmissioni. Nella cifratura a chiave pubblica, coesistono due chiavi: una chiave pubblica e una privata. Una persona o un'organizzazione di solito non divulga la chiave privata, mentre rivela quella pubblica. I dati codificati con la chiave pubblica possono essere decodificati solo con la chiave privata; i dati codificati con la chiave privata possono essere decodificati solo con la chiave pubblica.

Importante

Ricordate che la chiave pubblica può essere resa nota a coloro coi quali intendete comunicare in modo sicuro, ma non rivelate mai a nessuno la vostra chiave privata.

Poiché la cifratura esula dallo scopo di questo manuale, per approfondimenti vi consigliamo di consultare altra documentazione. In questo capitolo, comunque, cercheremo di fornirvi le informazioni principali su GnuPG per iniziare a usare la cifratura nella vostra corrispondenza. Per maggiori informazioni su GnuPG, inclusa la guida utente online, visitate la pagina Web http://www.gnupg.org/. Se desiderate avere maggiori informazioni relative a GnuPG, PGP e alla tecnologia di cifratura, consultate la la Sezione B.8.

B.2. Messaggi di avvertenza

Quando eseguite i comandi GnuPG, probabilmente verrà visualizzato il seguente messaggio:

```
gpg: Warning: using insecure memory!
```

Questa avvertenza indica che gli utenti non root non possono bloccare le pagine della memoria. Se gli utenti potessero farlo, potrebbero effettuare attacchi di negazione del servizio out-of-memory, causando un probabile problema di sicurezza. Per maggiori dettagli, fate riferimento alla pagina Web http://www.gnupg.org/faq.html#q6.1.

Se avete effettuato l'aggiornamento da una versione precedente di GnuPG, potreste visualizzare il seguente messaggio:

```
gpg: WARNING: --honor-http-proxy is a deprecated option.
gpg: please use "--keyserver-options honor-http-proxy" instead
```

Questa avvertenza indica che il file `~/.gnupg/options` contiene la riga:

```
honor-http-proxy
```

La versione 1.0.7 preferisce una sintassi diversa. Modificate la riga come indicato di seguito:

```
keyserver-options honor-http-proxy
```

B.3. Creazione di due chiavi

Per poter usare GnuPG, dovete innanzitutto creare due nuove chiavi: una chiave pubblica e una privata.

Per generare una coppia di chiavi, al prompt della shell digitate quanto segue:

```
gpg --gen-key
```

Poiché di solito lavorate con l'account utente, questo comando deve essere eseguito dal vostro account utente e non come utente root.

Compare una schermata introduttiva, con le opzioni per le chiavi, tra cui un'opzione consigliata (default), simile alla seguente:

```
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
   (1) DSA and ElGamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
Your selection?
```

In realtà, la maggior parte delle schermate che vi richiedono di scegliere un valore visualizza l'opzione di default chiusa tra parentesi. Potete accettare le opzioni di default premendo [Invio].

Nella prima schermata dovrete accettare l'opzione di default: `(1) DSA and ElGamal`. Questa opzione vi consente di creare una firma digitale e cifrare (e decifrare) con due tipi di tecnologie. Digitate **1** e premete [Invio].

Scegliete poi la dimensione o la lunghezza della chiave. In generale, più la chiave è lunga, maggiore è la resistenza agli attacchi verso i vostri messaggi di posta. La dimensione predefinita, 1024 bit, è sufficiente per la maggior parte degli utenti. Dunque premete pure [Invio].

Nell'opzione successiva dovete specificare la durata della validità della chiave. Di solito il valore di default (`0 = key does not expire`) è la scelta migliore. Se stabilite una data di scadenza, ricordate che le persone a cui avete fornito la chiave pubblica devono essere informate della scadenza ed è quindi necessario indicare loro la nuova chiave pubblica. Se, al contrario, non scegliete una data di scadenza, vi verrà richiesto di confermare la vostra decisione. Premete [y] per la conferma.

È ora necessario indicare un ID utente costituito dal vostro nome, dal vostro indirizzo e-mail ed eventualmente da un commento. Al termine vi viene presentato un riepilogo delle informazioni inserite.

Una volta confermate le vostre scelte, dovete inserire una frase di accesso.

Suggerimento

Come per le password dell'account, è necessario inserire una frase di accesso sicura in GnuPG per ottenere una sicurezza ottimale. Potete inserire, per esempio, lettere maiuscole e minuscole, numeri o segni di punteggiatura.

Dopo aver inserito e verificato la frase di accesso, vengono generate le chiavi. Compare un messaggio simile al seguente:

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++.+++++.++++++++....++++++++++..+++++.+++++.+++++++.+++++++
+++.++++++++++++++++++++++++++++++++++++++++.........................++++
```

Cessata l'attività sullo schermo, le vostre nuove chiavi vengono create e posizionate nella directory `.gnupg` all'interno della vostra directory home. Per ottenere un elenco delle chiavi, usate il comando:

```
gpg --list-keys
```

L'output visualizzato sarà simile al seguente:

```
/home/newuser/.gnupg/pubring.gpg
--------------------------------------
pub  1024D/B7085C8A 2000-06-18 Your Name <you@yourisp.net>
sub  1024g/E12AF9C4 2000-06-18
```

Se avete creato una chiave GnuPG con la versione 1.0.6 o inferiore e avete esportato la chiave privata per importarla in una chiave nuova, dovete fidarvi esplicitamente della vostra chiave per firmare gli elementi con la versione 1.0.7. Per fidarvi della vostra chiave, digitate il comando seguente (sostituire *<id-utente>*):

```
gpg --edit-key <id-utente>
```

Al prompt `Command>` digitate **`trust`** e selezionate `5 = I trust ultimately` per rendere fidata la vostra chiave.

B.4. Creazione di un certificato di revoca

Una volta create le chiavi, dovete creare un certificato di revoca per la chiave pubblica. Se dimenticate la frase di accesso oppure se vi accorgete che è stata compromessa, potete pubblicare questo certificato per informare gli utenti che la vostra chiave pubblica non va più utilizzata.

Nota Bene

Quando generate un certificato di revoca, non state revocando la chiave appena creata. Vi garantite semplicemente un modo sicuro per revocare la chiave pubblica. Supponiamo di creare una chiave e poi di dimenticare la frase di accesso, di cambiare provider (indirizzi) oppure di subire un crash del disco fisso. Il certificato di revoca può essere usato per rendere inutilizzabile la vostra chiave pubblica.

La vostra firma sarà valida per i destinatari della corrispondenza prima che la chiave sia revocata e sarete in grado di decifrare i messaggi ricevuti prima della revoca. Per creare un certificato di revoca, usate l'opzione `--gen-revoke`:

```
gpg --output revoke.asc --gen-revoke  <you@yourisp.net>
```

Se omettete l'opzione `--output revoke.asc` il vostro certificato di revoca viene visualizzato sullo schermo. Invece di copiare e incollare i contenuti dell'output in un file di vostra scelta usando un editor di testi, quale Pico, è probabilmente più semplice inviare l'output a un file nella vostra directory di login. In questo modo potete memorizzare il certificato per scopi futuri oppure copiarlo su un dischetto e conservarlo in un luogo sicuro.

L'output è simile a quanto segue:

```
sec  1024D/823D25A9 2000-04-26  nome <you@yourisp.net>

Create a revocation certificate for this key?
```

Premete [Y] per creare un certificato di revoca per la chiave elencata. Vi verrà quindi richiesto di selezionare il motivo della revoca e di fornire una descrizione opzionale. Dopo avere confermato la motivazione, digitate la frase di accesso utilizzata per generare la chiave.

Il certificato di revoca (`revoke.asc`) appena creato viene posizionato nella directory di login. Copiate il certificato in un dischetto floppy e conservatelo in un luogo sicuro. Se non sapete come copiare un file su dischetto con Red Hat Linux, consultate la *Red Hat Linux Getting Started Guide*.

B.5. Esportazione della chiave pubblica

Prima di poter usare la cifratura a chiave pubblica, le altre persone devono ricevere una copia di tale chiave. Per inviarla ai vostri destinatari o al server delle chiavi, è necessario *esportare* la chiave.

Per esportare la vostra chiave, in modo da poterla visualizzare su una pagina Web o incollarla in un messaggio e-mail, digitate quanto segue:

```
gpg --armor --export <you@yourisp.net> > mykey.asc
```

Non viene visualizzato alcun output, perché non solo avete esportato la chiave pubblica, ma avete reindirizzato l'output in un file chiamato, per esempio, `mykey.asc`. Se non aggiungete `> mykey.asc`, la chiave viene visualizzata come output standard sullo schermo del monitor.

A questo punto il file `mykey.asc` può essere inserito in un messaggio e-mail o esportato in un server di chiavi. Per vedere la chiave, digitate `less mykey.asc` per aprire il file in un pager (digitate [q] per uscire dal pager). L'output sarà simile al seguente:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDkHP3URBACkWGsYh43pkXU9wj/X1G67K8/DSrl85r7dNtHNfLL/ewil10k2
q8saWJn26QZPsDVqdUJMOdHfJ6kQTAt9NzQbgcVrxLYNfgeBsvkHF/POtnYcZRgL
tZ6syBBWs8JB4xt5V09iJSGAMPUQE8Jpdn2aRXPApdoDw179LM8Rq6r+gwCg5ZZa
pGNlkgFu24WM5wC1zg4QTbMD/3MJCSxfL99Ek5HXcB3yhj+o0LmIrGAVBgoWdrRd
BIGjQQFhV1NSwC8YhN/4nGHWpaTxgEtnb4CI1wI/G3DK9olYMyRJinkGJ6XYfP3b
cCQmqATDF5ugIAmdditnw7deXqn/eavaMxRXJM/RQSgJJyVpbAO2OqKe6L6Inb5H
kjcZA/9obTm499dDMRQ/CNR92fA5pr0zriy/ziLUow+cqI59nt+bEb9nY1mfmUN6
SW0jCH+pIQH51erV+EookyOyq3ocUdjeRYF/d2jl9xmeSyL2H3tDvnuE6vgqFU/N
sdvby4B2Iku7S/h06W6GPQAe+pzdyX9vS+Pnf8osu7W3j60WprQkUGF1bCBHYWxs
YWdoZXIgPHBhdWxnYWxsQHJlZGhhdC5jb20+iFYEExECABYFAjkHP3UECwoEAwMV
AwIDFgIBAheAAAoJEJECmvGCPSWpMjQAoNF2zvRgdR/8or9pBhu95zeSnkb7AKCm
/uXVS0a5KoN7J61/1vEwx11poLkBDQQ5Bz+MEAQA8ztcWRJjW8cHCgLaE402jyqQ
37gDT/n4VS66nU+YItzDFScVmgMuFRzhibLblfO9TpZzxEbSF3T6p9hLLnHCQ1bD
HRsKfh0eJYMMqB3+HyUpNeqCMEEd9AnWD9P4rQtO7Pes38sV01X0OSvsTyMG9wEB
vSNZk+Rl+phA55r1s8cAAwUEAJjqazvk0bgFrw1OPG9m7fEeDlvPSV6HSA0fvz4w
c7ckfpuxg/URQNf3TJA00Acprk8Gg8J2CtebAyR/sP5IsrK5llluGdk+l0M85FpT
/cen2OdJtToAF/6fGnIkeCeP1O5aWTbDgdAUHBRykpdWU3GJ7NS6923fVg5khQWg
uwrAiEYEGBECAAYFAjkHP4wACgkQkQKa8YI9JamliwCfXox/HjlorMKnQRJkeBcZ
iLyPH1QAoI33Ft/0HBqLtqdtP4vWYQRbibjW
=BMEc
-----END PGP PUBLIC KEY BLOCK-----
```

B.5.1. Esportazione in un server delle chiavi

Se scrivete solo a pochi destinatari, potete esportare la vostra chiave pubblica e inviarla loro personalmente. Invece, se corrispondete con molte persone, distribuire la chiave potrebbe farvi perdere molto tempo, dunque vi conviene utilizzare un server delle chiavi.

Un server delle chiavi è un "deposito" in Internet che può contenere e distribuire la vostra chiave pubblica a chiunque la richieda. Sono disponibili molti server delle chiavi e la maggior parte di essi cerca di rimanere sincronizzato con gli altri. Inviare la vostra chiave a un server delle chiavi è come distribuirla a tutti i server. I destinatari potranno richiedere la vostra chiave pubblica a un server delle chiavi e importarla nel proprio keyring, (file contenente le chiavi pubbliche e private), dopodiché potranno corrispondere con voi in modo sicuro.

Suggerimento

Poiché la maggior parte dei server delle chiavi è sincronizzata, inviare la chiave pubblica a un server solo equivale a inviarla a tutti. Tuttavia, è possibile trovare diversi server delle chiavi. Potete iniziare la ricerca e ottenere maggiori informazioni in *Keyserver.Net* disponibile all'indirizzo http://www.keyserver.net.

Potete inviare la vostra chiave pubblica dal prompt della shell o da un browser; naturalmente dovete essere online per inviare o ricevere le chiavi da un server delle chiavi.

- Dal prompt della shell, digitate quanto segue:
  `gpg --keyserver search.keyserver.net --send-key you@yourisp.net`

- Dal vostro browser andate sul sito di Keyserver.Net (http://www.keyserver.net) e selezionate l'opzione per aggiungere la vostra chiave pubblica PGP.

  È ora necessario copiare e incollare la chiave pubblica nell'apposita area della pagina Web. Se non sapete come farlo, seguite le istruzioni qui elencate:

  - Aprite il file con la chiave pubblica esportata (per esempio *`mykey.asc`*, nella Sezione B.5) con un pager — usate per esempio, il comando `less mykey.asc`.
  - Con il mouse, copiate il file selezionando tutte le righe da `BEGIN PGP` a `END PGP` (vedere la Figura B-1).
  - Incollate i contenuti del file *`mykey.asc`* nell'apposita area della pagina su Keyserver.Net facendo clic con il tasto centrale del mouse (o con entrambi i tasti se avete un mouse a due pulsanti). Selezionate poi il pulsante **Submit** sulla pagina del server delle chiavi. Se commettete un errore, premete il pulsante **Reset** per cancellare quanto inserito.

Figura B-1. Copia della chiave pubblica

Se state inviando la vostra chiave a un altro server delle chiavi basato sul Web, vale comunque la transazione descritta sopra.

Questo è quanto dovete fare. Indipendentemente dal fatto di usare il prompt della shell o il Web, compare un messaggio con indicato che la vostra chiave è stata inviata correttamente — al prompt della shell o al sito Web del server delle chiavi. Da questo punto in poi, gli utenti che desiderano comunicare in modo sicuro con voi possono importare la vostra chiave pubblica e aggiungerla al proprio keyring.

B.6. Importazione di una chiave pubblica

L'altra "estremità" dello scambio di chiavi è importare le chiavi pubbliche di altre persone nel proprio keyring — operazione tanto facile quanto esportare le chiavi. Quando importate la chiave pubblica di qualcuno, potete decifrare la loro posta e controllare la loro firma digitale tramite la chiave pubblica che avete memorizzato nel vostro keyring.

Per importare la chiave in modo semplice, scaricatela e salvatela dal Web.

Dopo aver scaricato una chiave e averla salvata nel file *key.asc*, utilizzate il comando riportato di seguito per aggiungerla al vostro keyring.

```
gpg --import key.asc
```

Un altro modo di salvare la chiave consiste nell'utilizzare il comando del vostro browser **Save As**. Se utilizzate un browser come **Mozilla** e notate una chiave in un server delle chiavi, potete salvare la pagina come testo (andate alla voce **File => Save Page As**). Nel menu a discesa accanto a **Files of Type**, selezionate **Text Files**. È ora possibile importare la chiave — ma ricordate il nome del file che avete salvato. Supponiamo per esempio di avere appena salvato una chiave in un file di testo chiamato *newkey.txt*. Per importare il file, dal prompt della shell digitate il seguente comando:

```
gpg --import newkey.txt
```

L'output è simile a quanto segue:

```
gpg: key F78FFE84: public key imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Per verificare se il processo si è concluso correttamente, utilizzate il comando `gpg --list-keys`; dovreste vedere le vostre nuove chiavi elencate nel keyring.

Quando importate una chiave pubblica, potete aggiungerla al vostro *keyring* (un file in cui vengono conservate chiavi pubbliche e segrete). Quando poi eseguite il download di un documento da tale entità, potete verificare la validità del documento con la chiave che avete aggiunto al keyring.

B.7. Cosa sono le firme digitali?

Le firme digitali possono essere paragonate alla propria firma scritta. Diversamente dalla corrispondenza tradizionale, in cui è possibile falsificare la grafia di un'altra persona, le firme digitali non possono essere contraffatte. Questo perché la firma viene generata con la vostra chiave segreta che può essere verificata dal destinatario tramite la chiave pubblica.

Una firma digitale è composta anche dalla data e dall'ora di invio del documento. Così se qualcuno tenta di modificare il documento, la verifica della firma lo segnalerà e non andrà a buon fine. Alcune applicazioni di posta elettronica, quali **Exmh** o **KMail** di KDE, comprendono la possibilità di firmare documenti con GnuPG nell'interfaccia dell'applicazione.

Esistono due tipi utili di firme digitali: *clearsigned* e *detached signatures*. Entrambi i tipi offrono la stessa sicurezza per l'autenticazione, senza richiedere di decodificare l'intero messaggio.

In un messaggio clearsigned la vostra firma appare come un blocco di testo inserito nel contesto della lettera. Una firma detached viene inviata come file separato insieme alla corrispondenza.

B.8. Risorse aggiuntive

La tecnologia di cifratura è un argomento talmente vasto da non poter essere trattato ampiamente in una breve introduzione a GnuPG. Dunque, se vi occorrono ulteriori informazioni a riguardo, consultate le fonti elencate qui di seguito.

B.8.1. Documentazione installata

- `man gpg` e `info gpg` — Guida di riferimento per comandi e opzioni GnuPG.

B.8.2. Siti Web utili

- http://www.gnupg.org — il sito Web di GnuPG con link utili alle release più recenti di GnuPG, una guida utente completa e altre risorse di cifratura.
- http://hotwired.lycos.com/webmonkey/backend/security/tutorials/tutorial1.html — visitate *Encryption Tutorial* nel sito di Webmonkey: scoprirete molte novità sulle tecniche di cifratura e su come applicarle.
- http://www.eff.org/pub/Privacy — il sito di Electronic Frontier Foundation, archivio su privacy, sicurezza, cifratura e sorveglianza.

B.8.3. Libri correlati

- *The Official PGP User's Guide* di Philip R. Zimmerman; edizioni MIT Press.
- *PGP: Pretty Good Privacy* di Simson Garfinkel; edizioni O'Reilly & Associates, Inc.
- *E-Mail Security: How to Keep Your Electronic Messages Private* di Bruce Schneier; edizioni John Wiley & Sons.

Indice

Simboli

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Colophon

I manuali sono scritti in formato DocBook SGML v4.1. I formati HTML e PDF vengono prodotti usando i fogli stile DSSSL personali e script wrapper jade personali. I file SGML DocBook sono scritti in **Emacs** con l'aiuto della modalitá PSGML.

Garrett LeSage ha creato le grafiche di ammonizione (nota, suggerimento, importante attenzione e avviso). Essi possono essere ridistribuiti liberamente con la documentazione Red Hat.

Il team di documentazione del prodotto di Red Hat Linux é composto dalle seguenti persone:

Sandra A. Moore — Primary Writer/Maintainer della *Red Hat Linux x86 Installation Guide*; Contributing Writer alla *Red Hat Linux Getting Started Guide*

Tammy Fox — Primary Writer/Maintainer della *Red Hat Linux Customization Guide*; Contributing Writer alla *Red Hat Linux Getting Started Guide*; Writer/Maintainer dei fogli stile DocBook personali e degli script.

Edward C. Bailey — Primary Writer/Maintainer della *Red Hat Linux System Administration Primer*; Contributing Writer alla *Red Hat Linux x86 Installation Guide*

Johnray Fuller — Primary Writer/Maintainer della *Red Hat Linux Reference Guide*; Co-writer/Co-maintainer della *Red Hat Linux Security Guide*; Contributing Writer alla *Red Hat Linux System Administration Primer*

John Ha — Primary Writer/Maintainer alla *Red Hat Linux Getting Started Guide*; Co-writer/Co-maintainer della *Red Hat Linux Security Guide*; Contributing Writer alla *Red Hat Linux System Administration Primer*