Red Hat Linux 7.1

Official Red Hat Linux Reference Guide

ISBN: N/A


Red Hat, Inc.

2600 Meridian Parkway
Durham , NC 27713 USA

Research Triangle Park, NC 27709 USA

rhl-rg(IT)-7.1-Print-RHI (2001-02-21T10:50-0500)

Stampato in Canada, Irlanda e Giappone

Indice

Red Hat Linux 7.1

Introduzione ix
- Ricerca della documentazione adatta ix
- Convenzioni xii
- Uso del mouse xvi
- Copia e incolla in X xvi
- Prossimamente xvi
- Ricordatevi di registrarvi xvii

Parte I Il sistema 19

Capitolo 1 Struttura del filesystem 21
- 1.1 Perché condividere una struttura comune? 21
- 1.2 Panoramica sull'FHS 21
- 1.3 /proc e i suoi "file" 26
- 1.4 Directory speciali di Red Hat 27

Capitolo 2 Utenti e gruppi 29
- 2.1 Tool per l'amministrazione di utenti e gruppi 29
- 2.2 Utenti standard 29
- 2.3 Gruppi standard 30
- 2.4 Gruppi privati utente 31

Capitolo 3 Processo di avvio, init e spegnimento 35
- 3.1 Introduzione 35
- 3.2 I retroscena del processo di avvio 35
- 3.3 Informazioni su Sysconfig 43
- 3.4 Inizializzazione dei runlevel 56
- 3.5 Utility di initscript 57
- 3.6 Esecuzione dei programmi all'avvio 57

3.7 Chiusura del sistema 57
3.8 Differenze nel processo di avvio di altre architetture 58

Capitolo 4 LDAP (Lightweight Directory Access Protocol) 59
4.1 Cos'è il protocollo LDAP? 59
4.2 Vantaggi e svantaggi del protocollo LDAP 59
4.3 Uso dell'LDAP 60
4.4 Terminologia dell'LDAP 61
4.5 OpenLDAP 2.0 - Versione aggiornata 62
4.6 I file di OpenLDAP 62
4.7 Demoni e utility di OpenLDAP 64
4.8 Moduli per aggiungere funzioni a LDAP 65
4.9 LDAP HowTo: un rapido riepilogo 66
4.10 Configurazione del sistema per l'autenticazione con OpenLDAP 66
4.11 Risorse aggiuntive 69

Capitolo 5 CCVS (Principi del Credit Card Verification System) 71
5.1 Utilizzi del CCVS 71
5.2 Processo di verifica della carta di credito 73
5.3 Requisiti per l'uso di CCVS 73
5.4 Installazione del CCVS 76
5.5 Prima di configurare il CCVS 76
5.6 Configurazione del CCVS 77
5.7 Conti commerciante multipli 82
5.8 Avvio del CCVS 83
5.9 Considerazioni sui linguaggi 84
5.10 Assistenza per il sistema CCVS 84
5.11 Risorse aggiuntive 84

Capitolo 6 Sendmail 87
6.1 Introduzione a Sendmail 87
6.2 Installazione predefinita di Sendmail 88

6.3 Modifiche della configurazione 89
6.4 Blocco degli spam 90
6.5 Uso di Sendmail con LDAP 91
6.6 Risorse aggiuntive 92

Parte II La sicurezza 95

Capitolo 7 Compendio sulla sicurezza di Red Hat Linux 97
7.1 L'inevitabile dilemma sulla sicurezza 97
7.2 Approccio attivo contro approccio passivo 98
7.3 Sviluppo delle politiche di sicurezza 100
7.4 Ulteriori passi per la protezione del sistema 101
7.5 L'importanza di password sicure 101
7.6 Sicurezza della rete 102
7.7 Risorse aggiuntive 103

Capitolo 8 Moduli di autenticazione PAM 105
8.1 I vantaggi di PAM 105
8.2 File di configurazione PAM 105
8.3 Password shadow 111
8.4 Utilizzo di rlogin, rsh e rexec con PAM 111
8.5 Risorse aggiuntive 112

Capitolo 9 Kerberos 5 su Red Hat Linux 113
9.1 Perché usare Kerberos? 113
9.2 Perché non usare Kerberos? 113
9.3 Terminologia Kerberos 114
9.4 Funzionamento di Kerberos 115
9.5 Configurazione di un server Kerberos 5 su Red Hat Linux 7.1 116
9.6 Configurazione di un client Kerberos 5 su Red Hat Linux 7.1 119
9.7 Kerberos e PAM 120
9.8 Risorse aggiuntive 120

Capitolo 10 Installazione e configurazione di Tripwire 123
10.1 Come usare Tripwire 123
10.2 Istruzioni per l'installazione 125
10.3 Posizione dei file 128
10.4 Componenti di Tripwire 128
10.5 Modifica del file di policy 129
10.6 Scelta delle chiavi 129
10.7 Inizializzazione del database 130
10.8 Controllo dell'integrità 130
10.9 Visualizzazione dei report 131
10.10 Aggiornamento del database dopo un controllo dell'integrità 133
10.11 Aggiornamento del file di policy 134
10.12 Tripwire e la posta elettronica 135
10.13 Risorse aggiuntive 136

Capitolo 11 Protocollo SSH 139
11.1 Introduzione 139
11.2 Sequenza degli eventi di una connessione SSH 140
11.3 Livelli di sicurezza SSH 142
11.4 File di configurazione OpenSSH 144
11.5 Più di una Secure Shell 145
11.6 SSH per le connessioni remote 147

Capitolo 12 Controllo degli accessi e dei privilegi 149
12.1 Utility shadow 149
12.2 Configurazione dell'accesso alla console 150
12.3 Gruppo floppy 154

Parte III Apache 155

Capitolo 13 Utilizzo di Apache come server Web sicuro 157
13.1 Introduzione 157
13.2 Ringraziamenti 158

13.3 Panoramica sui pacchetti relativi alla sicurezza 158
13.4 Installazione del server sicuro 160
13.5 Installazione del server sicuro con Red Hat Linux 161
13.6 Aggiornamento da una versione precedente di Red Hat Linux 162
13.7 Installazione del server sicuro dopo l'installazione di Red Hat Linux 163
13.8 Aggiornamento da una versione precedente di Apache 164
13.9 Panoramica sui certificati e la sicurezza 165
13.10 Utilizzo di chiavi e certificati pre-esistenti 166
13.11 Tipi di certificati 167
13.12 Creazione di una chiave 168
13.13 Come richiedere un certificato a una CA 170
13.14 Creazione di un certificato "self-signed" 172
13.15 Verifica del certificato 173
13.16 Accesso al server sicuro 174
13.17 Risorse aggiuntive 175

Capitolo 14 Direttive e moduli Apache 177
14.1 Avvio e chiusura di httpd 177
14.2 Direttive di configurazione in httpd.conf 178
14.3 Aggiungere moduli al server 199
14.4 L'uso degli host virtuali 202

Parte IV Appendici 207

Appendice A Parametri generali dei moduli 209
A.1 Come specificare i parametri dei moduli 210
A.2 Parametri per i CD-ROM 210
A.3 Parametri SCSI 213
A.4 Parametri Ethernet 217

Appendice B Introduzione al partizionamento del disco 225
B.1 Concetti di base riguardanti i dischi fissi 225

Appendice C Dischetto dei driver 247
C.1 Perché ho bisogno di un disco contenente dei driver? 247

Appendice D RAID (Redundant Array of Independent Disks) 251
D.1 Cos'è il RAID? 251

Appendice E PowerTools 255
E.1 Cosa sono i PowerTools? 255
E.2 Pacchetti PowerTools 255
E.3 Installazione dei pacchetti PowerTools 257
E.4 Rimozione dell'installazione di PowerTools 258

Introduzione

Benvenuti nella *Official Red Hat Linux Reference Guide*.

La *Official Red Hat Linux Reference Guide* contiene informazioni utili relative al sistema Red Hat Linux. Dai concetti di base, come la struttura dei filesystem, ad argomenti più complessi, come il partizionamento del disco e il controllo dell'autenticazione, ci auguriamo che questo libro possa rappresentare una risorsa preziosa.

In questo manuale vengono trattati vari argomenti tra cui:

- *Partizionamento del disco* — concetti e strategie sul partizionamento del disco per l'installazione di più sistemi operativi sullo stesso disco fisso.
- *Avvio di Red Hat Linux* — informazioni sui runlevel, sulle directory `rc.d` e su come attivare le vostre applicazioni preferite all'avvio del sistema.
- *Sicurezza del sistema e della rete* — per scoprire i metodi più usati da chi vuole compromettere il vostro sistema e per evitare problemi di sicurezza.
- *RAID* — per utilizzare più dischi fissi come un'unica unità logica, aumentandone così le prestazioni e l'affidabilità.
- *Installazione dei server Web sicuri* — per fornire al vostro server Web Apache funzionalità di cifratura.

Prima di leggere questa guida, assicuratevi di conoscere i passi relativi all'installazione contenuti nella *Official Red Hat Linux x86 Installation Guide*, i concetti fondamentali contenuti nella *Official Red Hat Linux Getting Started Guide* e le istruzioni relative alla personalizzazione che potete trovare nella *Official Red Hat Linux Customization Guide*. La *Official Red Hat Linux Reference Guide* contiene informazioni su argomenti piuttosto complessi che necessitano di una conoscenza abbastanza approfondita del sistema Red Hat Linux.

Tutti i manuali della versione ufficiale di Red Hat Linux sono disponibili in formato HTML e PDF all'indirizzo http://www.redhat.com/support/manuals.

Ricerca della documentazione adatta

È sempre necessario reperire la documentazione adatta al proprio livello di conoscenza. La *Official Red Hat Linux Reference Guide* tratta gli aspetti e le opzioni più tecniche del sistema Red Hat Linux. In questa sezione vi aiuteremo a stabilire se questo manuale contiene le informazioni di cui avete bisogno oppure se consultare altri manuali Red Hat Linux o risorse online.

Gli utenti di Red Hat Linux possono essere suddivisi in tre gruppi, in base al loro livello di esperienza. Per ogni "categoria di appartenenza" è indicato il tipo di documentazione da consultare:

Nuovi utenti di Linux

Questi utenti non hanno mai utilizzato un sistema operativo Linux (o Linux-like) oppure lo conosce appena. Potrebbero saper usare altri sistemi operativi (per esempio Windows). Se è il vostro caso passate alla *Documentazione per i nuovi utenti di Linux*.

Utenti con qualche nozione di Linux

Questi utenti hanno già installato e utilizzato Linux in precedenza (ma non Red Hat Linux) oppure hanno un po' di esperienza con altri sistemi operativi simili a Linux. Vi riconoscete in questo tipo di utente? Allora consultate la *Documentazione per i più esperti*.

Utenti esperti di Linux

Questi utenti hanno installato e usato Red Hat Linux in precedenza. Se appartenete a questa categoria, leggete la *Documentazione per i guru di Linux*.

Documentazione per i nuovi utenti di Linux

Per chi non conosce Linux, la quantità di informazioni disponibili su qualsiasi argomento, come per esempio la stampa, l'avvio del sistema o il partizionamento del disco fisso, può sembrare enorme. All'inizio è opportuno raccogliere una base minima di informazioni sul funzionamento di Linux, prima di affrontare argomenti più complessi.

Innanzitutto dovete reperire un po' di documentazione utile. Infatti, senza la documentazione adatta non potrete far funzionare il vostro sistema Red Hat Linux nel modo desiderato.

Dovreste cercare i seguenti tipi di documentazione:

- *Breve storia di Linux* — molti aspetti di Linux sono legati alla sua storia. La cultura di Linux è basata su eventi, necessità e requisiti del passato. Una conoscenza basilare della storia di Linux può aiutarvi a capire come risolvere potenziali problemi, anche prima di incontrarli.
- *Funzionamento di Linux* — Anche se non è necessario investigare gli aspetti più arcani del kernel di Linux, può senz'altro essere utile capire come funziona il "cuore" del sistema. Ciò è particolarmente importante se avete sempre utilizzato altri sistemi operativi, infatti molte delle idee che vi siete fatti sul funzionamento dei computer potrebbero non essere applicabili a Linux.
- *Introduzione ai comandi (con esempi)* — si tratta forse della documentazione più importante per l'uso del sistema Linux. Linux si basa sulla filosofia secondo cui è meglio utilizzare tanti piccoli comandi collegati in diversi modi piuttosto che avere pochi comandi (complessi) che svolgono l'intero lavoro da soli. Senza esempi che illustrino questo approccio, l'elevato numero di comandi disponibili su Red Hat Linux potrebbe sicuramente intimidirvi.

  Ricordatevi che non occorre imparare a memoria tutti i comandi. Esistono diversi modi per facilitare la ricerca del comando specifico di cui avete bisogno per l'esecuzione di un task. È importante

conoscere solo il modo generale in cui Linux funziona, cioè il task che vi occorre eseguire e come accedere allo strumento che vi fornisce le istruzioni necessarie per eseguire il comando.

La *Official Red Hat Linux x86 Installation Guide* costituisce un valido riferimento per installare e configurare correttamente il sistema Red Hat Linux. La *Official Red Hat Linux Getting Started Guide* ripercorre la storia di Linux, dei comandi fondamentali di sistema, di GNOME, KDE, RPM e di molti altri concetti fondamentali. Iniziate con questi due libri e utilizzateli come base su cui costituire le vostre conoscenze.

Oltre ai manuali Red Hat Linux esistono molte altre fonti eccellenti dove trovare documentazione gratuite o poco costose:

Introduzione ai siti Web di Linux

- http://www.redhat.com — sul nostro sito Web è disponibile la documentazione LDP (Linux Documentation Project), le versioni online dei manuali Red Hat Linux, le FAQ (Frequently Asked Questions), un database per aiutarvi nella ricerca del gruppo di utenti Linux più vicino a voi, informazioni tecniche nel Support Knowledge Base di Red Hat.
- http://www.linuxheadquarters.com — il sito Web del "quartier generale" di Linux visualizza alcune guide che illustrano passo per passo i numerosi task di Linux.

Introduzione ai newsgroup di Linux

Potete entrare a far parte di un newsgroup leggendo gli interventi di altri, tentando di risolvere i problemi e ponendo delle domande. Gli esperti di Linux sono sempre disposti ad aiutare i nuovi utenti su varie problematiche di Linux. Per accedere al newsgroup, visitate il sito http://www.deja.com. Esistono comunque dozzine di newsgroup correlati a Linux, tra cui:

- linux.help — un ottimo posto dove ricevere aiuto dagli altri utenti di Linux.
- linux.redhat — questo newsgroup si occupa essenzialmente di tematiche legate a Red Hat Linux.
- linux.redhat.install — se avete domande sull'installazione, questo è il newsgroup a cui rivolgervi.
- linux.redhat.misc — per chi ha domande o richieste che non rientrano nelle categorie tradizionali.
- linux.redhat.rpm — per chi ha problemi con l'uso dell'RPM.

Libri su Linux per inesperti

- *Red Hat Linux for Dummies, 2nd Edition* di Jon "maddog" Hall, IDG
- *Special Edition Using Red Hat Linux* di Alan Simpson, John Ray e Neal Jamison, Que
- *Running Linux* di Matt Welsh e Lar Kaufman, O'Reilly & Associates
- *Red Hat Linux 7 Unleashed* di William Ball e David Pitts, Sams

I libri elencati sopra sono una fonte eccellente di informazione: trattano infatti i diversi argomenti discussi in questo manuale e molti capitoli elencano libri di riferimento specifici, soprattutto alla voce *Risorse aggiuntive*.

Documentazione per i più esperti

Se avete già utilizzato altre distribuzioni di Linux, probabilmente avete una conoscenza base dei comandi più utilizzati. Tuttavia, dopo l'installazione, potreste avere delle difficoltà con la configurazione.

La *Official Red Hat Linux Customization Guide* è stata ideata per illustrarvi i vari modi in cui il sistema Red Hat Linux può essere configurato per soddisfare le vostre esigenze personali. Usate questo manuale per apprendere tutte le opzioni di configurazione possibili e il modo in cui applicarle.

Se la *Official Red Hat Linux Customization Guide* non contiene le informazioni che cercate, consultate i documenti HOWTO (LDP), disponibili all'indirizzo http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html. In queste pagine sono contenute informazioni di tutti i tipi: a partire dal kernel di basso livello fino all'uso di Linux per stazioni radio amatoriali.

Documentazione per i guru di Linux

Se utilizzate Red Hat Linux da molto tempo, probabilmente saprete già che il modo migliore per capire un particolare programma è leggere il suo codice sorgente e/o i file di configurazione. Uno dei vantaggi di Red Hat Linux è proprio la facilità con cui è possibile leggere il suo codice sorgente.

Ovviamente non tutti sono programmatori in C, dunque il codice sorgente può non essere utile. Comunque se avete le conoscenze e le abilità necessarie per leggerlo, il codice sorgente contiene tutte le risposte alle vostre domande.

Convenzioni

Leggendo questo manuale, noterete che alcune parole sono stampate con font e dimensioni diversi. Si tratta di un modo sistematico per evidenziare parole particolari, ovviamente 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 per i nomi di file). In questi casi devono essere considerati parte integrante 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 particolare ha 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.

La directory `/usr/share/doc` contiene la documentazione sui vari programmi.

Installate il pacchetto RPM `webalizer` se desiderate 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 (contrariamente al software di sistema). Per esempio:

Utilizzate Netscape Navigator per navigare sul Web.

[tasto]

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

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

[tasti]-[combinazione]

Una combinazione di tasti viene rappresentata come nel seguente esempio:

La combinazione di tasti [Ctrl]-[Alt]-[Barra spaziatrice] fa riavviare il sistema X Window.

testo nell'interfaccia grafica utente (GUI)

Un titolo, una parola o una frase, contenuti in una schermata o in una finestra grafica, sono rappresentati con questo stile. (Parole o frasi associate a una casella di controllo oppure a un campo). Per esempio:

Sulla videata di GNOME **Control Center**, potete personalizzare il vostro window manager.

Selezionate la casella **Richiedi password**, se desiderate impostare una password per interrompere il salvaschermo.

livello superiore di un menu su una schermata o finestra GUI

Le parole con questo stile grafico rappresentano i livelli superiori di un menu a tendina. Infatti facendo clic su tali parole, compare il resto del menu. Per esempio:

Alla voce **Settings** nel terminale di GNOME, vedrete le seguenti opzioni di menu: **Preferenze**, **Reset terminale**, **Ripristina e cancella** e **Selettore colori**.

Una sequenza di comandi selezionata all'interno di un menu GUI viene rappresentata in questo modo:

Fate clic su **Programmi**=>**Applicazioni**=>**Emacs** per avviare l'editor di testi Emacs.

pulsanti su una schermata o finestra GUI

Questo stile grafico indica che, facendo clic su un pulsante della schermata grafica, viene visualizzato un testo. Per esempio:

Fate clic su **Indietro** per tornare alla pagina Web precedente.

`output del computer`

Le parole rappresentate con questo stile indicano il testo visualizzato dal computer sulla linea di comando. Vedrete le risposte ai comandi digitati, ai messaggi di errore e ai prompt interattivi. Per esempio:

Usate `ls` per visualizzare il contenuto di una directory:

```
$ ls
Desktop                 axhome            logs          nirvana.gif
Mail                    backupfiles       mail          reports
```

L'output ritornato in risposta al comando (in questo caso, il contenuto della directory) viene rappresentato con questo stile grafico.

`prompt`

Un prompt, ossia un modo del computer di segnalarvi che è pronto a ricevere un input, viene rappresentato con questo stile. Per esempio:

```
$
#
[truk@bleach truk]$
leopard login:
```

`input dell'utente`

Il testo che l'utente deve digitare o sulla linea di comando o in una casella di testo, su una schermata grafica viene rappresentato con questo stile. Per esempio:

Per avviare il vostro sistema con un programma di installazione dovete digitare il comando **`text`** al prompt `boot:`.

Ecco un altro esempio, con la parola **`root`** rappresentata come input che va digitato dall'utente:

Se dovete collegarvi come root la prima volta che accedete al sistema e state utilizzando una schermata di login grafica, digitate **`root`** al prompt `Login`. Al prompt `Password` inserite la password di root.

voce del glossario

Una parola contenuta nel glossario viene rappresentata con questo stile grafico. Per esempio:

Il **demone** lpd gestisce le richieste di stampa.

In questo caso, lo stile della parola **demone** indica che nel glossario è disponibile la versione di questo termine.

Inoltre troverete diversi simboli utilizzati per attirare la vostra attenzione su informazioni di particolare rilievo, precedute, a seconda dell'importanza, dalle parole "Nota Bene", "Attenzione", "Avvertimento". Per esempio:

Nota Bene

Ricordate che in Linux le maiuscole e le minuscole sono considerate in modo diverso. In altre parole rosa non è uguale a ROSA o a rOsA.

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

Se decidete di effettuare il partizionamento automatico, l'installazione di classe Server rimuove tutte le partizioni esistenti su tutti i dischi fissi installati.

Uso del mouse

Red Hat Linux è stato ideato per un mouse a tre tasti. Se invece il vostro mouse ne ha solo uno, potete selezionare l'emulazione dei tre pulsanti durante il processo di installazione. In questo modo, premendo contemporaneamente i due tasti, potete simulare il terzo tasto mancante (quello centrale).

In questa guida, quando viene indicato di fare clic con il mouse su qualche oggetto, significa che dovete premere il tasto sinistro. Nel caso in cui è necessario usare il tasto destro o centrale, vi verrà richiesto in modo esplicito. (Naturalmente vale l'opposto se avete configurato il mouse per essere usato da una persona mancina).

L'espressione "trascina e lascia" potrebbe suonarvi familiare. Se vi viene indicato di trascinare un oggetto e lasciarlo sul desktop grafico, fate clic su questo oggetto e tenete premuto il tasto sinistro del mouse. Trascinate l'oggetto muovendo il mouse nella nuova posizione e lasciate "cadere" l'oggetto.

Copia e incolla in X

Copiare e incollare dei testi in X è davvero semplice se usate il mouse. Per copiare, fate clic con il mouse sul testo da selezionare. Per incollare, fate clic con il pulsante centrale nel punto in cui volete posizionare il testo.

Prossimamente

La *Official Red Hat Linux Reference Guide* fa parte dell'impegno di Red Hat nel fornire un supporto utile e immediato agli utenti di Red Hat Linux. Le prossime edizioni conterranno informazioni più dettagliate inerenti l'amministrazione del sistema, i tool e altre risorse per aiutarvi ad ampliare le potenzialità del vostro sistema Red Hat Linux e la vostra competenza nell'usarlo.

Ovviamente potete contribuire anche voi!

Inviateci suggerimenti!

Se individuate delle imprecisioni nella *Official Red Hat Linux Reference Guide* o se pensate di poter contribuire al miglioramento di questo manuale, inviate i vostri suggerimenti al seguente indirizzo: http://bugzilla.redhat.com/bugzilla.

Assicuratevi di menzionare l'identificatore del manuale:

```
rhl-rg(IT)-7.1-Print-RHI (2001-02-21T10:50-0500)
```

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.

Ricordatevi di registrarvi

Se avete acquistato il prodotto ufficiale Red Hat Linux 7.1, ricordatevi di registrarvi per sfruttare i vantaggi a cui avete diritto come clienti Red Hat.

Vi offriamo diversi vantaggi in base al tipo di prodotto Red Hat Linux che avete acquistato:

- Assistenza ufficiale di Red Hat — il nostro team di assistenza Red Hat, Inc. è a vostra disposizione per risolvere i problemi che potreste incontrare durante l'installazione.
- Red Hat Network — collegandovi al sito http://www.redhat.com/network potete aggiornare i vostri pacchetti e ricevere avvisi di sicurezza specifici per il vostro sistema.
- Accesso FTP privilegiato — niente più notti insonni trascorse a scaricare il vostro software preferito. I possessori di Red Hat Linux 7.1 hanno accesso gratuito a redhat.com, il servizio FTP per i clienti di Red Hat che offre giorno e notte un servizio a banda larga.
- *Under the Brim:* la E-Newsletter ufficiale di Red Hat — ogni mese riceverete direttamente da Red Hat le ultime novità e informazioni sui prodotti.

Per registrarvi collegatevi all'indirizzo http://www.redhat.com/apps/activate/. L' **ID prodotto** è riportato sulla scheda rossa e bianca contenuta nella vostra confezione di Red Hat Linux.

Per maggiori informazioni sull'assistenza tecnica di Red Hat Linux, consultate l'appendice *Ricevere assistenza tecnica* nella *Official Red Hat Linux x86 Installation Guide*.

Buona fortuna e grazie per aver scelto Red Hat Linux!!

Il team della documentazione di Red Hat

Parte I Il sistema

1 Struttura del filesystem

1.1 Perché condividere una struttura comune?

La struttura a filesystem di un sistema operativo è il suo livello più elementare di organizzazione. Quasi tutti i modi in cui un sistema operativo interagisce con gli utenti, le applicazioni e i modelli di sicurezza dipendono dal modo in cui il sistema memorizza i suoi file su un dispositivo di memorizzazione primario (solitamente un disco fisso). Per svariate ragioni è importante che gli utenti, così come i programmi al momento dell'installazione e dopo, possano fare riferimento a una linea guida comune per sapere dove leggere e scrivere i file binari, di configurazione, di log, ecc.

Un filesystem può essere visto come comprendente due diverse categorie logiche di file:

- I file condivisibili e i file non condivisibili
- I file variabili e i file statici

I file **condivisibili** sono file a cui vari host possono accedere, mentre i file **non condivisibili** non sono disponibili per altri host. I file **variabili** possono cambiare in qualsiasi momento senza l'intervento (passivo o attivo) dell'amministratore del sistema, i file **statici**, come i file di documentazione o i file binari, non cambiano senza un'azione dell'amministratore del sistema.

La ragione che ci porta a classificare i file in questo modo ha a che fare con il tipo di autorizzazione dato alla directory che contiene i file. Il modo in cui il sistema operativo e i suoi utenti utilizzano i file determina la directory dove questi verranno inseriti, indipendentemente dal fatto che la directory sia montata in modalità di sola lettura o di lettura e scrittura e indipendentemente dal livello di accesso autorizzato a ogni file. Il livello massimo di questa organizzazione è fondamentale, poiché l'accesso alle directory sottostanti può essere limitato o possono insorgere problemi di sicurezza, se il livello massimo è disorganizzato o privo di struttura.

Tuttavia, il fatto di avere una struttura non significa molto a meno che non sia standard. La creazione di strutture rivali rischia di causare problemi anziché risolverli. Per questo motivo, Red Hat ha scelto la struttura di filesystem più comune estendendola leggermente per adattarla a file speciali utilizzati all'interno di Red Hat Linux.

1.2 Panoramica sull'FHS

Red Hat è fedele al **Filesystem Hierarchy Standard** (**FHS**), documento che definisce i nomi e la posizione di molti file e directory. Continueremo a seguire lo standard perché Red Hat Linux sia conforme all'FHS.

L'FHS corrente è il documento di riferimento per qualsiasi filesystem conforme all'FHS, ma lo standard lascia molte zone indefinite ed estensibili. In questa sezione viene fornita una panoramica sullo standard e una descrizione delle parti del filsystem non coperte dallo standard.

Lo standard completo è disponibile all'indirizzo:

http://www.pathname.com/fhs

La conformità con lo standard è molto importante, ma i due fattori fondamentali sono la compatibilità con altri sistemi conformi e la capacità di montare la partizione `/usr` come partizione in sola lettura (perché contiene file eseguibili comuni e non va modificata dagli utenti). `/usr` può essere montato dal CD-ROM o da un'altra macchina tramite NFS in sola lettura.

1.2.1 Organizzazione dell'FHS

Le directory e i file qui menzionati rappresentano un piccolo sotto-insieme di quelli specificati dal documento FHS. Per informazioni più dettagliate, consultate l'ultimo documento dell'FHS.

La directory `/dev`

La directory `/dev` contiene voci del filesystem che rappresentano dispositivi collegati al sistema. Questi file sono essenziali perché il sistema funzioni correttamente.

La directory `/etc`

La directory `/etc` è riservata ai file locali del vostro computer. Nessun file binario deve essere inserito in `/etc`. Tutti i file binari che sono stati precedentemente inseriti in `/etc` devono essere trasferiti in `/sbin` o possibilmente in `/bin`.

Le directory `X11` e `skel` devono essere sotto-directory di `/etc`:

```
/etc
  |- X11
  |- skel
```

La directory `X11` contiene i file di configurazione di X11, come per esempio `XF86Config`. La directory `skel` contiene i file di base per gli utenti, cioè i file che vengono copiati automaticamente nelle directory home quando viene creato un nuovo utente.

La directory `/lib`

La directory `/lib` contiene solo le librerie necessarie all'esecuzione dei programmi presenti in `/bin` e `/sbin`. Queste immagini di libreria condivise sono particolarmente importanti per l'avvio del sistema e l'esecuzione di comandi all'interno del filesystem di root.

La directory `/mnt`

La directory `/mnt` si riferisce ai filesystem montati temporaneamente, come i CD-ROM e i dischetti floppy.

La directory `/opt`

La directory `/opt` fornisce un'area per la memorizzazione di pacchetti applicativi statici e di grandi dimensioni.

Per i pacchetti che vogliono evitare di posizionare i file attraverso il filesystem, `/opt` fornisce un sistema organizzativo logico e prevedibile sotto la directory del pacchetto. In questo modo l'amministratore del sistema può facilmente determinare il ruolo di ogni file all'interno di un pacchetto particolare.

Per esempio, se `sample` è il nome di un pacchetto particolare all'interno di `/opt`, allora tutti i suoi file dovrebbero essere inseriti in `/opt/sample`. Per esempio `/opt/sample/bin` per i binari e `/opt/sample/man` per le pagine man.

Anche i pacchetti che comprendono più sotto-pacchetti, ognuno con un compito particolare, vanno inseriti in `/opt`, avranno così un modo standardizzato di organizzarsi. Per esempio, il pacchetto `sample` può avere diversi tool appartenenti ognuno alla propria sotto-directory come `/opt/sample/tool1` e `/opt/sample/tool2`, ognuno di questi può avere il proprio `bin`, `man` e altre directory simili.

La directory `/sbin`

La directory `/sbin` contiene gli eseguibili utilizzati solo dall'utente root, tra cui quelli necessari per avviare, montare e ripristinare il filesystem. L'FHS dice:

> "`/sbin` contiene normalmente i file essenziali per l'avvio del calcolatore oltre a quelli presenti in /bin. Qualunque altro eseguibile di sistema utilizzato dopo il mount della `/usr` (quando non si sono verificati problemi) deve essere collocato in `/usr/sbin`. I comandi per l'amministrazione locale del sistema devono essere inseriti in `/usr/local/sbin`."

In `/sbin` potete trovare i seguenti programmi:

```
arp, clock, getty, halt, init, fdisk,
fsck.*, ifconfig, lilo, mkfs.*, mkswap, reboot,
route, shutdown, swapoff, swapon, update
```

La directory /usr

La directory /usr contiene tutti i file condivisi nello stesso calcolatore. La directory /usr ha solitamente una partizione dedicata e dovrebbe essere montata in sola lettura. Di seguito viene mostrata la struttura della partizione /usr:

```
/usr
  |- bin
  |- doc
  |- etc
  |- games
  |- include
  |- kerberos
  |- lib
  |- libexec
  |- local
  |- man
  |- sbin
  |- share
  |- src
  |- X11R6
```

La directory bin contiene gli eseguibili, doc contiene le pagine di documentazione non conformi a FHS, etc contiene i file di configurazione del sistema, games quelli per i giochi, include contiene i file header di C, kerberos contiene i binari e molte altre cose per Kerberos e lib contiene file oggetti e librerie che non sono stati concepiti per essere usati direttamente dagli utenti o dagli script della shell. La directory libexec contiene piccoli programmi di help richiamati da altri programmi, sbin è per i binari di amministrazione del sistema (quelli che non appartengono a /sbin), share contiene i file non specifici per l'architettura, src contiene i codici sorgenti e X11R6 serve per il sistema X Window (XFree86 in Red Hat Linux).

La directory /usr/local

L'FHS dice:

> "La directory /usr/local viene utilizzata dall'aministratore di sistema quando installa il software a livello locale. Prima che il software sia aggiornato deve essere effettuato un back up di questa directory. Può essere usato per i programmi e i dati che sono condivisibili con altri gruppi di host, ma che non si trovano in /usr."

La directory /usr/local ha una struttura simile alla directory /usr. Contiene le sottodirectory seguenti, che hanno uno scopo simile a quelle contenute nella directory /usr:

```
/usr/local
       |- bin
```

```
      |- doc
      |- etc
      |- games
      |- info
      |- lib
      |- man
      |- sbin
      |- src
```

La directory `/var`

Da quando FHS permette al sistema di montare `/usr` in sola lettura, è necessario che i file di sistema delle directory di `spool` e quelle di `lock` siano memorizzati in `/var`. L'FHS in riferimento a `/var` dice:

> "…file di dati variabili. Questa directory contiene i file di spool, di amministrazione, di log e i file temporanei."

Le seguenti directory sono tutte sottodirectory di `/var`:

```
/var
  |- arpwatrch
  |- cache
  |- db
  |- ftp
  |- gdm
  |- kerberos
  |- lib
  |- local
  |- lock
  |- log
  |- named
  |- nis
  |- opt
  |- preserve
  |- run
  +- spool
       |- anacron
       |- at
       |- cron
       |- fax
       |- lpd
       |- mail
       |- mqueue
       |- news
       |- rwho
```

```
        |- samba
        |- slrnpull
        |- squid
        |- up2date
        |- uucp
        |- uucppublic
        |- vbox
        |- voice
    |- tmp
    |- www
    |- yp
```

I file di log del sistema, come `messages` e `lastlog` si trovano nella directory `/var/log`. La directory `/var/lib` contiene i database del sistema RPM. I file lock si trovano in `/var/lock`, solitamente in directory particolari per il programma che usa il file. La directory `/var/spool` ha delle sottodirectory per vari sistemi che devono memorizzare file di dati.

1.2.2 `/usr/local` in Red Hat Linux

Nei sistemi Red Hat Linux, l'uso della directory `/usr/local` è leggermente diverso da quello specificato dall'FHS. L'FHS dice che in `/usr/local` va memorizzato il software non interessato agli aggiornamenti del sistema. Poiché gli aggiornamenti di Red Hat vengono effettuati con il sistema RPM e Gnome-RPM, non dovete proteggere i file mettendoli in`/usr/local`. Invece, vi raccomandiamo di usare `/usr/local` per il software locale del vostro computer.

Per esempio, supponiamo di montare `/usr` via NFS in sola lettura da un host chiamato `jake`. Se desiderate installare un pacchetto o un programma, ma non è permesso scrivere su `jake`, potrete comunque installarlo sotto `/usr/local`. Nel paragrafo seguente dovrete cercare di convincere l'amministratore di sistema di `jake` a installare il programma su `/usr`, voi potrete disinstallarlo da `/usr/local`.

1.3 `/proc` e i suoi "file"

La directory `/proc` contiene particolari file che estraggono o inviano informazioni al kernel.

Tuttavia, la directory `/proc` è molto più potente di quanto non crediate. Attraverso i vari file di questa directory (che non sono file ma interfacce nel kernel), un amministratore del sistema può usare `/proc` come metodo per accedere a informazioni sullo stato del kernel, gli attributi della macchine, gli stati dei singoli processi ecc. Usando `cat` in combinazione con le interfacce in `/proc`, potete accedere immediatamente a un'enorme quantità di informazioni su qualsiasi sistema. Per esempio se volete vedere come i registri della memoria sono attualmente assegnati sul vostro computer:

```
[truk@tictactoe /proc]$ cat iomem
00000000-0009fbff : System RAM
```

```
0009fc00-0009ffff : reserved
000a0000-000bffff : Video RAM area
000c0000-000c7fff : Video ROM
000f0000-000fffff : System ROM
00100000-07ffffff : System RAM
  00100000-002553d7 : Kernel code
  002553d8-0026d91b : Kernel data
e0000000-e3ffffff : VIA Technologies, Inc. VT82C597 [Apollo VP3]
e4000000-e7ffffff : PCI Bus #01
  e4000000-e4003fff : Matrox Graphics, Inc. MGA G200 AGP
  e5000000-e57fffff : Matrox Graphics, Inc. MGA G200 AGP
e8000000-e8ffffff : PCI Bus #01
  e8000000-e8ffffff : Matrox Graphics, Inc. MGA G200 AGP
ea000000-ea00007f : Digital Equipment Corporation DECchip 21140
  ea000000-ea00007f : eth0
ffff0000-ffffffff : reserved
[truk@tictactoe /proc]$
```

Oppure (cosa ancora più utile), se vi collegate a una macchina sconosciuta e volete sapere il tipo e la velocità del processore, potete usare il comando seguente:

```
cat /proc/cpuinfo
```

Altre informazioni sul sistema sono contenute in `cmdline`, `meminfo`, `partitions`, `version` ecc.

Le directory in `/proc` rappresentano un insieme di informazioni su un'applicazione o un processo particolare. Per esempio, la directory `/proc/sys/kernel` è ricca di informazioni sul kernel. È indicato, per esempio, il numero massimo di thread (`threads-max`) e di messaggi (`msgmax`).

1.4 Directory speciali di Red Hat

Oltre ai file RPM che risiedono nella directory `/var/lib/rpm` (vedere il capitolo sugli RPM nella *Official Red Hat Linux Customization Guide* per maggiori informazioni sugli RPM), esistono altri due luoghi speciali riservati alla configurazione e al funzionamento di Red Hat Linux.

I tool di configurazione forniti con Red Hat Linux installano molti script, bitmap e file di testo in `/usr/lib/rhs`. Poiché questi file sono generati dal software sul vostro sistema, non è consigliabile modificarli a mano.

Nell'altro luogo "speciale" (`/etc/sysconfig`) sono conservate le informazioni sulla configurazione. Molti script eseguiti durante l'avvio usano i file di questa directory. Tali file possono essere modificati a mano, ma possono essere configurati anche usando Linuxconf, un tool del pannello di controllo o un altro tool di configurazione. Per informazioni sull'utilizzo di Linuxconf, consultate la *Official Red Hat Linux Customization Guide*.

2 Utenti e gruppi

Il controllo degli **utenti** e dei **gruppi** è alla base dell'amministrazione del sistema Red Hat Linux.

Gli **utenti** possono essere o le persone vere e proprie (account riuniti in un utente fisico specifico) oppure utenti logici (account esistenti per le applicazioni in modo che possano svolgere azioni particolari). Entrambi i tipi di utenti, veri o logici, possiedono un **ID utente** e un **ID Gruppo**. Solitamente gli ID utente sono univoci (ma non è obbligatorio).

I **gruppi** sono sempre espressioni logiche dell'organizzazione. Gli utenti possono formare dei gruppi che a loro volta creano le fondamenta per riunire gli utenti e concedere loro i permessi per leggere, scrivere oppure eseguire un determinato file.

A qualsiasi file creato viene assegnato un utente e un gruppo, inoltre vengono assegnati permessi di lettura, scrittura ed esecuzione per il proprietario del file, per il gruppo assegnato e per ogni altro utente su quell'host. L'utente e il gruppo di un particolare file e i permessi relativi al file stesso possono essere modificati dall'utente root o, in misura minore, dall'autore del file.

Uno dei compiti più importati dell'amministratore del sistema è la corretta gestione degli utenti e dei gruppi e quindi l'assegnazione e la revoca dei permessi. Per fortuna Red Hat Linux rende questo lavoro il più semplice possibile pur garantendo la sicurezza dei file sull'host.

2.1 Tool per l'amministrazione di utenti e gruppi

La gestione degli utenti e dei gruppi è sempre stata piuttosto noiosa, ma Red Hat Linux fornisce qualche strumento e convenzione per rendere tutto ciò più semplice.

Pur potendo usare `useradd` per creare un nuovo utente dal prompt della shell, un modo più diffuso per gestire gli utenti e i gruppi è tramite Linuxconf (per maggiori dettagli, consultate la *Official Red Hat Linux Customization Guide*).

2.2 Utenti standard

La Tabella 2–1, *Utenti standard* elenca gli utenti standard creati dal processo di installazione (si tratta essenzialmente del file `/etc/passwd`). In questa tabella l'ID del gruppo (GID) rappresenta il *gruppo primario* dell'utente. Per informazioni più dettagliate sulla gestione dei gruppi, consultate la Sezione 2.4, *Gruppi privati utente*.

Tabella 2–1 Utenti standard

Utente	UID	GID	Directory home	Shell
root	0	0	`/root`	`/bin/bash`
bin	1	1	`/bin`	
daemon	2	2	`/sbin`	
adm	3	4	`/var/adm`	
lp	4	7	`/var/spool/lpd`	
sync	5	0	`/sbin`	`/bin/sync`
shutdown	6	0	`/sbin`	`/sbin/shutdown`
halt	7	0	`/sbin`	`/sbin/halt`
mail	8	12	`/var/spool/mail`	
news	9	13	`/var/spool/news`	
uucp	10	14	`/var/spool/uucp`	
operator	11	0	`/root`	
games	12	100	`/usr/games`	
gopher	13	30	`/usr/lib/gopher-data`	
ftp	14	50	`/var/ftp`	
nobody	99	99	`/`	

2.3 Gruppi standard

Nella Tabella 2–2, *Gruppi standard*, troverete i gruppi standard come configurati dal processo di installazione (si tratta essenzialmente del file `/etc/group`).

Tabella 2–2 Gruppi standard

Gruppo	GID	Membri
root	0	root
bin	1	root, bin, daemon

Gruppo	GID	Membri
daemon	2	root, bin, daemon
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	
disk	6	root
lp	7	daemon, lp
mem	8	
kmem	9	
wheel	10	root
mail	12	mail
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	
nobody	99	
users	100	

2.4 Gruppi privati utente

Red Hat Linux utilizza uno schema di **gruppo privato utente** (**UPG**), che rende i gruppi di UNIX più semplici da amministrare. Lo schema UPG non aggiunge o modifica nulla nella gestione standard dei gruppi di UNIX. Offre semplicemente una nuova convenzione. Ogni utente nuovo appartiene, per default, a un gruppo unico. Lo schema funziona nel seguente modo:

gruppo privato utente

Ogni utente ha un gruppo primario, del quale è l'unico membro.

umask = 002

Normalmente nei sistemi UNIX la umask è 022 e impedisce agli altri utenti e agli *altri membri di un gruppo primario di utenti* di modificare i file. Poiché ogni utente ha il proprio gruppo privato nello schema, non è necessaria la "protezione dei gruppi". Una umask 002 impedisce agli utenti di modificare i file personali di altri utenti. La umask è impostata in `/etc/profile`.

setgid bit nelle directory

Se impostate il setgid bit in una directory (con il comando `chmod g+s`*`directory`*), il gruppo dei file creati nella directory viene configurato come il gruppo della directory.

Molte organizzazioni IT hanno la consuetudine di creare un gruppo per ogni progetto principale e poi assegnare alle persone il gruppo in cui essi stanno lavorando. L'uso di questo schema tradizionale di gestione dei file si è rivelato piuttosto complesso, perché quando un utente crea un file, questo viene associato al gruppo primario a cui l'utente appartiene. Quando una sola persona lavora su molti progetti, è difficile associare i file esatti al gruppo giusto. Invece, con l'uso dello schema UPG, i gruppi sono assegnati automaticamente ai file creati all'interno di quella directory, che rende molto più semplice la gestione dei progetti di gruppo che condividono una directory comune.

Per esempio, supponiamo di avere in corso un grande progetto chiamato *devel*, con utenti che modificano i file *devel* in una directory `devel`. Create un gruppo chiamato `devel`, aggiungete la directory `devel` (`chgrp`) e tutti gli utenti del progetto al gruppo `devel`.

È possibile aggiungere un utente a un gruppo utilizzando Linuxconf (vedere la *Official Red Hat Linux Customization Guide*). Se preferite utilizzare la linea di comando, digitate il comando `/usr/sbin/groupadd` *`nome del gruppo`* per creare un gruppo. Poi, con il comando `/usr/bin/gpasswd -a` *`nome di login nome del gruppo`* aggiungete al gruppo *nome di login* dell'utente. (Per maggiori informazioni sulle diverse opzioni, consultate le pagine man dei comandi `groupadd` e `gpasswd`). Il file `/etc/group` contiene le informazioni sui gruppi per il vostro sistema.

Se avete creato il gruppo `devel`, aggiunto utenti e cambiato il gruppo per la directory `devel` nel gruppo `devel` e se avete impostato il setgid bit per la directory `devel`, tutti gli utenti *devel* potranno modificare i file *devel* e creare nuovi file nella directory `devel`. I file creati manterranno sempre il proprio stato di gruppo `devel`, così altri utenti *devel* saranno sempre in grado di modificarli.

Se avete in corso numerosi progetti come *devel* e altrettanti utenti che vi lavorano, tali utenti non dovranno mai modificare la propria umask o il gruppo nel muoversi da un progetto all'altro. Se impostato correttamente, il setgid bit "seleziona" sulle directory principali di ogni progetto il gruppo corretto per i file creati in quella directory.

Poiché la directory home di ogni utente appartiene all'utente e al suo gruppo privato, è più sicuro impostare il setgid bit sulla directory home. Comunque i file vengono creati per default con il gruppo primario dell'utente, in questo modo il setgid bit risulta ridondante.

2.4.1 Logica dei gruppi privati utente

Sebbene l'UPG non sia nuovo in Red Hat Linux, ancora molte persone hanno dei dubbi e si chiedono per esempio perché l'UPG sia necessario. Cercheremo di fornire maggiori dettagli con un esempio:

- Intendete far lavorare un gruppo di persone su una serie di file nella directory `/usr/lib/emacs/site-lisp`. Volete però che solo alcune di queste persone abbiano la facoltà di modificare la directory.
- Create innanzitutto un gruppo `emacs`:

  ```
  /usr/sbin/groupadd emacs
  ```

  Poi digitate:

  ```
  chown -R root.emacs /usr/lib/emacs/site-lisp
  ```

  Per associare il contenuto della directory al gruppo `emacs`, aggiungete l'utente adatto al gruppo:

  ```
  /usr/bin/gpasswd -a <nome utente> emacs
  ```

- Per autorizzare gli utenti a creare i file nella directory, digitate:

  ```
  chmod 775 /usr/lib/emacs/site-lisp
  ```

- Tuttavia, quando un utente crea un nuovo file, questo viene assegnato al gruppo di default dell'utente (di solito `users`). Per impedire che ciò avvenga, digitate:

  ```
  chmod 2775 /usr/lib/emacs/site-lisp
  ```

  In questo modo, tutti i file creati nella directory verranno assegnati al gruppo `emacs`.

- Tuttavia, per permettere a un altro utente nel gruppo `emacs` di modificare un nuovo file, è necessario che questo sia creato con la modalità 664. Per farlo, usate 002 come umask di default.
- Non bisogna dimenticare però che se il vostro gruppo di default è `users`, ogni file creato nella propria directory home sarà modificabile da chiunque nel gruppo `users` (di solito tutti).
- Per porre rimedio a questo problema, attribuite a ogni utente un "gruppo privato" come gruppo di default.

A questo punto, dopo aver impostato umask 002 come default e aver attribuito a ognuno un gruppo privato di default, è possibile impostare in modo molto semplice i gruppi a cui gli utenti potranno accedere, senza dover lavorare ulteriormente ogni qualvolta vengano creati o modificati dei file contenuti

nella directory comune al gruppo. Create solo il gruppo, aggiungete gli utenti ed eseguite i comandi `chown` e `chmod` per le directory del gruppo.

3 Processo di avvio, init e spegnimento

Questo capitolo contiene informazioni relative a ciò che accade all'avvio o allo spegnimento del sistema Red Hat Linux.

3.1 Introduzione

Uno degli aspetti che rendono Red Hat Linux un sistema potente è il metodo di avviare e arrestare il sistema operativo: nel caricare i programmi specifici usando le loro configurazioni particolari, vi permette di modificare quelle configurazioni preposte al controllo del processo di avvio e di arrestare il sistema in modo "aggraziato" e organizzato. Mentre gli altri sistemi operativi cercano di controllare il modo in cui il computer esegue l'avvio o di impedirvi di personalizzare il processo di spegnimento, Red Hat Linux consente pieno accesso a ogni fase di questo processo.

Oltre al fatto di controllare il processo di avvio o di spegnimento, la "natura aperta" di Red Hat Linux vi aiuta a determinare la fonte esatta della maggior parte dei problemi legati all'avvio o allo spegnimento del sistema. Capire questo processo è senz'altro utile per la risoluzione dei problemi di base.

3.2 I retroscena del processo di avvio

Nota Bene

Questa sezione si dedica in particolare al processo di avvio con processore x86, che può variare leggermente a seconda dell'architettura del vostro sistema. Comunque, quando il kernel viene rilevato e caricato dal sistema, il processo di avvio di default è identico per tutte le architetture. Per maggiori informazioni su un processo di avvio diverso da x86, consultate la Sezione 3.8, *Differenze nel processo di avvio di altre architetture*.

Quando un computer viene avviato, il processore controlla alla fine il **BIOS** (Basic Input/Output System) alla fine della memoria di sistema e lo avvia. Il programma BIOS è scritto in una memoria permanente in sola lettura e può sempre essere utilizzato. Il BIOS fornisce l'interfaccia per le periferiche e controlla la prima fase del processo di avvio.

Il BIOS testa il sistema, cerca e controlla le periferiche e poi cerca un'unità da utilizzare per avviare il sistema. Di solito controlla nell'unità floppy (o CD-ROM, nei sistemi più recenti) se vi sono supporti avviabili e poi controlla il disco fisso. Nella maggior parte dei casi,la sequenza delle unità utilizzate per l'avvio è controllata da una particolare configurazione del BIOS. Quando Red Hat Linux viene installato sul disco fisso di un sistema il BIOS cerca un **Master Boot Record** (MBR) nel primo settore del primo disco fisso, ne carica il contenuto in memoria e gli passa il controllo del processo.

Il codice di questo MBR cerca la prima partizione attiva e poi ne legge il record di avvio contenente le istruzioni su come caricare il loader di avvio **LILO** (*LI*nux *LO*ader). L'MBR carica poi LILO, che assume il controllo del processo (se LILO è installato sull'MBR). Nella configurazione di default di Red Hat Linux, LILO utilizza le impostazioni nell'MBR per visualizzare le opzioni di avvio e autorizzare l'input utente con cui il sistema operativo si avvia.

Probabilmente vi starete domandando come fa LILO a sapere cosa fare una volta letto l'MBR. LILO in realtà ha già letto le istruzioni usando `lilo` con il file di configurazione `/etc/lilo.conf`.

3.2.1 Opzioni nel file `/etc/lilo.conf`

In genere non occorre cambiare il Master Boot Record sul disco fisso, a meno che non dobbiate avviare un sistema operativo appena installato oppure stiate cercando di utilizzare un nuovo kernel. Se dovete creare un nuovo MBR utilizzando LILO, ma con una configurazione diversa, è necesssario modificare `/etc/lilo.conf` e rieseguire `lilo`.

AVVERTIMENTO

Se intendete modificare `/etc/lilo.conf`, assicuratevi di effettuare una copia di backup del file prima di eseguire qualsiasi modifica. Inoltre controllate di avere un dischetto di avvio funzionante, in modo da poter avviare il sistema ed effettuare le modifiche all'MBR se si verificano dei problemi. Per maggiori informazioni su come creare un dischetto di avvio, consultate le pagine man relative a `mkbootdisk`.

Il file `/etc/lilo.conf` viene utilizzato da `lilo` per stabilire quale sistema operativo utilizzare o quale kernel avviare e dove installare se stesso (per esempio `/dev/hda` per il primo dispositivo IDE). Ecco un esempio del file `/etc/lilo.conf`:

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=50
message=/boot/message
lba32
default=linux

image=/boot/vmlinuz-2.4.0-0.43.6
 label=linux
 initrd=/boot/initrd-2.4.0-0.43.6.img
```

```
    read-only
    root=/dev/hda5

  other=/dev/hda1
    label=dos
```

Questo esempio mostra un sistema configurato per avviare due sistemi operativi: Red Hat Linux e DOS. Qui di seguito sono visualizzate più in dettaglio alcune delle righe di questo file (il vostro `/etc/lilo.conf` potrebbe essere leggermente diverso):

- `boot=/dev/hda` chiede a LILO di cercare il primo controller IDE sul primo disco fisso.
- `map=/boot/map` individua il file map. Si consiglia di non modificare questo file.
- `install=/boot/boot.b` indica a LILO di installare il file specificato come nuovo settore di avvio. Si consiglia di non modificarlo. Se manca la riga `install`, LILO considera il default di `/boot/boot.b` come file da utilizzare.
- `prompt` indica a LILO di visualizzare quanto evidenziato nella riga `message`. Si sconsiglia di rimuovere la riga `prompt`. Se lo fate, potete comunque ottenere un prompt tenendo premuto il tasto [Shift] mentre l'elaboratore comincia ad avviarsi.
- `timeout=50` imposta quanto tempo LILO deve attendere l'input utente prima di avviare la riga entry di `default`. La quantità di tempo è calcolata in decimi di secondo e il default è 50.
- `message=/boot/message` rimanda alla schermata visualizzata da LILO per permettervi di selezionare il sistema operativo o il kernel da avviare.
- `lba32` descrive la geometria del disco fisso a LILO. Un'altra entry standard è `linear`. Si consiglia di non modificare questa riga, per evitare che il sistema non riesca più a effettuare l'avvio.
- `default=linux` indica a LILO quale sistema operativo avviare tra le opzioni indicate sotto questa riga. In questo caso nella riga `label` (disponibile per ogni opzione di avvio) si trova il nome `linux`.
- `image=/boot/vmlinuz-2.4.0-0.43.6` specifica al kernel linux di avviarsi con questa particolare opzione di avvio.
- `label=linux` indica il nome dei sistemi operativi visualizzati nella videata di LILO. In questo caso rappresenta anche il nome specificato nella riga `default`.
- `initrd=/boot/initrd-2.4.0-0.43.6.img` indica l'immagine del **disco ram iniziale** utilizzata all'avvio per inizializzare i dispositivi che rendono possibile l'avvio del kernel. Il disco ram iniziale è costituito da una serie di driver necessari per mettere in funzione il disco fisso e tutti i dispositivi che servono per caricare il kernel. Non tentate di condividere i dischi di ram iniziale tra vari calcolatori, a meno che non abbiano una configurazione hardware identica (e comunque egrave; meglio evitarlo).

- `read-only` attiva la modalità di sola lettura per la partizione di root, impedendo tutte le modifiche (vedere la riga `root` che segue).
- `root=/dev/hda5` indica a LILO quale partizione del disco utilizzare come partizione root.

Successivamente LILO mostra la videata iniziale Red Hat Linux con i diversi sistemi operativi instalati o i kernel che deve avviare. Se Red Hat Linux è il vostro unico sistema operativo e non avete modificato nulla in `/etc/lilo.conf`, vedrete come unica opzione linux. Se avete configurato LILO per avviare altri sistemi operativi, in questa videata potete selezionare quale sistema operativo eseguire. Utilizzate i tasti freccia per evidenziare il sistema da avviare e poi premete [Invio]

Se desiderate un prompt dove inserire i comandi per LILO, premete [Ctrl]-[X]. In questo modo LILO visualizza il prompt `LILO:` sullo schermo e attende un input dell'utende per un periodo di tempo prestabilito. (Questa quantità di tempo viene impostata dalla riga `timeout` nel file `/etc/lilo.conf`). Se il file di configurazione `/etc/lilo.conf` è impostato per far caricare a LILO diversi sistemi operativi, è ora necessario inserire il nome del sistema operativo che si desidera avviare.

Se LILO sta avviando Linux, carica innanzitutto in memoria il kernel con il file `vmlinuz` (più un numero di versione, per esempio: `vmlinuz-2.4.0-xx`) che si trova nella directory `/boot`. Il kernel passa poi il controllo a `init`.

Quando viene caricato il kernel, Linux è già operativo, ma solo a un livello base. Comunque senza applicazioni e senza la possibilità di fornire un input al sistema, non si può fare molto. Il programma `init` risolve questo problema, attivando i vari servizi che consentono al sistema di svolgere il proprio ruolo.

3.2.2 Init

Il kernel individua `init` nella directory `/sbin` e lo esegue. `init` poi coordina la fase restante del processo di avvio.

Quando `init` viene eseguito, diventa il padre di tutti i processi che si avviano automaticamente sul sistema Red Hat Linux. Innanzitutto esegue lo script `/etc/rc.d/rc.sysinit` che imposta il percorso, attiva lo swapping, controlla i filesystem e così via. In sostanza, `rc.sysinit` si occupa di tutti i processi che vanno eseguiti all'inizializzazione del sistema. Per esempio, su un sistema in rete, `rc.sysinit` utilizza le informazioni contenute nel file `/etc/sysconfig/network` per inizializzare i processi di rete. La maggior parte dei sistemi utilizza un orologio e `rc.sysinit` usa il file `/etc/sysconfig/clock` per inizializzare l'orologio. Se dovete inizializzare processi speciali per le porte seriali, `rc.sysinit` può eseguire anche `rc.serial`.

In seguito, `init` esegue lo script `/etc/inittab`, che descrive il modo in cui il sistema va configurato per ogni **runlevel** e imposta il runlevel di default. (Per maggiori informazioni sulla configurazione dei runlevel, consultate la Sezione 3.4, *Inizializzazione dei runlevel*). Questo file specifica, tra le altre cose, che `/sbin/update` va eseguito a ogni avvio dei runlevel. Il programma `update` viene utilizzato per ripulire i buffer difettosi su disco.

Quando si cambia un runlevel, `init` utilizza gli script in `/etc/rc.d/init.d` per avviare e bloccare diversi servizi come il server web, il server DNS ecc. Innanzitutto `init` configura la libreria delle funzioni sorgenti per il sistema (di solito `/etc/rc.d/init.d/functions`), che stabilisce come avviare o terminare un programma e come trovarne il PID. In seguito `init` determina il runlevel attuale e quello precedente.

A questo punto `init` avvia tutti i processi di background necessari al sistema per funzionare cercando nella relativa directory `rc` il runlevel (`/etc/rc.d/rc<`*x*`>.d`, dove <*x*> è un numero da 0 a 6). `init` termina tutti gli script kill (il loro nome comincia con una `K`), poi inizializza tutti gli script start (il loro nome comincia per `S`) nella directory di runlevel idonea. In tal modo tutti i servizi e le applicazioni si attivano correttamente). In realtà è possibile eseguire questi script anche manualmente, al termine dell'avvio, collegandosi come root ed eseguendo un comando simile ai seguenti: `/etc/rc.d/init.d/httpd stop` o `service httpd stop`. In questo modo viene disattivato il server `httpd`.

Nota Bene

Se intendete avviare i servizi manualmente, collegatevi come root. Se si verifica un errore durante l'esecuzione di `service httpd stop`, `/sbin` potrebbe non trovarsi in `/root/.bashrc` (o nel file `.rc` corretto per la shell in uso). Digitate l'intero comando `/sbin/service httpd stop` oppure aggiungete `export PATH="$PATH:/sbin"` al file `.rc` della shell. Se modificate il file di configurazione della shell, collegatevi come utente root per attivarlo.

Nessuno degli script che avviano e terminano i servizi si trova in `/etc/rc.d/init.d`. Quasi tutti i file contenuti in `/etc/rc.d/rc<`*x*`>.d` sono **link simbolici** per gli script che si trovano in `/etc/rc.d/init.d`. Un link simbolico è un file che fa riferimento a un altro file e viene usato in questo caso perché può essere creato e cancellato senza intaccare lo script che termina o attiva il servizio. I link simbolici ai diversi script sono numerati secondo un ordine particolare, con cui poi iniziano. È possibile modificare l'ordine in cui i servizi vengono avviati e terminati, modificando il nome del link simbolico relativo allo script che avvia o termina il servizio. È possibile assegnare ai link simbolici lo stesso numero di altri link, se desiderate che quel servizio venga avviato o terminato prima o dopo di un altro.

Per esempio, per trovare il runlevel 5, `init` controlla nella directory `/etc/rc.d/rc5.d`, individuando quanto segue (il vostro sistema e la configurazione potrebbero variare leggermente):

```
K01pppoe -> ../init.d/pppoe
K05innd -> ../init.d/innd
K10ntpd -> ../init.d/ntpd
K15httpd -> ../init.d/httpd
```

```
K15mysqld -> ../init.d/mysqld
K15pvmd -> ../init.d/pvmd
K16rarpd -> ../init.d/rarpd
K20bootparamd -> ../init.d/bootparamd
K20nfs -> ../init.d/nfs
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwalld -> ../init.d/rwalld
K20rwhod -> ../init.d/rwhod
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
K30mcserv -> ../init.d/mcserv
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K50snmpd -> ../init.d/snmpd
K54pxe -> ../init.d/pxe
K55routed -> ../init.d/routed
K60mars-nwe -> ../init.d/mars-nwe
K61ldap -> ../init.d/ldap
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
K75gated -> ../init.d/gated
K80nscd -> ../init.d/nscd
K84ypserv -> ../init.d/ypserv
K90ups -> ../init.d/ups
K96irda -> ../init.d/irda
S05kudzu -> ../init.d/kudzu
S06reconfig -> ../init.d/reconfig
S08ipchains -> ../init.d/ipchains
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13portmap -> ../init.d/portmap
S14nfslock -> ../init.d/nfslock
S18autofs -> ../init.d/autofs
S20random -> ../init.d/random
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
S35identd -> ../init.d/identd
S40atd -> ../init.d/atd
```

```
S45pcmcia -> ../init.d/pcmcia
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S60lpd -> ../init.d/lpd
S75keytable -> ../init.d/keytable
S80isdn -> ../init.d/isdn
S80sendmail -> ../init.d/sendmail
S85gpm -> ../init.d/gpm
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
S90FreeWnn -> ../init.d/FreeWnn
S90xfs -> ../init.d/xfs
S95anacron -> ../init.d/anacron
S97rhnsd -> ../init.d/rhnsd
S99linuxconf -> ../init.d/linuxconf
S99local -> ../rc.local
```

Questi link simbolici indicano a `init` che deve terminare `pppoe`, `innd`, `ntpd`, `httpd`, `mysqld`, `pvmd`, `rarpd`, `bootparamd`, `nfs`, `rstatd`, `rusersd`, `rwalld`, `rwhod`, `squid`, `amd`, `mcserv`, `yppasswdd`, `dhcpd`, `smb`, `vncserver`, `arpwatch`, `named`, `snmpd`, `pxe`, `routed`, `mars-nwe`, `ldap`, `kadmin`, `kprop`, `krb524`, `krb5kdc`, `gated`, `nscd`, `ypserv`, `ups`, e `irda`. Dopo aver chiuso tutti i processi, `init` controlla nella stessa directory e trova degli script start per `kudzu`, `reconfig`, `ipchains`, `portmap`, `nfslock`, `autofs`, `random`, `netfs`, `apmd`, `identd`, `atd`, `pcmcia`, `sshd`, `rawdevices`, `xinetd`, `lpd`, `keytable`, `isdn`, `sendmail`, `gpm`, `canna`, `crond`, `FreeWnn`, `xfs`, `anacron`, `rhnsd`, e `linuxconf`. L'ultima azione di `init` è di avviare `/etc/rc.d/rc.local` per eseguire gli script speciali configurati per quell'host. A questo punto il sistema funziona al runlevel 5.

Dopo che `init` ha percorso tutti i runlevel, lo script `/etc/inittab` crea un processo figlio `getty` per ciascuna console virtuale (prompt di login) di ogni runlevel (i runlevel da 2 a 5 dispongono di sei console; il runlevel 1, in modalità a utente singolo, dispone di un'unica console; i runlevel 0 e 6 non ne ottengono nessuna). In sostanza, `getty` apre delle linee tty, ne imposta la modalità, visualizza il prompt di login, riceve il nome dell'utente e poi inizializza il processo di login per quell'utente. Ciò permette all'utente di autenticarsi al sistema e di cominciare a usarlo.

Inoltre `/etc/inittab` indica a `init` come interpretare la sequenza di tasti [Ctrl]-[Alt]-[Canc]. Dato che Red Hat Linux va chiuso e riavviato in modo corretto, `init` esegue il comando `/sbin/shutdown -t3 -r now` quando un utente usa tale combinazione di tasti. Inoltre `/etc/inittab` specifica a `init` cosa fare in caso di cali di tensione, se il vostro sistema è collegato a un'unità UPS.

`/etc/inittab` esegue uno script chiamato `/etc/X11/prefdm` nel runlevel 5. Lo script `prefdm` avvia il display manager di X (`gdm` se usate GNOME, `kdm` se usate KDE, oppure `xdm` se usate AnotherLevel) a seconda di quanto contenuto nella directory `/etc/sysconfig/desktop`.

A questo punto dovrebbe comparire il prompt di login. Questa operazione richiede solo alcuni secondi.

3.2.3 SysV Init

Come illustrato precedentemente, il programma `init` viene attivato dal kernel all'avvio. Il suo compito è quello di avviare tutti i processi standard che vanno avviati con il sistema. Tra questi figurano i processi getty, che consentono di collegarsi al sistema, i demoni NFS e FTP e qualunque altro servizio vogliate mettere in funzione all'avvio del calcolatore.

SysV init è il processo standard nel mondo Linux per controllare l'esecuzione del software all'avvio. Questo perché è più facile da usare ma anche più potente e flessibile dell'init BSD tradizionale.

Diversamente da BSD init, i file di configurazione di SysV init si trovano in `/etc/rc.d` anziché direttamente in `/etc`. In `/etc/rc.d` troverete `rc`, `rc.local`, `rc.sysinit` e le seguenti directory:

```
init.d
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
```

SysV init rappresenta ogni runlevel init con una directory diversa, utilizzando il programma `init` e i link simbolici in ogni directory per terminare e avviare i servizi mentre il sistema si sposta da runlevel a runlevel.

In breve, la catena degli eventi per un avvio SysV è la seguente:

- Il kernel cerca `init` nella directory `/sbin`.
- `init` avvia lo script `/etc/rc.d/rc.sysinit`
- `rc.sysinit` gestisce quasi tutti i processi del loader di avvio ed esegue `rc.serial` (se presente)
- `init` esegue tutti gli script per il runlevel di default
- `init` esegue `/etc/rc.d/rc.local`

Il runlevel di default è definito in `/etc/inittab`. Dovreste vedere una riga in alto simile a:

```
id:3:initdefault:
```

In questo esempio il runlevel di default è il 3, ossia il numero dopo la prima colonna. Se desiderate modificarlo, potete digitare `/etc/inittab` manualmente. Prestate molta attenzione nel modificare

il file `inittab`. Se vi sbagliate, potete rimediare all'errore riavviando il computer, accedendo al prompt `boot:` con [Ctrl]-[X] e digitando

```
boot:  linux single
```

Questo *dovrebbe* consentirvi di eseguire l'avvio in modalità a utente singolo, in modo da poter ristabilire i valori iniziali di `inittab`.

Discuteremo ora delle informazioni contenute nei file della directory `/etc/sysconfig`. Questi file definiscono i parametri utilizzati dai diversi servizi del sistema quando vengono avviati.

3.3 Informazioni su Sysconfig

Le seguenti informazioni delineano alcuni dei numerosi file contenuti in `/etc/sysconfig`, spiegandone funzione e contenuto. Ovviamente queste informazioni non sono complete, poiché molti dei file hanno numerose opzioni, utilizzate solo in casi specifici e rari.

3.3.1 File contenuti in `/etc/sysconfig`

Nella directory `/etc/sysconfig` si trovano di solito i file seguenti:

- `amd`
- `apmd`
- `authconfig`
- `cipe`
- `clock`
- `desktop`
- `firewall`
- `harddisks`
- `hwconf`
- `i18n`
- `init`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`

- network
- pcmcia
- rawdevices
- sendmail
- soundcard
- ups
- vncservers

È possibile che nel vostro sistema ne manchi qualcuno, se non è installato il programma corrispondente.

Osserviamo questi file in dettaglio:

/etc/sysconfig/amd

Il file /etc/sysconfig/amd contiene diversi parametri utilizzati da amd che consentono di montare o smontare automaticamente i filesystem.

/etc/sysconfig/apmd

Il file /etc/sysconfig/apmd è utilizzato da apmd per sapere quali processi avviare/terminare/modificare in caso di sospensione o ripristino. Questo file è configurato per attivare o disattivare apmd durante l'avvio, a seconda del fatto che il vostro hardware supporti l'**Advanced Power Management** (**APM**) oppure no. apm è un demone con funzioni di controllo che utilizza un codice APM nel kernel di Linux. Se usate Red Hat Linux su un portatile, apmd vi segnala anche lo stato della batteria.

/etc/sysconfig/authconfig

Il file /etc/sysconfig/authconfig stabilisce i tipi di autorizzazione da utilizzare su un host. Contiene una o più delle righe seguenti:

- USEMD5=<*valore*>, dove <*valore*> va sostituito con:
  - yes — se volete usare MD5 per l'autenticazione.
  - no — se non volete usare MD5 per l'autenticazione.

- USEKERBEROS=<*valore*>, dove <*valore*> va sostituito con:
  - yes — se volete utilizzare Kerberos per l'autenticazione.
  - no — se non volete utilizzare Kerberos per l'autenticazione.

- `USELDAPAUTH=<valore>`, dove `<valore>` va sostituito con:
  - `yes` — se volete utilizzare LDAP per l'autenticazione.
  - `no` — se non volete utilizzare LDAP per l'autenticazione.

`/etc/sysconfig/cipe`

Il file `/etc/sysconfig/cipe` configura `cipe` all'avvio.

Può contenere i valori seguenti (esempio):

- `DEVICE=eth0`: specifica l'adattatore di rete utilizzato da `cipe`.
- `PORT=9999`: stabilisce il numero della porta UDP utilizzata dal processo `cipe` in entrambi gli endpoint.
- `PEER=0.0.0.0`: specifica il vero indirizzo dell'endpoint remoto di `cipe`. È possibile configurare questo indirizzo anche in modo dinamico, impostando il valore su 0.0.0.0.
- `IPADDR=0.0.0.0`: specifica l'indirizzo virtuale all'estremità locale del tunnel di `cipe`.
- `PTPADDR=0.0.0.0`, indica l'indirizzo virtuale all'estremità remota del tunnel di `cipe`.

`/etc/sysconfig/clock`

Il file `/etc/sysconfig/clock` controlla l'interpretazione dei valori letti dall'orologio del sistema. Nelle prime versioni di Red Hat Linux venivano usati i seguenti valori (non utilizzateli in questa versione):

- `CLOCKMODE=<valore>`, dove `<valore>` va sostituito con:
  - `GMT` — indica che l'orologio è impostato secondo l'ora del meridiano di Greenwich.
  - `ARC` — indica che è attivo il time offset di 42 anni della console ARC (solo su sistema Alpha).

Attualmente i valori corretti sono:

- `UTC=<valore>`, dove `<valore>` va sostituito con i seguenti valori booleani:
  - `true` — indica che l'orologio è impostato secondo l'ora del meridiano di Greenwich. Qualsiasi altro valore indica che è configurato con l'ora locale.
- `ARC=<valore>`, dove `<valore>` va sostituito con:
  - `true` — indica che il time offset di 42 anni è attivo. Qualsiasi altro valore indica che viene utilizzato il metodo normale per la gestione del tempo di UNIX (solo su sistemi Alpha).

- `ZONE=<nome del file>` — indica il file del fuso orario sotto `/usr/share/zoneinfo` dove `/etc/localtime` ne rappresenta una copia, per esempio:

```
ZONE="America/New York"
```

/etc/sysconfig/desktop

Il file `/etc/sysconfig/desktop` specifica quale manager del desktop eseguire, per esempio:

```
DESKTOP="GNOME"
```

/etc/sysconfig/firewall

Il file `/etc/sysconfig/firewall` contiene varie impostazioni del firewall. Questo file viene creato di default, ma è vuoto.

/etc/sysconfig/harddisks

Il file `/etc/sysconfig/harddisks` vi consente di configurare il disco fisso.

Non effettuate modifiche a questo file, a meno che non sia strettamente necessario. Se modificate i valori di default memorizzati nel file, potreste danneggiare tutti i dati presenti sul disco fisso.

Il file `/etc/sysconfig/harddisks` può contenere i campi seguenti:

- `USE_DMA=1`: impostando il valore 1 viene abilitato il DMA. Tuttavia, con alcuni chipset e combinazioni del disco fisso, il DMA può provocare il danneggiamento dei dati. *Prima di abilitare il DMA, controllate la documentazione del disco fisso.*
- `Multiple_IO=16`: se impostato su 16 abilita diversi settori per ogni interrupt di I/O. Se abilitata, questa caratteristica riduce del 30-50% le informazioni aggiuntive del sistema operativo. *Utilizzatelo con cautela.*
- `EIDE_32BIT=3`: abilita il supporto (E)IDE 32-bit I/O per una scheda di interfaccia.
- `LOOKAHEAD=1`: abilita l'unità read-lookahead.
- `EXTRA_PARAMS=`: specifica dove si possono aggiungere altri parametri.

/etc/sysconfig/hwconf

Il /etc/sysconfig/hwconf elenca tutti i componenti hardware rilevati da kudzu sul sistema e tutti i driver usati, l'ID del rivenditore e del dispositivo. Il programma kudzu rileva e configura componenti hardware nuovi e/o modificati. Il file /etc/sysconfig/hwconf non è stato ideato per essere modificato manualmente. Se lo fate, i dispositivi potrebbero risultare aggiunti o rimossi.

/etc/sysconfig/i18n

Il file /etc/sysconfig/i18n imposta la lingua di default, per esempio:

```
LANG="en_US"
```

/etc/sysconfig/init

Il file /etc/sysconfig/init controlla il funzionamento del sistema durante l'avvio.

Possono essere utilizzati i valori seguenti:

- BOOTUP=<*valore*>, dove <*valore*> va sostituito con:
  - BOOTUP=color: richiama una schermata standard di avvio a colori standard, in cui il successo o il fallimento dei dispositivi e dei servizi sono visualizzati con colori diversi.
  - BOOTUP=verbose: richiama una schermata con stile antiquato, che visualizza soprattutto informazioni piuttosto che messaggi di successo o fallimento.
  - Qualsiasi altra cosa richiama una schermata nuova, ma senza formattazione ANSI.

- RES_COL=<*valore*>, dove <*valore*> è il numero di colonne della schermata dove vengono avviate le etichette dello stato. Il numero predefinito è 60.
- MOVE_TO_COL=<*valore*>, dove <*valore*> muove il cursore alla riga RES_COL. Di default vengono utilizzate le sequenze ANSI visualizzate tramite -e.
- SETCOLOR_SUCCESS=<*valore*>, dove <*valore*> determina il colore per la visualizzazione di un'operazione riuscita. Di default vengono usate le sequenze ANSI visualizzate da -e. Il colore impostato è il verde.
- SETCOLOR_FAILURE=<*valore*>, dove <*valore*> determina il colore per la visualizzazione di un'operazione fallita. Di default vengono usate le sequenze ANSI visualizzate da -e. Il colore impostato è il rosso.
- SETCOLOR_WARNING=<*valore*>, dove <*valore*> determina il colore per la visualizzazione di un avvertimento. Di default vengono usate le sequenze ANSI visualizzate da -e. Il colore impostato è il giallo.

- SETCOLOR_NORMAL=<*valore*>, dove <*valore*> imposta il colore al valore "normale". Di default vengono usate le sequenze ANSI visualizzate da `-e`.
- LOGLEVEL=<*valore*>, dove <*valore*> indica il livello di registrazione per il kernel della console iniziale. Il livello di default è 7; 8 significa "tutto" (incluso il debugging); 1 significa "nulla" ad eccezione dei kernel panic. `syslogd` si sovrappone a questo una volta avviato.
- PROMPT=<*valore*>, dove <*valore*> va sostituito con uno dei seguenti valori booleani:
  - `yes` — abilita il controllo della chiave per la modalità interattiva.
  - `no` — disabilita il controllo della chiave per la modalità interattiva.

/etc/sysconfig/irda

Il file `/etc/sysconfig/irda` controlla la configurazione dei dispositivi a infrarossi all'avvio del sistema.

È possibile utilizzare i valori seguenti:

- IRDA=<*valore*>, dove <*valore*> va sostituito con uno dei valori seguenti booleani:
  - `yes` — viene eseguito `irattach`. Controlla periodicamente la porta di connessione per i dispositivi a infrarossi, per verificare se tali dispositivi, come per esempio un altro portatile, cercano di creare una connessioni di rete. Se desiderate che dispositivi a infrarossi funzionino sul vostro sistema, è necessario impostare questa riga su `yes`.
  - `no` — non viene eseguito `irattach`. Si impedisce così la comunicazione con dispositivi a infrarossi.

- DEVICE=<*valore*>, dove <*valore*> va sostituito con il dispositivo (di solito una porta seriale) che gestisce le connessioni ai dispositivi a infrarossi.
- DONGLE=<*valore*>, dove <*valore*> specifica il tipo di adattatore utilizzato per la comunicazione con dispositivi a infrarossi. Questa impostazione esiste per le persone che utilizzano adattatori seriali piuttosto che vere porte a infrarossi. Un adattatore è un dispositivo collegato a una porta seriale tradizionale per comunicare tramite infrarossi. Questa riga è commentata di default, perchè i portatili con porte a infrarossi effettive sono molto più diffusi di quelli con adattatori aggiunti.
- DISCOVERY=<*valore*>, dove <*valore*> va sostituito con i seguenti valori booleani:
  - `yes` — avvia `irattach` nella modalità Discovery, ciò significa che vengono controllati altri dispositivi a infrarossi. È necessario attivare questo comando per cercare un collegamento a infrarossi.

– `no` — non avvia `irattach` nella modalità Discovery.

/etc/sysconfig/keyboard

Il file `/etc/sysconfig/keyboard` controlla il funzionamento della tastiera. È possibile utilizzare i seguenti valori:

- `KEYBOARDTYPE=sun|pc`, usata solo su SPARCs. La voce `sun` indica che una tastiera Sun è collegata a `/dev/kbd` e `pc` indica che una tastiera PS/2 è connessa a una porta PS/2.
- `KEYTABLE=<file>`, dove `<file>` rappresenta il nome di un file keytable. Per esempio, `KEYTABLE="us"`. I file che possono essere utilizzati come keytable partono da `/usr/lib/kbd/keymaps/i386` e da qui si suddividono in differenti layout di tastiera tutti etichettati come `<file>.kmap.gz`. Viene usato il primo file individuato in `/usr/lib/kbd/keymaps/i386` che coincide con le impostazioni di `KEYTABLE`.

/etc/sysconfig/kudzu

Il file `/etc/sysconfig/kuzdu` consente un controllo sicuro del vostro hardware tramite `kudzu` all'avvio. Per "controllo sicuro" si intende un controllo che disabilita la porta seriale e la verifica del monitor DDC.

- `SAFE=<valore>`, dove `<valore>` va sostituito con:
  – `yes` — `kuzdu` esegue un controllo sicuro.
  – `no` — `kuzdu` esegue un controllo normale.

/etc/sysconfig/mouse

Il file `/etc/sysconfig/mouse` viene utilizzato per indicare le informazioni relative al mouse disponibile. Utilizzate i valori seguenti:

- `FULLNAME=<valore>`, dove `<valore>` va sostituito con il nome del tipo di mouse utilizzato.
- `MOUSETYPE=<valore>`, dove `<valore>` indica:
  – `microsoft` — un mouse Microsoft.
  – `mouseman` — un mouse MouseMan.
  – `mousesystems` — un mouse Systems.
  – `ps/2` — un mouse PS/2.
  – `msbm` — un mouse bus Microsoft.

  - `logibm` — un mouse bus Logitech.
  - `atibm` — un mouse bus ATI.
  - `logitech` — un mouse Logitech.
  - `mmseries` — un mouse MouseMan antiquato.
  - `mmhittab` — un mouse mmhittab.

- `XEMU3=<valore>`, dove `<valore>` va sostituito con uno dei seguenti valori booleani:
  - `yes` — Il mouse ha solo due tasti, ma il terzo tasto viene emulato.
  - `no` — il mouse ha già tre tasti.

- `XMOUSETYPE=<valore>`, dove `<valore>` indica il tipo di mouse utilizzato con X. Le opzioni sono le stesse di `MOUSETYPE`.

Inoltre `/dev/mouse` è un link simbolico al dispositivo mouse in uso.

`/etc/sysconfig/network`

Il file `/etc/sysconfig/network` è utilizzato per specificare le informazioni relative alla configurazione di rete desiderata. È possibile usare i seguenti parametri:

- `NETWORKING=<valore>`, dove `<valore>` indica uno dei seguenti valori booleani:
  - `yes` — la rete deve essere configurata.
  - `no` — la rete non deve essere configurata.

- `HOSTNAME=<valore>`, dove `<valore>` deve essere sostituito dall'**FQDN** (**Fully Qualified Domain Name**), per esempio: `hostname.domain.com`.

Nota Bene

Per questioni di compatibilità con il vecchio software che si desidera installare (per esempio `trn`), il file `/etc/HOSTNAME` deve contenere questi valori.

- `GATEWAY=<valore>`, dove `<valore>` rappresenta l'indirizzo IP del gateway della rete.

- `GATEWAYDEV=<valore>`, dove `<valore>` rappresenta il dispositivo per accedere al gateway, per esempio: `eth0`.
- `NISDOMAIN=<valore>`, dove `<valore>` rappresenta il nome del dominio NIS.

/etc/sysconfig/pcmcia

Il file `/etc/sysconfig/pcmcia` viene usato per specificare le informazioni di configurazione PCMCIA. È possibile utilizzare i seguenti valori:

- `PCMCIA=<valore>`, dove `<valore>` indica:
  - `yes` — il supporto PCMCIA va abilitato.
  - `no` — il supporto PCMCIA non va abilitato

- `PCIC=<valore>`, dove al posto di `<valore>` si ha:
  - `i82365` — il computer ha un un chipset socket della PCMCIA di tipo i82365.
  - `tcic` — Il computer ha un un chipset socket della PCMCIA di tipo tcic.

- `PCIC_OPTS=<valore>`, dove `<valore>` rappresenta i driver socket (i82365 o tcic).
- `CORE_OPTS=<valore>`, dove `<valore>` rappresenta la lista delle opzioni `pcmcia_core`.
- `CARDMGR_OPTS=<valore>`, dove `<valore>` rappresenta la lista delle opzioni per il `cardmgr` della PCMCIA (come `-q` per la modalità silenziosa e `-m` per la ricerca dei moduli del kernel caricabili nella directory specificata). Per maggiori informazioni, leggete la pagina man relativa a `cardmgr`.

/etc/sysconfig/rawdevices

Il file `/etc/sysconfig/rawdevices` viene utilizzato per configurare i collegamenti raw device:

```
/dev/raw/raw1 /dev/sda1
/dev/raw/raw2 8 5
```

/etc/sysconfig/sendmail

Il file `/etc/sysconfig/sendmail` consente di inviare messaggi a uno o più destinatari, indirizzando il messaggio sulla rete necessaria. Il file imposta i valori di default per eseguire l'applicazione Sendmail. I valori di default eseguono il programma come demone in background e ne controllano la coda di attesa ogni ora nel caso in cui qualche messaggio sia tornato indietro.

È possibile usare i seguenti valori:

- DAEMON=<*valore*>, dove <*valore*> va sostituito con uno dei valori booleani seguenti:
  - yes — Sendmail può essere configurato per controllare l'arrivo di posta alla porta 25. yes implica l'uso delle opzioni -bd di Sendmail
  - no — Sendmail può non essere configurato per controllare l'arrivo di posta alla porta 25.

- QUEUE=1h viene trasmesso a Sendmail come -q$QUEUE. L'opzione -q non viene trasmessa a Sendmail se esiste /etc/sysconfig/sendmail e QUEUE è vuota o non definita.

/etc/sysconfig/soundcard

Il file /etc/sysconfig/soundcard viene generato da sndconfig e non deve essere modificato. Va usato solo per determinare quale scheda inserire nel menu, in modo che all'esecuzione successiva di sndconfig venga usata come scheda predefinita. Le informazioni sulla configurazione della scheda sonora si trovano nel file /etc/modules.conf.

Potrebbe contenere:

- CARDTYPE=<*valore*>, dove <*valore*> può essere per esempio, SB16, nel caso di una scheda audio Soundblaster 16.

/etc/sysconfig/ups

Il file /etc/sysconfig/ups è utilizzato per specificare le informazioni relative a qualsiasi **UPS** (**Uninterruptible Power Supplies**) collegato al vostro sistema. Un UPS può essere molto utile per un sistema Red Hat Linux perchè vi da il tempo per chiudere correttamente il sistema in caso di interruzione della corrente elettrica. Si possono usare i seguenti valori:

- SERVER=<*valore*>, dove <*valore*> è sostituito da:
  - yes — è collegato un dispositivo UPS al sistema
  - no — non è collegato alcun dispositivo UPS al sistema.

- MODEL=<*valore*>, dove <*valore*> deve essere impostato su NONE se nessun dispositivo UPS è collegato al sistema oppure deve essere:
  - apcsmart — per un UPS APC Smart oppure un dispositivo simile.
  - fentonups — per un UPS Fenton.
  - optiups — per un dispositivo UPS OPTI.

  - `bestups` — per un UPS Best Power.
  - `genericups` — per un dispositivo UPS generico.
  - `ups-trust425+625` — per un UPS Trust.

- `DEVICE=<`*`valore`*`>`, dove `<`*`valore`*`>` specifica il punto in cui è collegato il dispositivo UPS, per esempio: `/dev/ttyS0`.
- `OPTIONS=<`*`valore`*`>`, dove `<`*`valore`*`>` è un comando speciale da trasmettere al dispositivo UPS.

`/etc/sysconfig/vncservers`

Il file `/etc/sysconfig/vncservers` configura l'avvio del server **VNC** (**Virtual Network Computing**). VNC è un sistema di visualizzazione remoto che consente di mostrare un'ambiente desktop non solo sull'elaboratore dove è in esecuzione ma anche su reti diverse (da una LAN a Internet).

Può contenere:

- `VNCSERVERS=<`*`valore`*`>`, dove `<`*`valore`*`>` è impostato come `"1:root"`.

3.3.2 File in `/etc/sysconfig/network-scripts/`

Solitamente i file seguenti si trovano in `/etc/sysconfig/network-scripts`, dove `<`*`if-name`*`>` rappresenta il nome dell'interfaccia di rete:

- `/etc/sysconfig/network-scripts/ifup`
- `/etc/sysconfig/network-scripts/ifdown`
- `/etc/sysconfig/network-scripts/network-functions`
- `/etc/sysconfig/network-scripts/ifcfg-<`*`if-name`*`>`
- `/etc/sysconfig/network-scripts/ifcfg-<`*`if-name`*`>-<`*`clone-name`*`>`
- `/etc/sysconfig/network-scripts/chat-<`*`if-name`*`>`
- `/etc/sysconfig/network-scripts/dip-<`*`if-name`*`>`
- `/etc/sysconfig/network-scripts/ifup-post`

Osserviamo in dettaglio ogni file.

/etc/sysconfig/network-scripts/ifup e /etc/sysconfig/network-scripts/ifdown

Sono link simbolici a `/sbin/ifup` e `/sbin/ifdown`. Sono gli unici due script in questa directory che dovrebbero essere richiamati direttamente. Questi due script richiamano tutti gli altri script quando è necessario. Questi link simbolici servono solo per motivi di conformità. Probabilmente verranno rimossi nelle prossime versioni, quindi attualmente vanno utilizzati solo `/sbin/ifup` e `/sbin/ifdown`.

Questi script di solito hanno un argomento: il nome del dispositivo (per esempio: `eth0`). Durante la sequenza di avvio sono richiamati con un argomento di `boot` in modo tale che i dispositivi che non si intende considerare all'avvio (`ONBOOT=no`, [vedere sotto]) possano essere ignorati.

/etc/sysconfig/network-scripts/network-functions

Non si tratta di un file pubblico. Contiene funzioni usate dagli script per attivare e disattivare le interfacce. In particolare contiene il codice per gestire la configurazione dell'interfaccia e la modifica della configurazione tramite `netreport`, ossia il programma che ordina agli script di gestione della rete di inviare un segnale SIGIO per il processo che richiama `netreport` quando si verificano modifiche nello stato dell'interfaccia di rete.

/etc/sysconfig/network-scripts/ifcfg-<*if-name*> e /etc/sysconfig/network-scripts/ifcfg-<*if-name*>:<*clone-name*>

Il primo file identifica un'interfaccia, il secondo contiene solo le parti differenti in un'interfaccia "alias". Per esempio, i numeri di rete (network) possono essere differenti nel file clone, in quanto tutte le informazioni sul dispositivo dovrebbero essere nel file di base `ifcfg`, ma il resto deve rimanere invariato.

Le variabili che possono essere definite in un file `ifcfg` dipendono dal tipo di interfaccia.

Le seguenti variabili sono comuni a tutti i file di base:

- `DEVICE=`<*nome*>, dove <*nome* indica il nome del dispositivo fisico (ad eccezione dei dispositivi PPP allocati in modo dinamico, in cui viene definito un "nome logico").
- `IPADDR=`<*indir*>, dove <*indir*> indica l'indirizzo IP.
- `NETMASK=`<*maschera*>, dove <*maschera*> rappresenta il valore della maschera di rete.
- `NETWORK=`<*indir*>, dove <*indir*> indica l'indirizzo IP.
- `BROADCAST=`<*indir*>, dove <*indir*> è l'indirizzo di broadcast.
- `GATEWAY=`<*indir*>, dove <*indir*> rappresenta l'indirizzo del gateway.
- `ONBOOT=`<*risposta*>, dove <*risposta*> è sostituito da:

  - `yes` — il dispositivo viene attivato all'avvio.
  - `no` — il dispositivo non viene attivato all'avvio.
- `USERCTL=<risposta>`, dove `<risposta>` indica che:
  - `yes` — agli utenti standard è consentito controllare questo dispositivo.
  - `no` — agli utenti standard non è consentito controllare questo dispositivo.
- `BOOTPROTO=<proto>`, dove per `<proto>` si ha:
  - `none` — non viene utilizzato nessun protocollo all'avvio.
  - `bootp` — viene usato il protocollo BOOTP.
  - `dhcp` — viene usato il protocollo DHCP.

I valori seguenti sono comuni a tutti i file SLIP:

- `PERSIST=<risposta>`, dove per `<risposta>` si ha:
  - `yes` — questa interfaccia deve essere sempre attiva, anche se disattivata da una disconnessione del modem.
  - `no` — questa interfaccia non deve essere sempre attiva.

- `MODEMPORT=<porta>`, dove `<porta>` indica il nome del dispositivo relativo alla porta del monitor (per esempio, "`/dev/modem`").
- `LINESPEED=<baud>`, dove `<baud>` rappresenta la velocità del modem (per esempio, "`115200`").
- `DEFABORT=<risposta>`, dove `<risposta>` è sostituito da:
  - `yes` — inserisce la stringa di chiusura durante la creazione/modifica dello script per questa interfaccia.
  - `no` — non inserisce la stringa di chiusura durante la creazione/modifica dello script per questa interfaccia.

`/etc/sysconfig/network-scripts/chat-<if-name>`

Questo file è uno script chat per le connessioni SLIP e il suo scopo è quello di stabilire connessioni. Per i dispositivi SLIP, lo script DIP viene generato basandosi sulle informazioni di uno script chat.

/etc/sysconfig/network-scripts/ifup-post

Questo file è chiamato quando un dispositivo di rete è attivato (ad eccezione del dispositivo SLIP). Richiama lo script `/etc/sysconfig/network-scripts/ifup-routes` per attivare il routing statico e gli eventuali alias del dispositivo. Imposta il nome dell'host, se non è presente, a cui associare l'IP del dispositivo. Trasmette un SIGIO a tutti i programmi che hanno richiesto questo avviso degli eventi sulla rete.

Questo file potrebbe essere esteso per inizializzare la configurazione del name service, richiamare in modo arbitrario gli script e, se necessario, per molte altre funzioni.

3.4 Inizializzazione dei runlevel

L'idea di attivare servizi diversi in runlevel differenti si basa sul fatto che questi servizi diversi possono avere varie funzioni. Alcuni servizi non possono essere usati fino a quando il sistema si trova in uno stato o in una **modalità** particolare, per esempio, pronto per più di un utente oppure collegato a una rete. Se desiderate potete attivare il sistema in una modalità più bassa, per testare un problema di rete nel runlevel 2 oppure lasciare il sistema nel runlevel 3 senza eseguire una sessione di X. In questi casi eseguire i servizi che funzionano con una modalità maggiore non ha senso perché non funzionerebbero comunque in modo corretto. Avendo già stabilito che ogni servizio parta quando il sistema raggiunge il runlevl dove si trova, assicurate un processo di avvio e potete modificare velocemente la modalità della macchina senza dovervi preoccupare di attivare o disattivare i servizi manualmente.

In genere Red Hat Linux opera nel runlevel 3 — modalità multiutente. I seguenti runlevel sono definiti in Red Hat Linux:

- `0` — arresto
- `1` — modalità a utente singolo
- `2` — modalità multiutente, senza networking
- `3` — modalità multiutente completa
- `4` — non usato
- `5` — modalità multiutente completa (con schermata di login basata su X)
- `6` — riavvio

Il runlevel di default da cui un sistema si avvia e si chiude è configurato in `/etc/inittab`. Per maggiori informazioni su `/etc/inittab`, vedere la Sezione 3.2.3, *SysV Init*.

Se il vostro computer si trova in uno stato in cui non può avviarsi a causa di un `/etc/inittab` errato o non vi lascia entrare perché avete un `/etc/passwd` danneggiato o avete semplicemente dimenticato la vostra password, avviate la procedura per utente singolo digitando **`linux single`**

al prompt di LILO `boot:`. Verranno caricati il sistema base e una shell con la quale potrete modificare la vostra configurazione.

3.5 Utility di initscript

L'utility `chkconfig` fornisce un semplice strumento a linea di comando per la manutenzione della gerarchia delle directory `/etc/rc.d`. Solleva gli amministratori di sistema dall'incombenza di manipolare direttamente i numerosi link simbolici nelle directory che si trovano sotto `/etc/rc.d`.

Inoltre l'utility `ntsysv` nella directory `/usr/sbin` fornisce un'interfaccia grafica molto più facile da usare rispetto all'interfaccia a linea di comando di `chkconfig`. Entrambe queste utility vanno eseguite come utente di root.

Per maggiori informazioni, consultate le pagine man relative a `chkconfig` e `ntsysv`.

3.6 Esecuzione dei programmi all'avvio

Lo script del file `/etc/rc.d/rc.local` viene eseguito al momento dell'avvio, dopo che tutte le inizializzazioni sono state completate, e quando modificate i runlevel. Qui potete aggiungere comandi di inizializzazione. Per esempio, potete avere bisogno di eseguire l'avvio di un demone per la stampante.

Inoltre se vi occorre configurare una porta seriale, potete creare e modificare `/etc/rc.serial`, che verrà eseguito in modo automatico all'avvio. Questo script può eseguire una serie di comandi `setserial` per configurare le porte seriali del sistema. Per maggiori informazioni, consultate la pagina man relativa a `setserial`.

La configurazione di default di`/etc/rc.d/rc.local` crea un banner di login con la vostra versione del kernel e il tipo di macchina.

3.7 Chiusura del sistema

Per chiudere correttamente Red Hat Linux, usate il comando `shutdown`. Potete leggere la pagina man di `shutdown` per maggiori dettagli, ma i due utilizzi più comuni sono:

```
/sbin/shutdown -h now
/sbin/shutdown -r now
```

È necessario eseguire il comando `shutdown` come utente root. Dopo aver chiuso tutto, l'opzione `-h` spegne l'elaboratore e l'opzione `-r` lo riavvia.

Sebbene i comandi `reboot` e `halt` sono ora abbastanza "evoluti" da attivare il programma `shutdown` direttamente, se il vostro sistema si trova in un runlevel compreso tra 1 e 5 è meglio non utilizzarli, poiché non tutti i sistemi operativi Linux-like hanno queste proprietà.

AVVERTIMENTO

Se il computer non si spegne da solo, aspettate che a video compaia il messaggio "system is halted" prima di premere il pulsante power.

Se spegnete l'elaboratore prima di questo messaggio, potreste impedire che le partizioni del disco fisso vengano smontate. Questo può causare un danneggiamento dei filesystem, al punto che il sistema potrebbe non riuscire a effettuare l'avvio. Quindi attenzione!

3.8 Differenze nel processo di avvio di altre architetture

Ogni architettura supportata da Red Hat Linux avvia il sistema operativo in modo diverso. Comunque, una volta avviato il kernel e trasmesso il controllo del processo di avvio a `init`, la procedura è la stessa su qualsiasi tipo di architettura. L'unica differenza è nel modo in cui Red Hat Linux individua il kernel per caricarlo e far avviare `init`.

Per informazioni più dettagliate sui differenti metodi di avvio, consultate la documentazione relativa all'architettura che vi interessa.

4 LDAP (Lightweight Directory Access Protocol)

4.1 Cos'è il protocollo LDAP?

Il protocollo **LDAP** (**Lightweight Directory Access Protocol**) è uno standard aperto per i servizi su una rete Intranet o Internet. Una directory gestita dal protocollo LDAP è simile a una guida telefonica e può gestire molte altre informazioni, ma allo stato attuale viene usato principalmente per associare nomi a numeri telefonici e a indirizzi e-mail. Le directory supportano grandi volumi di traffico, ma i dati in esse contenuti non variano spesso.

Il protocollo LDAP è molto più utile di una guida telefonica cartacea, poiché è stata ideato per supportare la diffusione attraverso i server LDAP in Internet, come accade per il **Domain Name Server** (**DNS**). Il DNS funziona come una rubrica tenendo traccia della coppia nome_simbolico/IP. I server DNS collegano le macchine in rete basandosi su nomi di dominio qualificati o sul tipo di servizio richiesto da un dominio, come lo scambio di posta. Senza i server DNS, gli hostname non potrebbero essere tradotti in indirizzi IP, richiesti per la comunicazione TCP/IP. In futuro l'LDAP potrà offrire lo stesso tipo di accesso globale per molti tipi di informazione sulle directory: oggi, l'LDAP è comunemente usato all'interno di una singola grande azienda, come un'università o una società, per gestire i servizi inerenti le directory.

LDAP è un sistema client-server. Un client LDAP si connette a un server LDAP e richiede le informazioni o fornisce i dati necessari per accedere a una directory. Il server risponde alla richiesta, invia la query a un altro server oppure accetta le informazioni da inserire nella directory, in base ai permessi dell'utente.

LDAP è noto anche come **X.500 Lite**. X.500 è uno standard internazionale per le directory, include numerose caratteristiche interessanti ma è molto complesso e richiede grandi risorse di elaborazione e uno stack OSI compatibile. L'LDAP, al contrario, funziona in modo corretto su ogni PC ed è compatibile con il protocollo TCP/IP. L'LDAP può accedere alle directory X.500 ma non supporta tutte le funzioni di X.500.

In questo capitolo viene trattata la configurazione e l'uso di OpenLDAP, un'implementazione open-source di LDAP. OpenLDAP comprende `slapd` (un server LDAP stand-alone), `slurpd` (un server stand-alone con propagazione di LDAP), librerie che implementano il protocollo LDAP, utility, tool, e semplici client.

4.2 Vantaggi e svantaggi del protocollo LDAP

Il vantaggio principale nell'uso dell'LDAP è la possibilità di consolidare certi tipi di informazioni all'interno della vostra azienda. Per esempio, tutte le diverse liste di utenti azienda possono essere

riunite in una sola directory LDAP. Questa directory, in seguito, potrà essere interrogata da qualsiasi applicazione abilitata all'uso dell'LDAP e anche dagli utenti.

Tra gli altri vantaggi offerti dalla tecnologia LDAP vi è la semplicità di implementazione (rispetto a X.500) e la coerenza dell'API. Ciò significa che il numero delle applicazioni e dei gateway che sfruttano l'LDAP possono crescere in futuro.

Lo svantaggio consiste nel fatto che per utilizzare l'LDAP occorre usare un client abilitato a passare attraverso un gateway LDAP. Come già accennato, la presenza dell'LDAP crescerà in futuro, ma attualmente non esistono molte applicazioni disponibili per Linux che lo sfruttano. Inoltre, benché l'LDAP supporti alcuni controlli sull'accesso, non supporta tutti gli aspetti della sicurezza garantiti da X.500.

4.3 Uso dell'LDAP

Molte applicazioni Netscape, incluso il Netscape Roaming Access, sono abilitate al protocollo LDAP. Sendmail può usare l'LDAP per cercare un indirizzo. La vostra azienda potrebbe usare l'LDAP come una directory condivisa da tutta la società e come un name-service (al posto del NIS o del flat-file). Potrete anche usare un server LDAP personale per la vostra rubrica e-mail privata (consultate la Sezione 4.11, *Risorse aggiuntive*).

Dal momento che l'LDAP è un protocollo aperto e configurabile, può essere utilizzato per memorizzare quasi ogni tipo di informazione relativa a una struttura organizzativa particolare.

4.3.1 Applicazioni LDAP

Sono disponibili molte applicazioni client LDAP, ciò semplifica notevolmente la visualizzazione e la modifica di informazioni LDAP:

- Browser/Editor LDAP — un tool user-friendly scritto al 100% in Java per un utilizzo semplice in diverse piattaforme, reperibile all'indirizzo http://www.iit.edu/~gawojar/ldap
- GQ — un client LDAP basato su GTK, fornito con Red Hat Linux 7.1 oppure reperibile all'indirizzo http://biot.com/gq
- kldap — un client LDAP per il progetto KDE, disponibile all'indirizzo http://www.mountpoint.ch/oliver/kldap

4.3.2 LDAP e PAM

Il protocollo LDAP può essere utilizzato come servizio di autenticazione tramite il modulo `pam_ldap`. Normalmente è usato come server centrale di autenticazione, in modo tale che gli utenti abbiano una login unificato che comprenda le login di console, i server POP e IMAP, le macchine connesse a una rete tramite Samba e perfino calcolatori Windows NT/2000. Con l'uso dell'LDAP tutte queste "situazioni" di login si affidano a un unico ID utente e a una singola password,

semplificando notevolmente l'amministrazione. Il modulo `pam_ldap` è fornito nel pacchetto `nss_ldap`.

4.4 Terminologia dell'LDAP

Un'**entry** è un'unità in una directory LDAP, identificata dal proprio e unico **Distinguished Name** (DN).

Ogni entry possiede degli attributi, ossia parti di informazione direttamente associate all'entry. Per esempio, un'azienda potrebbe essere un'entry LDAP. Gli attributi associati all'azienda possono essere il numero di fax, l'indirizzo e così via. Le persone potrebbero essere altre entry nella directory LDAP. Gli attributi comuni alle persone sono il numero di telefono e l'indirizzo e-mail.

Alcuni attributi sono necessari, mentre altri sono facoltativi. Una **objectclass** evidenzia gli attributi necessari e quelli opzionali. Le definizioni di objectclass si trovano in diversi file contenuti nella directory `/etc/openldap/schema`.

L'**LDAP Data Interchange Format** (LDIF) è un file ASCII in formato testo utilizzato per le entry. I file che importano o esportano dati da un server LDAP devono essere in formato LDIF. Un esempio di entry LDIF è:

```
[<id>]
dn: <distinguished name>
<tipoattr>: <valoreattr>
<tipoattr>: <valoreattr>
<tipoattr>: <valoreattr>
```

Un'entry può contenere il numero necessario di coppie `<tipoattr>: <valoreattr>`. Una riga bianca indica che la voce è completa e che sta per iniziare un'altra entry.

Le coppie `<tipoattr>` e `<valoreattr>` *devono* essere definite in uno schema prima di poter essere utilizzate. Non è possibile definirle in un file LDIF e aspettarsi che un server LDAP sia in grado di utilizzare queste informazioni senza fornire dati corrispondenti nei file schema.

Quanto racchiuso tra < > rappresenta una variabile e può essere configurato quando aggiungete un'entry LDAP, con l'eccezione di `<id>`. L'`<id>` è un numero configurato di solito dai tool LDAP quando viene aggiunge una nuova entry e probabilmente non vi capiterà mai di doverlo impostare.

4.5 OpenLDAP 2.0 - Versione aggiornata

OpenLDAP 2.0 rappresenta un ulteriore aggiornamento per l'applicazione e contiene:

- *Supporto LDAPv3* — ora funziona con SASL, TLS e SSL ed è interamente compatibile con RFC 2251-2256; le modifiche rispetto alla versione precedente mirano a rendere LDAP un protocollo molto più sicuro.
- *Supporto IPv6 Support* — ora supporta la generazione futura del protocollo Internet.
- *LDAP tramite IPC* — OpenLDAP può comunicare all'interno di un particolare sistema senza dover attraversare una rete, garantendo così una maggiore sicurezza.
- *API C aggiornata* — migliora il modo in cui i programmatori possono collegarsi all'applicazione e utilizzarla.
- *Supporto LDIFv1* — interamente compatibile con la versione 1 di LDAP Data Interchange Format (LDIF).
- *Server LDAP stand-alone aggiornato* — Comprende un sistema di controllo dell'accesso aggiornato, un raggruppamento dei thread, tool migliori e altro ancora.

4.6 I file di OpenLDAP

I file di configurazione di OpenLDAP vengono installati nella directory `/etc/openldap`. Se digitate `ls` in `/etc/openldap`, vedrete qualcosa di simile a:

```
ldap.conf        ldapsearchprefs.conf  schema
ldapfilter.conf  ldaptemplates.conf    slapd.conf
```

4.6.1 Modifica di `/etc/openldap/slapd.conf`

Il file `slapd.conf` si trova in `/etc/openldap` e contiene le informazioni per la configurazione del server LDAP `slapd`. È necessario apportare alcune modifiche a questo file in modo da renderlo specifico per il vostro dominio e server.

La riga di suffisso richiama il dominio per il quale il server LDAP deve fornire le informazioni. Tale riga va modificata da:

```
suffix          "dc=your-domain, dc=com"
```

in questo modo riflette il nome del dominio. Per esempio:

```
suffix          "dc=acmewidgets, dc=com"
```

oppure

```
suffix          "dc=acmeuniversity, dc=edu"
```

L'entry rootdn rappresenta il DN per un'utente che non ha limitazioni nel controllo di accesso o nei parametri limite amministrativi impostati per le operazioni sulla directory LDAP. L'utente rootdn può essere considerato un utente root per la directory LDAP. La riga rootdn va modificata da:

```
rootdn          "cn=root, dc=your-domain, dc=com"
```

in qualcosa di simile al seguente esempio:

```
rootdn          "cn=root, dc=redhat, dc=com"
```

oppure

```
rootdn          "cn=ldapmanager, dc=my_organization, dc=org"
```

Modificate la riga da rootpw:

```
rootpw          secret
```

in:

```
rootpw          {crypt}s4L9sOIJo4kBM
```

Nell'esempio illustrato sopra, viene utilizzata una password di root cifrata, un'idea senz'altro migliore rispetto al testo in chiaro contenuto nel file `slapd.conf`. Per creare questa stringa cifrata, utilizzate Perl:

```
perl -e "print crypt('passwd','a_salt_string');"
```

Nell riga Perl, *`salt_string`* rappresenta una stringa di due caratteri e *`passwd`* è la versione in testo in chiaro della password.

Potete anche copiare una entry `passwd`, da `/etc/passwd` ma non funziona se la entry è una password MD5 (di default in Red Hat Linux 7.1).

4.6.2 La directory `schema`

La directory `schema`, nuova per la versione 2 di OpenLDAP, contiene le diverse definizioni LDAP, che prima si trovavano nei file `slapd.at.conf` e `slapd.oc.conf`. Tutte le **definizioni sintattiche degli attributi** e **le definizioni objectclass** si trovano ora in file schema differenti. Si fa riferimento a questi file in `/etc/openldap/slapd.conf` utilizzando righe `include`, come visualizzato qui di seguito:

```
include  /etc/openldap/schema/core.schema
include  /etc/openldap/schema/cosine.schema
include  /etc/openldap/schema/inetorgperson.schema
include  /etc/openldap/schema/nis.schema
include  /etc/openldap/schema/rfc822-MailMember.schema
include  /etc/openldap/schema/autofs.schema
include  /etc/openldap/schema/kerberosobject.schema
```

Vi consigliamo di non modificare alcun oggetto definito nei file schema installati da OpenLDAP.

È possibile estendere lo schema utilizzato da OpenLDAP per supportare tipi di attributi aggiuntivi e gli object class che usano i file schema di default come guida. Per farlo, create un file `local.schema` nella directory `/etc/openldap/schema`. Fate riferimento a questo nuovo schema contenuto in `slapd.conf` aggiungendo la seguente riga sotto le vostre righe schema `include`:

```
include  /etc/openldap/schema/local.schema
```

È ora necessario definire i nuovi tipi di attributi e object class all'interno del file `local.schema`. Molte organizzazioni utilizzano tipi di attributi esistenti e object class dei file schema installati di default e li modificano per utilizzarli nel file `local.schema`. Ciò può aiutarvi a imparare la sintassi di schema pur venendo incontro alle esigenze immediate della vostra organizzazione.

La procedura di estensione degli schemi per soddisfare determinati requisiti è piuttosto complessa ed esula dall'obiettivo di questo capitolo. Per ulteriori informazioni sulla creazione di nuovi file schema, visitate il sito http://www.openldap.org/doc/admin/schema.html.

4.7 Demoni e utility di OpenLDAP

Il pacchetto OpenLDAP contiene due demoni: `slapd` e `slurpd`.

Il demone `slapd` è il demone LDAP di cui avrete bisogno per eseguire il supporto LDAP.

Il demone `slurpd` controlla la duplicazione delle directory LDAP in una rete, inviando le modifiche dalla directory master LDAP alle directory slave LDAP. Non avrete bisogno di usare `slurpd` a meno che non abbiate più di un server LDAP sulla vostra rete. Se avete due o più server LDAP, dovrete usare `slurpd` per mantenere sincronizzate le varie directory LDAP.

OpenLDAP comprende inoltre alcune utility in `/usr/bin` per aggiungere, modificare e cancellare entry in una directory LDAP:

- `ldapmodify` — modifica le entry in un database LDAP, accettando input standard o mediante file.
- `ldapadd` — aggiunge la entry alla vostra directory, accettando input standard o mediante file; `ldapadd` rappresenta un collegamento a `ldapmodify -a`.
- `ldapsearch` — cerca le entry in una directory LDAP utilizzando il prompt della shell.

- `ldapdelete` — cancella le entry di una directory LDAP accettando input tramite un file o un prompt della shell.

Ad eccezione di `ldapsearch`, ognuna di queste utility è molto più semplice da utilizzare poiché è sufficiente digitare il file con le modifiche da effettuare piuttosto che digitare i comandi uno dopo l'altro. Ognuna delle relative pagine man illustra la sintassi di questi file.

Per importare o esportare blocchi di informazioni con una directory `slapd` o per eseguire task amministrative simili, utility differenti posizionati in `/usr/sbin` sono necessari:

- `slapadd` — aggiunge entry da un file LDIF a una directory LDAP. Per esempio, eseguite `/usr/sbin/slapadd -l` *`ldif`*, dove *`ldif`* rappresenta il nome del file LDIF contenente le nuove entry.
- `slapcat` — estrae le entry da una directory LDAP e le salva in un file LDIF. Per esempio, eseguite `/usr/sbin/slapcat -l` *`ldif`* dove *`ldif`* rappresenta il nome del file LDIF di destinazione che conterrà la directory LDAP.
- `slapindex` — ricrea l'indice del database `slapd` basandosi sul contenuto attuale del database. Eseguite `/usr/sbin/slapindex` per avviare la ricreazione dell'indice.
- `slappasswd` — genera un valore per la password utente da usare con `ldapmodify` o il valore `rootpw` in `/etc/openldap/slapd.conf`. Eseguite `/usr/sbin/slappasswd` per creare la password.

AVVERTIMENTO

Assicuratevi di interrompere `slapd` prima di utilizzare `slapadd`, `slapcat` oppure `slapindex`, altrimenti mettete a rischio la consistenza del vostro database LDAP.

Per maggiori informazioni su ognuna di queste utility, consultate le pagine man.

4.8 Moduli per aggiungere funzioni a LDAP

Red Hat Linux comprende numerosi pacchetti che aggiungono ulteriori funzioni a LDAP.

Il modulo `nss_ldap` è un modulo LDAP per il **Solaris Nameservice Switch** (NSS). NSS è un insieme di librerie scritte in C necessarie per accedere alle informazioni contenute nella directory LDAP, invece di o in aggiunta al name service o ai file flat del **Network Information Service** (NIS)

Il modulo `pam_ldap` è necessario per integrare l'autenticazione di LDAP nel Pluggable Authentication Modules (PAM) API. Se usate `pam_ldap`, gli utenti possono autenticare e cambiare la loro

password usando le directory LDAP. I moduli `nss_ldap` e `pam_ldap` fanno parte del pacchetto `nss_ldap`.

Red Hat Linux comprende anche i moduli LDAP per il server Web Apache. Il modulo `auth_ldap` consente di autenticare i client HTTP per le entry degli utenti nella directory LDAP. Il modulo `php-ldap` aggiunge il supporto LDAP al linguaggio di scripting PHP4 HTML integrato. Per poter funzionare, i moduli `auth_ldap` e `php-ldap` dovranno essere compilati in Apache come **Dynamic Shared Objects** (**DSO**).

4.9 LDAP HowTo: un rapido riepilogo

Questa sezione illustra i passi principali per attivare una directory LDAP.

1. Assicuratevi che il pacchetto RPM `openldap` e qualsiasi altro pacchetto RPM relativo a LDAP siano stati installati.
2. Leggete la Quick Start Guide disponibile al sito OpenLDAP (http://www.openldap.org/faq/data/cache/172.html. Iniziate da "Create configuration file for slapd," visto che i file LDAP sono già installati) o il Linux-LDAP HOWTO (http://www.linuxdoc.org/HOWTO/LDAP-HOWTO.html) per le istruzioni relative all'uso di LDAP nel vostro sistema. Entrambi illustrano in dettaglio i passi rimanenti da seguire.
3. Modificate il file `/etc/openldap/slapd.conf` secondo le vostre esigenze (vedere la Sezione 4.6.1, *Modifica di `/etc/openldap/slapd.conf`* per maggiori informazioni sulla modifica di `slapd.conf`).
4. Avviate `slapd` digitando `/etc/rc.d/init.d/ldap start`. (Dopo aver configurato lDAP in modo corretto, dovreste utilizzare Linuxconf o `ntsysv` per configurare LDAP affinché si avvii con il sistema).
5. Create la vostra directory LDAP (alcuni esempi per le entry LDAP sono disponibili sul sito PADL Software all'indirizzo http://www.padl.com/ldap_examples.html).
6. Aggiungete le entry alla vostra directory LDAP con `ldapadd` o con uno script.
7. Usate `ldapsearch` per verificare che `slapd` funzioni.
8. A questo punto la vostra directory LDAP dovrebbe essere stata creata. Il prossimo passo è quello di configurare le applicazioni abilitate per LDAP in modo che possano utilizzare la directory LDAP.

4.10 Configurazione del sistema per l'autenticazione con OpenLDAP

Questa sezione offre un riepilogo su come configurare il vostro sistema Red Hat Linux per l'autenticazione tramite OpenLDAP. A meno che non siate esperti nell'uso di OpenLDAP, avrete bisogno

di una maggiore documentazione di quella fornita. Per ulteriori informazioni, consultate la Sezione 4.11, *Risorse aggiuntive*.

4.10.1 Installazione dei pacchetti LDAP necessari

Per prima cosa dovrete assicurarvi che vengano installati i pacchetti adeguati sia sul server LDAP che sulle macchine client LDAP. Sul server LDAP è necessario installare il pacchetto `openldap`.

Sulle macchine client LDAP è necessario installare i pacchetti `openldap`, `auth_ldap` e `nss_ldap`.

4.10.2 Modifica dei file di configurazione

Modifica del file `/etc/openldap/slapd.conf`

A questo punto è necessario assicurarsi che il file `slapd.conf` corrisponda alle specifiche della propria organizzazione.

Per maggiori informazioni su come modificare `slapd.conf`, consultate la Sezione 4.6.1, *Modifica di `/etc/openldap/slapd.conf`*.

Modifica del file `ldap.conf`

Modificate i file `ldap.conf` in `/etc` e `/etc/openldap` sul server e i client LDAP.

Modificate `/etc/ldap.conf`, il file di configurazione per `nss_ldap` e `pam_ldap`, in modo da riflettere la vostra base organizzativa e di ricerca. `/etc/openldap/ldap.conf` è il file di configurazione per gli strumenti a linea di comando come `ldapsearch`, `ldapadd` e va modificato per la configurazione del vostro LDAP. Entrambi questi file devono essere modificati per calcolatori client.

Modifica del file `/etc/nsswitch.conf`

Per utilizzare `nss_ldap`, dovete aggiungere `ldap` nei campi corretti in `/etc/nsswitch.conf`. Prestate molta attenzione nel modificare questo file; assicuratevi di sapere cosa fare. Per esempio:

```
passwd: files ldap
shadow: files ldap
group: files ldap
```

PAM e LDAP

Per avere applicazioni PAM standard, utilizzate LDAP per l'autenticazione, eseguite `authconfig` e selezionate **Usa LDAP**. Per maggiori informazioni su PAM, consultate il Capitolo 8, *Moduli di autenticazione PAM* e le relative pagine man.

4.10.3 Adattare il metodo di autenticazione allo standard LDAP

La directory `/usr/share/openldap/migration` contiene un set di script shell e Perl che vi consentono di adattare il vostro metodo di autenticazione al formato LDAP. Per usare questi script, dovrete avere il linguaggio Perl installato sul vostro sistema.

Prima di tutto è necessario modificare il file `migrate_common.ph` in modo che rispecchi il vostro dominio. Il dominio DNS di default dovrebbe essere modificato da:

```
$DEFAULT_MAIL_DOMAIN = "padl.com";
```

a:

```
$DEFAULT_MAIL_DOMAIN = "vostra_società.com";
```

È meglio modificare la base di default:

```
$DEFAULT_BASE = "dc=padl,dc=com";
```

in:

```
$DEFAULT_BASE = "dc=vostra_società,dc=com";
```

Poi, dovete decidere quale script utilizzare. La tabella seguente può fornirvi delle indicazioni:

Tabella 4–1 Script di migrazione LDAP

Name service attuale	LDAP funziona?	Utilizzate questo script:
`/etc` flat files	sì	`migrate_all_online.sh`
`/etc` flat files	no	`migrate_all_offline.sh`
NetInfo	sì	`migrate_all_netinfo_online.sh`
NetInfo	no	`migrate_all_netinfo_offline.sh`
NIS (YP)	sì	`migrate_all_nis_online.sh`
NIS (YP)	no	`migrate_all_nis_offline.sh`

Scegliete lo script adeguato al vostro name service.

I file `README` e `migration-tools.txt` nella directory `/usr/share/openldap/migration` forniscono maggiori dettagli su quanto illustrato sopra.

4.11 Risorse aggiuntive

Sono disponibili molte informazioni utili relative a LDAP. Usate queste risorse, soprattutto visitate il sito Web OpenLDAP e leggete LDAP HOWTO prima di iniziare a usare LDAP sul vostro sistema.

4.11.1 Documentazione installata

- La pagina man di `ldap` è un ottimo punto di partenza per conoscere questo protocollo. Esistono varie pagine man per i diversi demoni e utility di LDAP che forniscono maggiori informazioni relative a `ldapmodify`, `ldapsearch` e simili.
- `/usr/share/docs/openldap-`*`numeroversione`* — contiene un documento generale `README` e informazioni varie.

4.11.2 Siti Web utili

- http://www.openldap.org — pagina principale del progetto OpenLDAP: lo sforzo d'equipe per sviluppare una suite LDAP di applicazioni e tool di sviluppo "robusta, ricca di caratteristiche e open source".
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — un documento LDAP Linux HOWTO che tratta l'installazione attraverso l'autenticazione e la registrazione.
- http://www.padl.com — sviluppi di `nss_ldap` e `pam_ldap`, tra gli altri tool LDAP.
- http://www.innosoft.com/ldapworld — contiene informazioni relative alle specifiche delle RFC LDAP e della versione 3 di LDAP.
- http://www.kingsmountain.com/ldapRoadmap.shtml — la Road Map LDAP di Jeff Hodges contiene link a numerose e utili FAQ e include le news sul protocollo LDAP.
- http://www.rudedog.org/auth_ldap — pagina principale del modulo di autenticazione `auth_ldap` per Apache.
- http://www.stanford.edu/~bbense/Inst.html — illustra l'uso di LDAP con Sendmail.
- http://www.webtechniques.com/archives/2000/05/wilcox — un sito utile per gestire i gruppi in LDAP.
- http://www.ldapman.org/articles — contiene articoli che offrono una buona introduzione a LDAP, tra cui metodi per creare un'alberatura delle directory e personalizzare la struttura delle directory.

4.11.3 Libri correlati

- *Implementing LDAP* di Mark Wilcox; Wrox Press, Inc.
- *Understanding and Deploying LDAP Directory Services* di Tim Howes et al.; Macmillan Technical Publishing

5 CCVS (Principi del Credit Card Verification System)

Il Credit Card Verification System (CCVS, sistema di verifica delle carte di credito) utilizza il computer e il modem per simulare un sistema di gestione delle carte di credito (conosciuto anche come terminale **POS** (**Point Of Sale**). Il prodotto CCVS include diverse API che semplificano la personalizzazione e l'integrazione del sistema con gli applicativi e i database esistenti.

Il prodotto CCVS è un sistema software sicuro e di facile utilizzo. È stato scritto in ANSI C ed è conforme allo standard POSIX, il che lo rende facilmente integrabile con i moderni sistemi applicativi, la maggior parte dei linguaggi di programmazione e Internet. Il CCVS può essere usato per automatizzare le richieste di elaborazione delle carte di credito.

Il sistema CCVS può essere usato fuori dagli Stati Uniti se le banche o i fornitori del servizio supportano un protocollo compatibile con il CCVS. In Canada il CCVS supporta il protocollo NDC che può essere usato da qualsiasi banca per configurare il vostro conto. Nel caso vi troviate in altri stati, contattate il vostro fornitore di servizio. Il protocollo supportato da CCVS più utilizzato è il protocollo Visa 2nd Generation "K Format" (VITAL).

In Red Hat Linux è inclusa una versione demo di CCVS. La versione demo è completamente funzionante e può essere utilizzata per la verifica del sistema CCVS sul vostro calcolatore; la versione demo compie tutte le operazioni tranne il collegamento con l'istituizione finanziaria. Se decidete di acquistare il software CCVS per gestire le carte di credito, contattate Red Hat per acquistare la licenza. Per maggiori informazioni sull'attivazione del CCVS, visitate la pagina Web http://www.redhat.com/products/software/ecommerce/ccvs.

5.1 Utilizzi del CCVS

Il CCVS crea connessioni fra un'applicazione e-commerce e il gateway di pagamento della carta di credito. Mentre le modalità di utilizzo del CCVS dipendono dal protocollo usato dal vostro gateway di pagamento, in molti casi il CCVS può essere usato apportando pochissime modifiche a un sistema esistente. Per informazioni sui diversi protocolli supportati dal CCVS, visitate la pagina Web http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/protocol-specific.html.

Di seguito sono riportati alcuni esempi d'uso del software CCVS:

- Il CCVS supporta un sistema per gli operatori telefonici in modo da poter ricevere gli ordini via telefono. Le estensioni Tcl del CCVS possono essere usate per creare applicazioni grafiche basate su Tcl/Tk che presentano un'interfaccia semplice per l'operatore telefonico. L'operatore utilizza un banale X terminal e tutto il software è in esecuzione sul server centrale. Perciò il sistema CCVS

viene installato su un unico computer. Non è necessario che gli operatori attendano che la linea telefonica sia disponibile perchè può essere condivisa da più transazioni.

- Il CCVS può essere utilizzato per automatizzare la fatturazione clienti. Per esempio, un Internet Service Provider (ISP) può avere un database clienti su un database server. L'amministratore del database dell'IPS può scrivere uno script in Perl per integrare il sistema CCVS con un modulo per il database dell'IPS. Lo script viene eseguito ogni mese e legge i dati del clienti, elabora la fatturazione su base mensile e aggiorna i file del database per indicare che i pagamenti sono stati effettuati.
- Il CCVS può aiutare un negozio online che usa un call center per gli ordini a gestire i pagamenti. In questo modo, gli ordini elaborati sul Web con un'applicazione CGI standard o da un venditore con un programma Java personalizzato che usa la LAN possono utilizzare la stessa connessione per l'elaborazione e il pagamento. Inoltre, il sistema di verifica degli indirizzi (Address Verification System (AVS)) del CCVS previene la frode in entrambi i metodi di ordinazione senza dover implementare questa funzione separatamente in ogni applicazione.

Questi sono solo alcuni esempi d'uso del sistema CCVS. In realtà il CCVS può essere utilizzato per migliorare qualsiasi operazione basata sulla gestione delle carte di credito. Il sistema CCVS include i seguenti aspetti:

- Una libreria C con le API spiegate dettagliatamente per integrare la gestione delle carte di credito con le applicazioni esistenti.
- Un'estensione Tcl per la creazione di applicazioni Tcl (vedere per esempio il sito NeoWebScript).
- Un modulo Perl 5.0 che vi consente di integrare il sistema CCVS con il linguaggio più utilizzato per la creazione di programmi CGI.
- La possibilità di creare velocemente delle interfacce grafiche personalizzate Tcl/Tl— solitamente il tempo di sviluppo è inferiore a un giorno.
- I moduli Python, PHP3 e Java che permettono al CCVS di lavorare con altri linguaggi di programmazione.
- Programmi basati sulle linee di comando per un uso interattivo normalmente utilizzati nella shell di UNIX.
- Protezione AVS contro la frode che vi permette di verificare le informazioni sulla carta di credito. Molte case di clearing offrono riduzioni ai commercianti che usano l'AVS, anche per gli ordini via telefono.
- Assistenza per conti multipli che permette agli utenti di aprire un proprio centro commerciale virtuale comprendente un numero illimitato di negozi. Un **conto commerciante** è un tipo di conto bancario che permette a un'impresa di accettare dai propri clienti pagamenti tramite carta di credito.

- La capacità di gestire più transazioni in un'unica sessione, migliorando le prestazioni della linea (due secondi per transazione!) senza nessun complicazione o costo aggiuntivo.
- La sicurezza di poter verificare ed effettuare programmi di sviluppo sul prodotto senza addebitare veramente il denaro sulle carte di credito.

5.2 Processo di verifica della carta di credito

Come può un piccolo pezzo di plastica indicare al negoziante che vi potete permettere quel televisore?

Prima di tutto, il cliente presenta la carta di credito al commerciante. Successivamente il commerciante trasmette i dati in essa contenuti corredati del suo codice ID alla casa di clearing. La casa di clearing potrebbe essere una banca che ha rilasciato al negoziante l'accesso alla gestione delle carte di credito, ma è più probabile che sia una società che ha un contratto con la banca del negoziante.

I numeri della carta di credito e del negoziante sono trasmessi tramite la linea telefonica utilizzando un terminale POS, il CCVS o qualche altro software che permette di trasmettere le informazioni da un computer.

La casa di clearing contatta la banca che ha rilasciato la carta di credito del cliente e verifica se l'ammontare dell'acquisto può essere accettato. In caso positivo, la casa di clearing invia un messaggio di conferma al commerciante. Contemporaneamente, viene congelato il credito disponibile del cliente per il completamento della transazione.

Al termine della giornata lavorativa, il computer o il terminale per le carte di credito del negoziante contatta la casa di clearing e verifica tutte le transazioni della giornata per accertarsi che il sistema software del negoziante sia allineato con il sistema della casa clearing. Una volta verificate tutte le transazioni, la casa di clearing attiva il processo di trasferimento del denaro dalla banca del cliente al conto corrente bancario del negoziante.

5.3 Requisiti per l'uso di CCVS

Per utilizzare il sistema CCVS, è necessario avere un modem e un conto commerciante. La procedura riportata sotto spiega come attivarlo correttamente.

5.3.1 Modem

I protocolli per la gestione delle carte di credito non supportano né la compressione né la correzione degli errori. Perciò vi possiamo indicare come disabilitare tali caratteristiche per i modem seguenti:

- Hayes Optima
- US Robotics Courier
- US Robotics Sportster

- Chase Research PCI-RAS

Nota Bene

Vi consigliamo di utilizzare uno dei modem presenti in questo elenco!

Se usate un modem non supportato, potrebbe essere difficile far funzionare il sistema CCVS. Dovreste consultare anche l'elenco dell'hardware supportato sul sito http://www.redhat.com/support/hardware/ per verificare che il vostro modem sia compatibile con Red Hat Linux.

Se il modem che avete in dotazione non compare nell'elenco, consultate il manuale tecnico per trovare la stringa che disabilita la compressione e la correzione degli errori e la stringa che reimposta il modem. Queste due stringhe dovranno essere inserite durante la configurazione del CCVS.

5.3.2 Conto commerciante

Se state per impostare il conto commerciante, il fornitore del conto potrebbe richiedervi un certificato di compatibilità CCVS con il protocollo che usa. I certificati sono disponibili alla pagina Web http://www.redhat.com/products/software/ecommerce/ccvs/support/certifications.html. Stampate tutte le pagine corrispondenti al protocollo che desiderate utilizzare e mostratele al fornitore del vostro conto.

Il fornitore del vostro conto commerciante deve utilizzare uno dei protocolli supportati dal CCVS:

- Protocollo ETC PLUS di First Data Corporation (conosciuto comea FDR7, ETC+, ETC7, Omaha)
- Protocollo South Platform di First Data Corporation (conosciuto come Nabanco)
- Protocollo MAPP di Global Payment Systems (conosciuto come St. Louis)
- Protocollo NDC di Global Payment Systems (conosciuto come Atlanta)
- Protocollo VITAL di Visa International (conosciuto come VisaNet, Visa 2nd generation, K format)
- Protocollo UTF di Paymentech (conosciuto come GENSAR)
- Protocollo NOVA Information Systems

Se il fornitore del conto commerciante utilizza uno di questi protocolli, potete usare il sistema CCVS.

Una volta identificato quale protocollo volete utilizzare, consultate la relativa documentazione disponibile nella pagina Web http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/protocol-specific.html prima di iniziare la configurazione del CCVS. La *CCVS Protocol Guide*, disponibile via Web, descrive le funzionalità supportate dai vari protocolli.

5.3.3 Linee guida per l'utilizzo del CCVS

I requisiti presentati in questo paragrafo vi permettono di eseguire il sistema CCVS in modo più efficiente. Accertatevi di seguirli attentamente prima di utilizzare il software CCVS.

Uso esclusivo del modem con il CCVS in esecuzione

Non eseguite altre applicazioni che utilizzano la risorsa modem mentre state utilizzando il CCVS poiché potrebbero interferire con le transazioni per la gestione delle carte di credito.

Autorizzazioni, privilegi e accessi al modem

La maggior parte delle autorizzazioni richieste dal CCVS vengono impostate durante il processo di installazione attraverso la creazione di uno speciale gruppo chiamato ccvs. Tuttavia, dovrete essere al corrente di alcuni aspetti riguardanti le autorizzazioni del sistema e il CCVS. Tali aspetti sono spiegati in questa sezione.

Tutte le operazioni per una particolare configurazione del CCVS devono essere eseguite da un unico conto utente. È necessario disporre di un conto utente per impostare correttamente le proprietà e i permessi dei file. Questo conto deve essere aggiunto al gruppo ccvs prima di eseguire il programma di installazione.

Dopo aver aggiunto l'utente al gruppo ccvs, collegatevi al sistema con la sua login ed eseguite il programma di configurazione di CCVS (`ccvs_configure`). Terminato il programma di configurazione, lo stesso utente deve eseguire i comandi CCVS per la vostra configurazione.

Se volete che CCVS utilizzi un modem, dovete aggiungere il gruppo ccvs al gruppo uucp. Questo non è sufficiente; assicuratevi che il gruppo ccvs abbia accesso alla porta seriale del modem.

Se state utilizzando il PHP con CCVS, dovete abilitare il server Web all'esecuzione dei comandi CCVS. Perciò aggiungete l'utente del server Web al gruppo ccvs. Di solito è necessario aggiungerlo anche al gruppo uucp.

Se non state utilizzando il linguaggio di scripting PHP, ma volete che il server Web possa eseguire le applicazioni CCVS, avete un'altra possibilità (per esempio `suexec`, `setuid`) oltre all'inserimento dell'utente del server Web nel gruppo ccvs.

Versioni del software

Il CCVS richiede la versione 7.0 o una versione più recente di Tcl per eseguire l'interfaccia grafica inclusa o per utilizzare le API Tcl/Tk per sviluppare una propria interfaccia grafica. La versione 8.3 di Tcl è fornita con Red Hat Linux 7.1.

Il CCVS richiede la versione 5.0 o una versione più recente di Perl per poter utilizzare le API Perl allegate. La versione 5.6 di Perl è fornita con Red Hat Linux 7.1.

5.4 Installazione del CCVS

I pacchetti RPM del sistema CCVS sono inclusi nel CD Linux Applications Library Workstation.

Per installare i pacchetti CCVS potete usare RPM, Gnome-RPM o Kpackage:

- `CCVS` — Il nucleo del programma CCVS
- `CCVS-devel` — Il kit di sviluppo per il linguaggio C
- `CCVS-perl` — L'interfaccia Perl per il sistema CCVS
- `CCVS-python` — L'interfaccia Python per il sistema CCVS
- `CCVS-php3` — L'interfaccia PHP3 per il sistema CCVS
- `CCVS-tcl` — L'interfaccia Tcl per il sistema CCVS
- `CCVS-java` — L'interfaccia Java per il sistema CCVS (incluso il codice sorgente)
- `CCVS-examples` — Esempi di codice sorgente, necessari per lo sviluppo

5.5 Prima di configurare il CCVS

Prima di iniziare la configurazione del CCVS, dovete rispondere ad alcune domande sul sistema e su come volete configurare il CCVS. Per prepararvi alla configurazione, seguite questa procedura:

1. Leggete attentamente tutta la documentazione e l'errata fornita con il programma. Per informazioni su dove trovare la documentazione relativa al CCVS, consultate la Sezione 5.11, *Risorse aggiuntive*.
2. Compilate il file `setup.txt`. Il file `setup.txt` è un modulo in cui potete inserire tutte le informazioni relative al protocollo che desiderate utilizzare. Se lo compilate con attenzione, avrete tutte le informazioni necessarie all'installazione del CCVS a portata di mano. Potete trovarlo nella directory `/usr/share/doc/CCVS-<version>` oppure su Internet alla pagina http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/setup.txt.

Nota Bene

Nel modulo vi verranno chieste alcune informazioni relative ai protocolli. Fornite solo le informazioni relative al protocollo che utilizzate e ignorate tutto ciò che riguarda altri protocolli.

---

3. Durante il programma di configurazione del CCVS preparatevi a fornire alcune informazioni sul vostro modem. Di seguito sono riportate le stringhe init per i modem supportati:

Hayes Optima o ACCURA

```
\r~~~\rAT &D3 X4 E0 &K0 &Q0
```

U.S. Robotics Sportster o Courier

```
\r~~~\rAT E0 L0 M1 V1 X4 &K0 &M0 +FCLASS=0
```

Chase Research PCI-RAS

```
\r~~~\rAT E0 %C0 \\N0
```

Se usate un modem supportato, il programma di configurazione vi chiede di confermare la stringa init. Se il vostro modem non compare nell'elenco, consultate il manuale tecnico del modem per conoscere la stringa che disabilita la compressione e la correzione degli errori e la stringa per inizializzarlo.

5.6 Configurazione del CCVS

Dovete configurare il CCVS sia che lo usiate in modalità demo sia che lo usiate per elaborare dati.

Utilizzate il comando `su` per collegarvi con il nome dell'utente che avete creato per il sistema CCVS (questo utente deve appartenere al gruppo ccvs).

Eseguite il programma di configurazione del sistema CCVS con il seguente comando

```
/usr/sbin/ccvs_configure
```

La parte restante di questa sezione descrive il programma di configurazione del CCVS. Una volta che è comparsa la schermata di benvenuto, premete [Invio] per leggere la licenza del software CCVS. Potete usare i comandi standard di `more` per spostarvi durante la lettura della licenza.

Al termine della licenza compare il messaggio:

```
Type "accept" to accept this license, or anything else to exit.
```

Digitate la parola **`accept`** per accettare i termini della licenza e per continuare la configurazione del CCVS. Inserendo qualunque altra parola il programma di installazione termina.

In seguito compare la seguente schermata:

```
This program creates the configuration file for CCVS functions.
To do this, you will require the following information:
 1: The clearing protocol you will be using. This may be MAPP,
ETC+, or any of the other protocols which CCVS supports. There
is also a demo protocol; if you have downloaded the free demo of
CCVS, you will be using the demo protocol.
 2: The unique number which identifies you to the clearing
house. This may be your merchant account number or a terminal id
number, depending on what protocol you will be using. This number
will be supplied when you set up your merchant account.
```

```
 3: Your modem type, and the serial port your modem is attached
to. You will also need modem configuration strings. (We can
supply modem configuration strings for many popular modems.)
 4: The location of your data directory. This is where the
configuration file and data directories will be placed.
 5: Other information as needed for particular protocols. This
information will generally be supplied when you set up your
merchant account.

We supply a worksheet which you can use to organize all this
information, including the details for each protocol. See the
file "setup.txt" in /usr/share/doc/CCVS-<version>.

The configuration program is running as user "<username>".
It is important that this be the same user which the actual CCVS
software will run as. (We recommend creating a special user
account for just this purpose.)

Do you wish to continue configuring CCVS as user "<username>"?

[Enter Y to continue, or N to stop here:]
```

Premete il tasto [Y] per continuare. Se siete collegati come root, riceverete il seguente messaggio di errore. In tal caso, utilizzate il comando `su` per collegarvi con l'utente che avete creato per il sistema CCVS e rieseguite il comando `ccvs_configure`.

```
The configuration program may not be run as root. You must run
this as the same user which the actual CCVS software will run as.
(We recommend creating a special user account for just this
purpose.)
```

In seguito vi compare un prompt per l'inserimento di informazioni. Premendo il tasto **.** (un punto) seguito da [Invio], tornate al prompt precedente.

```
Do you want to configure CCVS for the free demo, or a working
merchant account? (If you have not purchased a license for CCVS,
only the demo configuration is available.)

[Enter Y to use the demo configuration, N for a real configuration,
or . to exit:]
```

Se non avete acquistato la licenza d'uso di CCVS, premete il tasto [Y]. Viene installata una versione demo che offre tutte le funzionalità tranne la connessione via modem. Se invece avete acquistato una licenza d'uso digitate [N].

```
Where do you want to place the CCVS configuration files and
transaction queues? This should be a directory name which is
```

```
writable by the current user.
The default is "/var/ccvs".
Enter directory, or Return for default value, or . by itself to
back up.
>
```

Se non avete necessità specifiche per la posizione dei file di configurazione del CCVS, lasciate la directory di default. Nel caso desideriate installarli in un'altra posizione, dovete impostare una variabile d'ambiente.

```
What do you want to name this configuration? This should be a
short filename.
The default is "ccvs".
Enter name, or Return for default value, or . by itself to back
up.
>
```

Per esempio potete avere una configurazione di nome **`tshirt`** per un negoziante che vende T-shirt e **`music`** per un rivenditore di spartiti musicali. Questi nomi sono utilizzati per distinguere le due configurazioni.

La versione demo del CCVS non richiede nessuna informazione da inserire. Se scegliete questa configurazione, compare il messaggio:

```
Writing "/var/ccvs/ccvs.conf"...

The CCVS system is now configured.
```

Adesso potete iniziare la verifica del software demo. Il software demo ha tutte le funzionalità del software CCVS tranne la possibilità di attivare il modem.

Se avete una licenza per la versione completa del CCVS e avete scelto di effettuare una vera installazione, inserite le informazioni seguenti:

```
Which protocol and merchant processor will you be using?

Credit card clearing protocols:
  1: ETC PLUS (FDR7/ETC7/FDR "Omaha"): First Data Corporation
  2: South Platform (FDR "Nabanco"): First Data Corporation
  3: MAPP: Global Payment Systems "St. Louis"
  4: NDC: Global Payment Systems "Atlanta" / NDC
  5: VITAL (Visa 2nd generation, K format): Visa/Total System Services
  6: UTF: Paymentech Inc.
  7: NOVA: NOVA Information Systems

[Enter a number, or . by itself to back up:]
```

Selezionate il protocollo per il quale avete una licenza e un conto commerciante validi.

```
What is the number of your merchant account?
Enter number, or . by itself to back up.
>
```

Questo numero vi è stato fornito con il vostro conto commerciante.

```
What is your CCVS software customer number?
Enter number, or . by itself to back up.
>
```

Questo numero vi è stato fornito con la licenza CCVS.

```
What is your CCVS software license key?
Enter number, or . by itself to back up.
>
```

Anche questo numero vi è stato fornito con la licenza CCVS.

```
What is the phone number of your merchant processor?
Enter number, or . by itself to back up.
>
```

Potrebbero comparire anche delle richieste aggiuntive in funzione del protocollo che è stato scelto. Se avete compilato il modulo `setup.txt`, è sufficiente consultarlo per trovare le informazioni da inserire. Per esempio il protocollo VITAL richiede varie informazioni come il vostro nome, il vostro indirizzo, la vostra banca ecc. Dovreste già aver raccolto queste informazioni per la creazione del conto commerciante VITAL. Questo è lo scopo di `setup.txt`, che dovreste avere compilato prima di iniziare la configurazione di CCVS. Per informazioni sull'uso di `setup.txt`, consultate la Sezione 5.5, *Prima di configurare il CCVS*.

A questo punto dovete inserire le informazioni per la comunicazione via modem. La configurazione del modem è molto importante. Accertatevi di inserire le informazioni corrette per il vostro sistema! Il CCVS non funziona se il modem non è configurato correttamente.

```
Do you want to configure a pool of several modems? (If you answer
yes, all the modems must be exactly the same make and model. If
you want to use just one modem, answer no.)

[Enter Y or N, or . to back up:]
```

Se avete più modem identici, potete configurare il sistema CCVS per usarli insieme come pool di modem. Ogni processo CCVS che deve usare la risorsa modem utilizza il primo modem libero del pool. Varie configurazioni CCVS possono condividere un gruppo di modem. Potete anche impostare un'unica configurazione con due modem, in modo che le autorizzazioni e l'elaborazione batch avvengano contemporaneamente.

```
What serial port is your modem connected to? (Do not include the
"/dev/" prefix.) The default is ttyS0. The modem should be
connected and ready now, so that the serial port can be tested.

Enter port name, or Return for default value, or . by itself to
back up.
>
```

Il programma verifica la porta seriale che avete selezionato; se ne configurate più di una, le controlla tutte. Non includete la directory `/dev/`. Questo passo può durare anche 30 secondi se il modem non viene rilevato correttamente.

```
What type of modem do you have? This information makes it
possible to suggest modem configuration strings. If your modem
is not listed, you can choose "none of the above"; but you will
then have to create your own configuration strings, which is a
difficult process.

 1: USR Sportster/Courier
 2: Hayes Optima
 3: Chase Research PCI-RAS
 4: None of the above

[Enter a number, or . by itself to back up:]
```

È necessario inserire le stringhe per l'inizializzazione, per la composizione del numero e per interrompere la comunicazione. (Se volete configurare un pool di modem, devono essere identici per utilizzare le stesse stringhe). Se il CCVS riconosce le stringhe per il vostro tipo di modem, allora vengono suggerite a video. Nel caso siano corrette, premete solamente [Invio].

```
The modem initialization string should set the modem to do no
protocol
negotiation. What string do you want to use?
A string which works for your modem is:
 \r~~~\rAT E0 L0 M1 V1 X4 &K0 &M0 +FCLASS=0
Enter string, or Return for suggested value.
>

The modem dial string should dial the modem. (Do not include a
phone number.)
What string do you want to use?
A string which works for your modem is:
 ATDT
Enter string, or Return for suggested value.
>
```

```
The modem hang-up string should hang the modem up if it's
connected. What string do you want to use?
A string which works for your modem is:
 ~~~+++~~~~~~~~~\rATH0\r~~~
Enter string, or Return for suggested value.
>

Initialize: \r~~~\rAT E0 L0 M1 V1 X4 &K0 &M0 +FCLASS=0
Dial: ATDT
Hang up: ~~~+++~~~~~~~~~\rATH0\r~~~
Are these the values you want?

[Enter Y to accept, N to change, . to back up.]
```

Sono esempi di messaggi che compaiono a video. Potrebbero essere diversi se avete un altro tipo di modem.

La prossima domanda riguarda la frequenza di baud del modem:

```
What baud rate do you want to use? You should use the
default unless you have explicit information that another
value is appropriate.
The default baud rate is 1200.

Enter rate, or Return for default value, or . by itself to
back up.
>
```

Dopo aver inserito le informazioni sulla configurazione del modem, compare:

```
Writing "/var/ccvs/ccvs.conf"...

The CCVS system is now configured.
```

5.7 Conti commerciante multipli

Se dovete gestire più conti, rieseguite la procedura di configurazione. Utilizzate un nome diverso per la configurazione di ogni conto.

La stessa porta seriale può essere condivisa per più di una configurazione. I modem vengono utilizzati nell'ordine di avvio.

5.8 Avvio del CCVS

Per usare il CCVS con una specifica applicazione, avete bisogno di collegarvi con la login dell'utente che ha creato la configurazione. Se state usando un conto utente ccvs e siete collegati al sistema con la login di un'altro utente, digitate `su ccvs` per passare all'utente giusto.

Per utilizzare il CCVS, dovete attivare il demone `ccvsd` per ogni account ed eseguire periodicamente il programma `cvupload`. (Va benissimo tramite `cron` una volta al giorno.) Per istruzioni relative ai processi automatici, consultate le pagine man di `cron`.

5.8.1 Il demone ccvsd

Per utilizzare il CCVS, dovete eseguire il demone `ccvsd`. Questo demone si occupa di attivare la linea telefonica e di gestire le transazioni. Il demone `ccvsd` deve essere eseguito con i diritti dell'utente che avete creato durante la configurazione del conto.

Per esempio, se volete attivare la gestione delle transazioni del rivenditore di spartiti menzionato nel programma di configurazione, e se avete installato il programma nella directory di default `/usr/sbin`, potete digitare il seguente comando:

```
/usr/sbin/ccvsd music
```

Ogni volta che aggiungete un conto commerciante, dovete eseguire il demone `ccvsd` per attivare la gestione delle transazioni per il nuovo conto.

Per maggiori informazioni su `ccvsd`, consultate la pagina man di `ccvsd`.

5.8.2 Il comando cvupload

Alcune transazioni (per es. le autorizzazioni) avvengono alla presentazione della carta di credito. Altre invece (per es. le vendite) vengono salvate ed elaborate in un secondo momento. Queste transazioni sono elaborate in gruppo secondo una modalità batch.

Il CCVS usa il programma `cvupload` per l'elaborazione in modalità batch. Perciò vi consigliamo di eseguire giornalmente il comando `cvupload` tramite il programma `cron` affinché ogni giorno vengano completate tutte le transazioni.

Per esempio, il comando per l'elaborazione periodica per il rivenditore di spartiti è il seguente:

```
/usr/sbin/cvupload music
```

Per maggiori informazioni sul programma `cvupload`, consultate la pagina man di `cvupload`.

5.9 Considerazioni sui linguaggi

- C — La libreria C di CCVS è inclusa nel pacchetto `CCVS-devel`. Durante la compilazione di programmi C che usano il sistema CCVS, aggiungete il flag `-lccvs` al linker.
- Java — Consultate la pagina Web http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/AdminJava.html per maggiori informazioni sulla costruzione dell'interfaccia Java di CCVS. Il codice sorgente per l'interfaccia Java è incluso nel pacchetto `CCVS-java`.
- Perl — L'interfaccia Perl è inclusa nel pacchetto `CCVS-perl`.
- Python — L'interfaccia Python è inclusa nel pacchetto `CCVS-python`.
- PHP — L'interfaccia PHP3 è inclusa nel pacchetto `CCVS-php3`.
- Tcl — L'interfaccia Tcl è inclusa nel pacchetto `CCVS-tcl`.

5.10 Assistenza per il sistema CCVS

L'assistenza per il CCVS può essere acquistata da Red Hat. Quando acquistate la chiave per attivare il sistema CCVS, accertatevi che l'assistenza sia disponibile. Consultate la pagina Web http://www.redhat.com/products/software/ecommerce/ccvs per maggiori informazioni sull'acquisto di una chiave e sull'assistenza disponibile per il CCVS.

Nel caso vi rivolgiate all'assistenza, dovete specificare le informazioni seguenti:

- Il nome della vostra azienda
- La versione di CCVS che state utilizzando
- Il vostro numero commerciante
- Il vostro numero cliente CCVS
- Il vostro sistema operativo e la relativa versione

Il supporto tecnico Red Hat si impegna a rispondere alle richieste riguardanti il sistema CCVS. Comunque non possiamo fornire assistenza per prodotti commerciali di altre aziende, eccetto per problemi riguardanti l'integrazione con il sistema CCVS.

5.11 Risorse aggiuntive

Sono disponibili ulteriori informazioni sul CCVS.

5.11.1 Documentazione installata

- `/usr/share/doc/CCVS-<numero-versione>` — Contiene i file `CHANGES`, `LICENSE` e `README` nonché il file `setup.txt` utile per raccogliere le informazioni necessarie prima di iniziare la configurazione.
- Digitate `man ccvs` per ottenere una descrizione dei vari stadi di una transazione, i codici di errore di CCVS e altro ancora. Le pagine man di `ccvsd`, `cvreport` e `cvupload` descrivono varie opzioni utilizzabili con questi comandi.

5.11.2 Siti Web utili

- http://www.redhat.com/products/software/ecommerce/ccvs — Da questa pagina potete accedere a varie risorse CCVS, fra cui domande ricorrenti (FAQ), specifiche techniche e informazioni generali sul CCVS.
- http://www.redhat.com/products/software/ecommerce/ccvs/support/documentation.html — Contiene link a guide che riportano diversi modi di utilizzare CCVS. Questi manuali online spiegano tutto, dall'installazione alla configurazione del CCVS e contengono una descrizione completa degli API per le varie lingue utilizzabili.

6 Sendmail

6.1 Introduzione a Sendmail

Sendmail è un **mail transfer agent** (**MTA**) utilizzato su Internet. Gestisce un'alta percentuale di tutte le e-mail che viaggiano su Internet, trasferendole da un host all'altro. Esistono altri MTA (e possono essere usati senza problemi con Red Hat Linux), ma la maggior parte degli amministratori di sistema preferisce usare Sendmail, per via della sua potenza, scalabilità e compatibilità con gli standard di Internet.

Il compito principale di Sendmail, come quello di altri MTA è di muoversi in modo sicuro tra gli host, utilizzando di solito il **Simple Mail Transfer Protocol** (**SMTP**). Tuttavia Sendmail è altamente configurabile, e vi consente così di controllare la maggior parte degli aspetti sulla gestione della posta elettronica.

Si può far risalire Sendmail alla nascita della posta elettronica, avvenuta nel decennio precedente alla creazione di ARPANET, il precursore di Internet. A quei tempi, la casella postale di ogni utente consisteva in un file di sola lettura, in cui le applicazioni di posta aggiungevano semplicemente del testo. Ogni utente doveva scorrere tutto il file di posta per trovare vecchie e-mail e leggere i nuovi messaggi era un'impresa non da poco. Il primo vero trasferimento di un file contenente un messaggio di posta avvenne nel 1972, quando le e-mail cominciarono a essere trasferite via FTP sul protocollo di rete NCP. Questo semplice metodo di comunicazione si diffuse rapidamente, al punto da costituire la maggior parte del traffico di ARPANET in meno di un anno. Comunque, la mancanza di protocolli standardizzati, rendeva molto difficile la trasmissione da alcuni sistemi, fino a quando nel 1982 ARPANET si avvalse di TCP/IP. Nacque poi un nuovo protocollo, SMTP, per la trasmissione dei messaggi. Queste innovazioni insieme al fatto che tutti i file host vennero sostituiti con il DNS, consentirono la nascita degli MTA. Sendmail, nato da un sistema di consegna della posta elettronica chiamato Delivermail, divenne ben presto lo standard in concomitanza con il continuo diffondersi di Internet.

È importante conoscere le funzioni di Sendmail, per rendersi conto di ciò che è in grado di fare. In questi tempi caratterizzati da applicazioni "monolitiche" che soddisfano vari ruoli, potreste pensare che Sendmail è l'unica applicazione che vi occorre per avviare un server e-mail all'interno della vostra organizzazione. Tecnicamente è vero, poiché Sendmail può memorizzare la posta nelle directory utente e accettare nuova posta tramite la linea di comando. Gli utenti in realtà richiedono molto più della semplice consegna di posta. Quasi sempre desiderano interagire con la posta utilizzando il **mail user agent** (**MUA**) che si avvale del **Post Office Protocol** (**POP**), dell'**Internet Message Access Protocol** (**IMAP**) o perfino del Web. Questi protocolli possono funzionare insieme a Sendmail e SMTP, ma in realtà sono stati creati per ragioni differenti e possono funzionare singolarmente.

Enumerare tutte le funzioni per cui potrebbe essere configurato Sendmail esula dall'obiettivo di questo capitolo. Se però l'argomento vi interessa, consultate le numerose fonti di informazioni online e offline, con cui potrete capire quali file vengono installati per default con Sendmail, sapere come

modificare la configurazione di base, imparare come bloccare la posta indesiderata (spam) e ampliare Sendmail grazie al **Lightweight Directory Access Protocol** (**LDAP**).

6.2 Installazione predefinita di Sendmail

Sebbene sia possibile scaricare il codice sorgente di Sendmail e crearsi la propria copia, molti utenti preferiscono procurarsi Sendmail tramite l'RPM da CD-ROM (al momento dell'installazione di Red Hat Linux o successivamente).

Sendmail si trova nella directory `/usr/sbin`.

`sendmail.cf` il file di configurazione di Sendmail, lungo e dettagliato, è installato nella directory `/etc`. Si consiglia di non modificare direttamente il file `sendmail.cf` per via della sua complessità e lunghezza. Invece, per cambiare la configurazione di Sendmail, modificate il file `/etc/mail/sendmail.cf` e usate il macroprocessore `m4` per creare un nuovo `/etc/sendmail.cf` (dopo aver eseguito un backup dell'originale, ovviamente). Maggiori informazioni sulla configurazione di Sendmail sono contenute nella Sezione 6.3, *Modifiche della configurazione*.

Molti file di configurazione di Sendmail sono installati in `/etc/mail`, tra cui:

- `access` — indica quali sistemi possono utilizzare Sendmail.
- `domaintable` — vi consente di fornire la mappa del nome del dominio.
- `local-host-names` — indica la posizione dove si trovano tutti gli alias del vostro sistema.
- `mailertable` — elenca le istruzioni che annullano l'instradamento di domini particolari.
- `virtusertable` — vi permette di creare una forma di aliasing specifica per il dominio, autorizzando domini virtuali multipli su una sola macchina.

Molti file di configurazione `/etc/mail`, come per esempio `access`, `domaintable`, `mailertable` e `virtusertable`, devono archiviare le proprie informazioni in file database prima che Sendmail possa utilizzare qualsiasi modifica della configurazione. Per memorizzare queste modifiche nei file database, è necessario eseguire un comando con la seguente sintassi: `makemap hash /etc/mail/`*`nome`* `</etc/mail/`*`nome`*, dove *nome* va sostituito con il nome del file di configurazione da convertire.

Per esempio, se desiderate che tutta la posta indirizzata a un qualsiasi account `domain.com` venga inviata a `luca@altrodominio.com`, è necessario aggiungere una riga al file `virtusertable`:

```
@domain.com        luca@altrodominio.com
```

In seguito, per aggiungere questa nuova informazione al file `virtusertable.db`, eseguite `makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable` come utente root. In questo modo viene creato un nuovo file `virtusertable.db` che contiene la nuova configurazione.

6.3 Modifiche della configurazione

Nella directory `/etc` viene installato il file di default `sendmail.cf`. La configurazione predefinita dovrebbe funzionare per la maggior parte dei siti SMTP. *Non* funziona invece per i siti UUCP (UNIX to UNIX Copy). Se vi serve utilizzare i trasferimenti di posta UUCP, generate un nuovo file `sendmail.cf`.

Nota Bene

Nonostante i server SMTP siano supportati in modo automatico, i server **IMAP** (Internet Message Access Protocol) non lo sono. Se il vostro ISP usa un server IMAP al posto di uno SMTP, è necessario installare il pacchetto IMAP. Senza di questo il vostro sistema non è in grado di sapere come trasferire le informazioni al server IMAP o come recuperare la posta.

Se dovete generare un nuovo file `/etc/sendmail.cf` per configurare Sendmail, dovreste utilizzare il macroprocessore `m4`. Qualora dobbiate modificare `/etc/mail/sendmail.mc` per aggiungere nuove funzioni a Sendmail, eseguite il backup dell'attuale `/etc/sendmail.cf` e createne uno nuovo eseguendo il comando `m4 /etc/mail/sendmail.mc > /etc/sendmail.cf`. Aggiungete poi tutte le modifiche precedenti dal file di backup `/etc/sendmail.cf` a quello nuovo. Dopo aver creato un nuovo `/etc/sendmail.cf`, è necessario riavviare Sendmail per renderlo attivo. Il modo più semplice per farlo è digitare, come utente root, il comando `/sbin/service sendmail restart`.

`m4` è il macroprocessore installato di default con Sendmail. `m4` è compreso nel pacchetto `sendmail-cf`, installato in `/usr/lib/sendmail-cf`.

Dovreste consultare il file `/usr/lib/sendmail-cf/README` prima di modificare qualsiasi file nella directory `/usr/lib/sendmail-cf`, poiché possono condizionare la configurazione futura dei file `/etc/sendmail.cf`.

Non utilizzate Linuxconf per configurare Sendmail! Il modulo `mailconf` di Linuxconf, ideato per rendere più semplice la modifica di `/etc/sendmail.cf`, contiene informazioni obsolete circa le regole utilizzate nella configurazione di Sendmail.

Una configurazione standard di Sendmail prevede l'uso di un singolo elaboratore come gateway di posta per tutti gli altri computer in rete. Per esempio: una società desidera che un elaboratore chiamato `mail.bigcorp.com` gestisca tutta la posta. È necessario aggiungere su questa macchina solo i nomi dei computer, per i quali `mail.bigcorp.com` invierà la posta a `/etc/mail/local-host-names`. Ecco un esempio:

```
# sendmail.cw - include all aliases for your machine
# here.
torgo.bigcorp.com
poodle.bigcorp.com
devel.bigcorp.com
```

Sugli altri elaboratori `torgo`, `poodle` e `devel`, va ora modificato il file `/etc/sendmail.cf` per il "mascheramento", come avviene per `mail.bigcorp.com` quando invia la posta. In questo modo l'elaborazione di tutta la posta locale viene inviata a `bigcorp.com`. Modificate le righe `DH` e `DM` nel file `/etc/sendmail.cf` nel seguente modo:

```
# a chi invio nomi non qualificati
# (zero significa invio a livello locale)
DRmail.bigcorp.com

# chi riceve tutto il traffico di posta locale
DHmail.bigcorp.com

# per chi eseguo il mascheramento (zero in caso di nessun mascheramento)
DMbigcorp.com
```

Con questo tipo di configurazione, `bigcorp.com` è l'unico elaboratore ad aver inviato tutta la posta e ogni messaggio inviato a `torgo.bigcorp.com` ad altri host verrà spedito a `mail.bigcorp.com`.

Ricordatevi che se configurate il sistema in modo da "assumere l'identità" di un altro sistema, qualsiasi e-mail inviata al vostro sistema, arriverà in realtà al sistema che state mascherando. Se per esempio alcuni file di log vengono inviati periodicamente a `root@poodle.bigcorp.com` dal demone `cron`, arriveranno sempre a `root@mail.bigcorp.com`.

6.4 Blocco degli spam

Per **spam** si intende di solito un messaggio di posta indesiderato ricevuto da un utente che probabilmente non conosce il mittente e che non ha mai richiesto tale comunicazione. Si tratta di un vero e proprio abuso degli standard di comunicazione di Internet.

Per fortuna Sendmail è in grado di bloccare le nuove tecniche di spamming. Già di default blocca molti dei metodi di spamming più diffusi, così per poter ricevere gli spam dovrete attivarli di proposito modificando il file `/etc/mail/sendmail.cf`. L'opzione per l'invio di messaggi SMTP, per

esempio, è disattivato di default dalla versione 8.9 di Sendmail. Nelle versioni precedenti Sendmail avrebbe consentito al vostro host di posta (`x.org`) di accettare messaggi da una parte (`y.com`) e di inviarli a una terza parte (`z.net`). Ora invece, è necessario specificare a Sendmail di autorizzare un dominio a recapitare posta al vostro dominio. Modificate semplicemente `/etc/mail/relay-domains` e riavviate Sendmail, digitando come root il comando `/sbin/service sendmail restart` per attivare le modifiche.

Comunque, spesso accade che gli utenti siano bombardati da spam provenienti da altri server su Internet che non è possibile controllare. In questi casi, potete utilizzare l'opzione relativa al controllo dell'accesso tramite il file `/etc/mail/access`. Collegatevi come utente root e aggiungete i domini che desiderate bloccare o a cui volete consentire l'accesso, per es.:

```
badspammer.com       550 Go away and don't spam us anymore
tux.badspammer.com   OK
10.0                 RELAY
```

`/etc/mail/access` è un database, quindi è necessario utilizzare makemap per attivare le modifiche, ricreando la mappa del database. Per farlo collegatevi come utente root ed eseguite il comando `makemap hash /etc/mail/access < /etc/mail/access`.

Questo esempio mostra che qualsiasi e-mail inviata da `badspammer.com` al vostro elaboratore, viene bloccata con un codice di errore 550 RFC 821 e il messaggio viene rinviato al mittente. Viene accettata solo la posta inviata dal sottodomino `tux.badspammer.com`. L'ultima riga mostra che tutta la posta inviata dalla rete 10.0.*.* può essere ricevuta dal server di posta.

Come avrete già capito, questo esempio è solo la punta dell'iceberg di quanto Sendmail può fare in termini di autorizzazione o blocco dell'accesso. Per informazioni ed esempi più dettagliati, consultate`/usr/share/doc/sendmail/README.cf`.

6.5 Uso di Sendmail con LDAP

Come già illustrato nel Capitolo 4, *LDAP (Lightweight Directory Access Protocol)*, il protocollo LDAP è un modo molto veloce e potente per trovare informazioni specifiche su un particolare utente in un gruppo molto più ampio. Potreste utilizzare, per esempio, un server LDAP per cercare un indirizzo e-mail particolare in una directory comune aziendale, inserendo il cognome dell'utente. In questo tipo di implementazione LDAP risulta molto diverso da Sendmail: LDAP archivia le informazioni gerarchiche sugli utenti e Sendmail riceve solo i risultati delle richieste di LDAP in messaggi e-mail pre-indirizzati.

Tuttavia, Sendmail supporta un'integrazione maggiore con LDAP, quando lo utilizza per sostituire file come `aliases` e `virtusertables`, su server di posta diversi che funzionano insieme per offrire supporto ad aziende medio-grandi. In breve, è possibile utilizzare LDAP per riunire il livello di instradamento della posta di Sendmail e i diversi file di configurazione in un potente cluster LDAP, potenziato da molte applicazioni diverse.

L'attuale versione di Sendmail contiene il supporto per LDAP. Per ampliare il server Sendmail utilizzando LDAP, procuratevi prima un server LDAP, come OpenLDAP, configurato in modo corretto. Poi, è necessario modificare il file `/etc/mail/sendmail.mc` per includere:

```
LDAPROUTE_DOMAIN('vostrodominio.com')dnl
FEATURE('ldap_routing')dnl
```

Nota Bene

Si tratta solo di una configurazione di base di Sendmail con LDAP. La vostra configurazione dovrà essere molto diversa da questa in base all'implementazione di LDAP, soprattutto se desiderate configurare Sendmail su diverse macchine per utilizzare un server LDAP comune.

Per informazioni ed esempi più dettagliati sulla configurazione di LDAP, consultate `/usr/share/doc/sendmail/README.cf`.

In seguito ricreate il file `/etc/sendmail.cf` eseguendo il comando `m4` e riavviando Sendmail. Per maggiori istruzioni su come ricreare il file, consultate il Sezione 6.3, *Modifiche della configurazione*.

Il Capitolo 4, *LDAP (Lightweight Directory Access Protocol)* contiene ulteriori informazioni su LDAP.

6.6 Risorse aggiuntive

All'inizio molti utenti trovano difficile configurare Sendmail, per via delle numerose opzioni disponibili. La documentazione aggiuntiva su Sendmail può senz'altro aiutarvi nell'impostare le opzioni di configurazione.

6.6.1 Documentazione installata

La migliore fonte di informazione su come configurare Sendmail è contenuta nei pacchetti `sendmail` e `sendmail-cf`.

- `/usr/share/doc/sendmail/README.cf` — contiene informazioni relative a `m4`, la posizione dei file per Sendmail, i mailer supportati, il modo per accedere alle opzioni avanzate e molto altro.
- `/usr/share/doc/sendmail/README` — contiene informazioni sulla struttura delle directory di Sendmail, il supporto per il protocollo IDENT, i dettagli sui permessi delle directory e i problemi comuni causati da questi permessi se configurati in modo errato.

6.6.2 Siti Web utili

- http://www.sendmail.net — novità, interviste e articoli relativi a Sendmail. Offre un'ampia panoramica delle numerose opzioni disponibili.
- http://www.sendmail.org — mostra una classificazione tecnica dettagliata delle caratteristiche di Sendmail e illustra esempi di configurazione.

6.6.3 Libri correlati

- *Sendmail* di Bryan Costales e Eric Allman et al, O'Reilly & Associates — un buon libro di riferimento su Sendmail scritto con la partecipazione del creatore di Delivermail e Sendmail.

Parte II La sicurezza

7 Compendio sulla sicurezza di Red Hat Linux

Oltre all'installazione e alla configurazione di Red Hat Linux è di estrema importanza assicurare al vostro sistema un livello adeguato di sicurezza, in base al suo ruolo, importanza e uso. La sicurezza è un tema molto complesso che comprende il costante emergere di problemi, effettivi o potenziali.

Molti amministratori di sistemi commettono l'errore di occuparsi solo di problemi minori e isolati, lasciandosi sfuggire quelli maggiori e più pericolosi: questo per via della natura amorfa e intricata di tali problemi. Garantire la sicurezza del sistema va ben oltre l'installazione dell'ultimo aggiornamento o la configurazione di un determinato file oppure il controllo attento dell'accesso alle risorse di sistema da parte degli utenti. È un modo di osservare le diverse minacce al sistema e di determinare le misure idonee per prevenirle o combatterle.

Nessun sistema è completamente al sicuro, a meno che non sia spento (e anche in questo caso può comunque essere rubato). Quando il sistema è acceso, è vulnerabile agli attacchi, da scherzi innoqui a virus distruttori di hardware fino alla cancellazione di dati. Ma non tutto è perduto. Con la giusta prospettiva e gli strumenti adatti, potrete assicurarvi molti anni di tranquillità. Nelle prossime sezioni viene delineato un modo per affrontare il problema della sicurezza e le potenziali minacce, vengono inoltre illustrati i diversi strumenti per la sicurezza, i costi e i vantaggi nell'utilizzarli con Red Hat Linux.

7.1 L'inevitabile dilemma sulla sicurezza

Tutti gli utenti di qualsiasi sistema operativo devono affrontare un dilemma comune durante la creazione di un modello di sicurezza per il proprio sistema. Da un lato, evitano di rendere il sistema talmente sicuro da impedirgli di eseguire in modo corretto qualsiasi cosa. Ma dall'altro lato, evitano di rendere il sistema così poco sicuro da permettere che chiunque possa accedervi e fare ciò che vuole, anche cancellare il lavoro di altri o peggio ancora.

Non esiste un modo corretto per risolvere questo dilemma. Alcuni sistemi, per via del loro scopo o dell'importanza dei dati che proteggono, propendono verso una soluzione del dilemma, mentre altri sistemi, per via dei numerosi utenti da cui sono utilizzati o del fatto che sono elaboratori test, propendono verso l'altra soluzione.

Nel configurare la sicurezza del sistema, il passo più importante da eseguire è determinare da che lato del dilemma sulla sicurezza propende il vostro sistema. A volte questo compito è affidato alla politica aziendale. Oppure siete dei ricercatori che lavorano su un sistema non collegato a reti pubbliche e quindi nessuno, all'infuori di voi, ha accesso fisico all'elaboratore. Oppure siete utenti privati collegati con una connessione a banda larga e (giustamente) preoccupati dei modi in cui utenti malintenzionati in tutto il mondo possano danneggiare i vostri dati.

Indipendentemente dagli innumerevoli scenari possibili in cui potete trovarvi, avete la responsabilità di stabilire la misura adatta di "esposizione" al rischio in funzione degli obiettivi che il vostro sistema deve realizzare. Poi, una volta stabilita tale misura, cercate di configurare e mantenere le direttive di sicurezza per il vostro sistema.

7.2 Approccio attivo contro approccio passivo

È sempre possibile dividere gli approcci al problema della sicurezza in due tipi: **attivo** o **passivo**. Un approccio **attivo** verso la sicurezza comprende tutte le azioni compiute per prevenire una falla nel vostro modello di sicurezza del sistema. Un approccio **passivo** invece comprende le azioni compiute per controllare la sicurezza del sistema basandosi sul modello di sicurezza.

Tutti gli utenti dovrebbero utilizzare entrambi gli approcci, poiché si rafforzano a vicenda. Il fatto di scoprire, grazie alle registrazioni del server, che un particolare utente sta cercando di penetrare nel vostro sistema (approccio passivo) può indurvi a installare un'applicazione per impedirgli di arrivare al prompt del login (approccio attivo). Allo stesso modo, il fatto che non usiate le password shadow per proteggere il vostro sistema (approccio attivo), può indurvi a modificare i file chiave del vostro sistema con l'utilizzo di un tool come Tripwire (approccio passivo). Per maggiori informazioni su Tripwire, consultate Capitolo 10, *Installazione e configurazione di Tripwire*.

Red Hat Linux contiene numerosi strumenti per aiutarvi con l'implementazione di entrambi gli approcci verso la sicurezza. Tuttavia, per impedire una dipendenza eccessiva dagli strumenti che proteggono il sistema, è di fondamentale importanza l'uso corretto dei metodi con ogni tipo di approccio.

7.2.1 Strumenti e metodi per un approccio attivo alla sicurezza

La maggior parte dei tool per garantire la sicurezza di Red Hat Linux ha la funzione di proteggere attivamente il sistema. Sono qui elencati alcuni dei tool open source più comuni e utili:

- *Utility shadow* — una serie di tool per gestire gli utenti e i gruppi locali su un sistema che usa password cifrate.
- *Kerberos 5* — un sistema sicuro che fornisce servizi di autenticazione di rete. Impedisce l'uso di password ovvie trasmesse su una rete per accedere a servizi Per maggiori informazioni relative a Kerberos 5, consultate il Capitolo 9, *Kerberos 5 su Red Hat Linux*.
- *OpenSSL* — vi aiuta a proteggere numerosi servizi che supportano le operazioni su un livello di crittografia. Per maggiori informazioni su OpenSSL, consultate la *Official Red Hat Linux Customization Guide*.
- *OpenSSH* — una serie di utility che possono sostituire facilmente tool tanto diffusi quanto poco sicuri come `telnet` e `ftp` con tool potenti e sicuri come `ssh` e `scp`. Per maggiori informazioni su OpenSSH, consultate la *Official Red Hat Linux Customization Guide*.

Sono elencati qui di seguito le azioni che supportano un approccio attivo:

- *Limitare il numero degli utenti che possono eseguire i comandi come root* — un'alta percentuale di tutti i problemi di sicurezza derivano, almeno in modo indiretto, da utenti che conoscono la password di root oppure autorizzati tramite `sudo` a eseguire comandi al livello di root.
- *Sapere quali software sono installati sul vostro sistema e rimanere aggiornati sulla scoperta di nuove "falle" nel sistema* — se infatti non sapete quali pacchetti sono installati sul vostro sistema, non potrete tenervi aggiornati e se non controllate le fonti di informazione, come Red Hat Network non saprete mai se dovete aggiornare i pacchetti.
- *Limitare al minimo i servizi in esecuzione sul sistema* — in sostanza, più servizi avete, maggiore è il pericolo di un accesso non autorizzato. Risparmiate le risorse di sistema (e il problema di mantenere servizi che non usate) e rimuovete i pacchetti che non usate. Infine, eseguite un tool come `ntsysv` per impedire che servizi non necessari vengano attivati all'avvio del sistema. Vedere la sezione *Controllo dell'accesso ai servizi* nella *Official Red Hat Linux Customization Guide*.
- *Richiedere agli utenti di creare password sicure e di modificarle spesso* — la maggior parte dei problemi di sicurezza sono causati da accesso non autorizzato al sistema. Si può ridurre questo rischio richiedendo agli utenti di utilizzare metodi di sicurezza attivi per proteggere le loro "chiavi" al vostro sistema.
- *Assicurarsi che i permessi ai file non siano aperti quando non è necessario* — quasi nessun file dovrebbe essere modificabile da tutti.

7.2.2 Strumenti e metodi per un approccio passivo alla sicurezza

Sebbene la maggior parte dei tool per Red Hat Linux siano ideati per un approccio attivo, esistono alcuni strumenti che rendono la sicurezza passiva un "fardello" amministrativo meno pesante:

- *Tripwire* — un'applicazione ideata per avvertirvi se i file e le directory di sistema specificati sono stati modificati. In questo modo saprete se utenti non autorizzati hanno accesso al vostro sistema o se utenti autorizzati effettuano modifiche non necessarie a file importanti. Per maggiori informazioni su Tripwire, consultate il Capitolo 10, *Installazione e configurazione di Tripwire*.
- *COPS* — una serie di tool per la sicurezza ideati per numerose funzioni, dal controllo delle porte aperte su un host specifico alla verifica delle password utente facilmente individuabili.

Qui di seguito sono elencati i metodi che supportano un approccio passivo alla sicurezza:

- *Effettuare controlli sistematici dei log di sistema* — Red Hat Linux è impostato di default per raccogliere una quantità enorme di dati utili nei log di sistema che si trovano nella directory `/var/log`, soprattutto nel file `messages`. Un'attività semplice eseguita come utente root, per esempio la stringa `grep "session opened for user root" /var/log/messages | less`, vi consente di effettuare una verifica parziale del vostro sistema e di controllare

chi sta accedendo al sistema come root. Ciò vi consente, per esempio, di ridurre velocemente il numero di utenti possibili che potrebbero aver modificato un determinato file modificabile solo da root, paragonando l'ora in cui il file in questione è stato modificato con l'ora dei vari login contenuta nel file `/var/log/messages`. Comunque, ricordatevi che questo metodo non è infallibile, perché chi ha l'autorizzazione a modificare un file di sistema tanto importante, probabilmente ha anche i permessi per modificare il file `/var/log/messages` e cancellare così le proprie tracce.

7.3 Sviluppo delle politiche di sicurezza

Ogni sistema, dal calcolatore utilizzato per uso privato al server aziendale usato da migliaia di utenti, dovrebbe seguire una politica di sicurezza. Per politica di sicurezza si intende una serie di indicazioni utilizzate per giudicare se un'attività o un'applicazione deve essere effettuata o utilizzata su un sistema, in base agli obiettivi particolari di quel sistema.

Le politiche di sicurezza possono variare molto a seconda dei sistemi usati, ma la cosa più importante è ricordarsi che ne esiste una per il proprio sistema, che sia scritta oppure no nel manuale delle politiche aziendali.

Tutte le politiche di sicurezza dovrebbero essere create utilizzando le regole di base seguenti:

- *Semplicità* — più la politica di sicurezza è semplice e diretta, maggiore è la probabilità che le indicazioni vengano seguite e che la sicurezza del sistema venga garantita.
- *Facilità di applicazione* — i metodi e i tool di sicurezza, come ogni cosa, sono soggetti a modifiche, dettate soprattutto da nuove sfide e necessità. La vostra politica di sicurezza dovrebbe essere ideata in modo da ridurre al minimo l'impatto delle modifiche sul sistema e sugli utenti.
- *Promuovere la libertà tramite la fiducia nell'integrità del sistema* — evitate metodi e tool di sicurezza che diminuiscono inutilmente l'uso del vostro sistema per renderlo più sicuro. Esistono infatti metodi e tool di qualità che rendono il sistema più sicuro, ma offrono al contempo, quando possibile, una campo di azione più ampio per gli utenti.
- *Riconoscere la possibilità di errori* — il modo migliore per incorrere in un problema di sicurezza è quello di aver troppa fiducia nelle proprie capacità. Dunque non dormite sugli allori, ma siate sempre vigili.
- *Concentrarsi sui problemi concreti e tralasciare quelli teorici* — impiegate tempo e sforzi gestendo i problemi più importanti. Ponetevi delle priorità e tappate prima le "falle" maggiori. Per stabilire cosa controllare prima, consultate la pagina Web http://www.sans.org/topten.htm o siti simili dove sono elencati problemi di sicurezza specifici che costituiscono davvero una minaccia e dove vedere che cosa fare per evitarli o risolverli.
- *Prontezza* — stabilite quali sono i problemi e determinate se costituiscono un rischio. Non perdete tempo pensando di poter rimandare. Quello che conta è il presente, soprattutto quando il vostro sistema è in pericolo.

Se pensate che la vostra politica di sicurezza sia talmente restrittiva da impedire che il sistema possa essere utilizzato per lo scopo prefisso, non esitate a modificare la politica per allentare l'accesso al sistema. Allo stesso modo, se pensate che la sicurezza del sistema venga continuamente compromessa, dovreste modificare alcuni aspetti della vostra politica per restringere l'accesso. Soprattutto però, ricordate che una politica di sicurezza non è un'idea o un documento statico e quindi va modificata con il cambiare degli obiettivi e degli utenti. Riconsiderate sempre la vostra politica alla luce di nuovi requisiti.

7.4 Ulteriori passi per la protezione del sistema

Molti utenti basano la maggior parte della propria politica di sicurezza sul numero di utenti che hanno l'accesso root al sistema. Questo è sicuramente un primo passo fondamentale, ma per rendere il sistema sicuro occorre molto di più. Le questioni sulla sicurezza si intrecciano spesso con temi molto ampi sulla stabilità del sistema. Un sistema davvero sicuro bilancia i metodi e i tool di sicurezza con una consapevolezza dei vari modi in cui possono essere inflitti i danni.

Innanzitutto, se il sistema è utilizzato da più utenti, molti dei quali cambiano spesso, assicuratevi di cancellare subito i vecchi. Sarebbe poi buona abitudine creare una lista di controllo chiara e concisa delle azioni da effettuare quando un account utente o un gruppo non sono più necessari.

Limitate l'accesso fisico al sistema. Se sul vostro sistema sono contenuti file importanti e qualcuno tenta di accedervi, sarà molto più facile se riesce a rubare il calcolatore, avrà infatti più tempo poi per riuscire a trovare questi file. Evitate dunque di diffondere informazioni sul computer che contiene file tanto importanti.

Soprattutto non considerate solo i metodi di base per risolvere i vostri problemi di sicurezza. Non dovete proteggere una possibile via di accesso per poi lasciarne un'altra totalmente scoperta. Naturalmente il modo in cui evitare una simile situazione dipende da voi e dalle necessità dei vostri utenti. Assicuratevi solo di non concentrare troppo la vostra attenzione in una sola direzione.

7.5 L'importanza di password sicure

Le password costituiscono le chiavi per accedere al sistema. È inutile ribadire l'importanza di renderle il più sicure possibile per impedire un login non autorizzato, ossia il primo passo verso problemi di sicurezza di gran lunga maggiori. Una fase semplice quanto fondamentale è di creare password sufficientemente complesse da ridurre gli attacchi al sistema.

Molte password utente sono davvero facili da indovinare. Red Hat Linux fornisce diversi modi per garantire l'autenticazione al sistema, tra cui l'uso di password cifrate, con il comando `crypt`, le password shadow (per informazioni più dettagliate, consultate la Sezione 12.1, *Utility shadow*), Kerberos 5 ecc. In tutte le situazioni dove occorre scegliere una password come parte di uno schema di autenticazione, la sicurezza di quello schema dipende, almeno in parte, dalla complessità della password scelta.

Perchè scegliere password sicure e difficili da indovinare? In sostanza, il prezzo di un computer potente continua a diminuire in funzione del numero crescente di strumenti e metodi gratuiti ed efficaci per individuare le password. Per via del modo in cui le password vengono memorizzate in molti degli schemi più semplici di autenticazione, se un malintenzionato riesce ad accedere ai file contenenti le password utente per il vostro sistema, può di sicuro indovinarne almeno una in un lasso di tempo relativamente breve, verificando le password cifrate con l'uso di una lista di parole contenute nei dizionari. Sebbene gli schemi di autenticazione siano consapevoli di questo genere di attacchi e usino dei metodi per renderli improbabili, nessuno di questi metodi è infallibile. Quindi scegliete con cura la vostra password e modificatela frequentemente, soprattutto con l'account di root.

Una password sicura ha le seguenti caratteristiche:

- *è lunga almeno otto caratteri* — più la parola è breve, più è facile individuarla.
- *è composta da caratteri, numeri e simboli* — i numeri e i simboli posizionati tra le lettere (o viceversa) aumentano il numero di opzioni possibili per un determinato carattere, questo rende più sicura l'intera password.
- *è unica* — scegliete password differenti l'una dall'altra. Se infatti tutte le password sono uguali o simili, le proporzioni di una falla nel sistema possono aumentare notevolmente.

Evitate di usare password che:

- *trovate nel dizionario* — utilizzando come password parole contenute nei dizionari, agevolate in modo esponenziale l'individuazione della password. Non fatelo e soprattutto non eliminate gli schemi di autenticazione che impediscono agli utenti di utilizzare tali parole.
- *sono legate a informazioni personali* — se come password usate la data del compleanno, il nome del coniuge o la marca della macchina, potrete sicuramente incorrere in problemi. Pensate a ogni password usata e cercate di capire se qualcuno che vi conosce potrebbe indovinarle. Se esiste anche solo la minima possibilità che questo possa avvenire, non usate quelle password.
- *risultano difficili da digitare* — se la vostra password è talmente complessa da doverla ridigitare più volte, occhi indiscreti potrebbero osservare senza problemi il movimento delle vostre dita e indovinare quindi la password. Infine, allenatevi nel digitare la password quando siete soli in modo da aumentare la velocità.

7.6 Sicurezza della rete

Se usate Red Hat Linux su una rete (per esempio: LAN, WAN o Internet), sappiate che il vostro sistema corre rischi maggiori. Oltre agli attacchi ai file contenenti le password e agli utenti con accesso inadeguato, la presenza del sistema su una rete di dimensioni più ampie accresce la possibilità di problemi di sicurezza e del modo in cui possono presentarsi.

Sono state create numerose misure di sicurezza per Red Hat Linux e altrettanti tool open source sono compresi nella distrubuzione di base. Comunque, nonostante siate preparati, possono verificarsi problemi con la sicurezza del sistema, dovuti in parte alla topologia della rete e a decine di altri fattori. Per determinare la fonte e il metodo di un problema di sicurezza della rete, valutate i modi più probabili in cui può verificarsi un problema:

- *prevedendo i dati di autenticazione* — molti dei metodi di autenticazione predefiniti in Linux e in altri sistemi operativi dipendono dall'invio di informazioni di autenticazione "in chiaro", nome utente e password vengono trasmessi sulla rete in chiaro. Esistono purtroppo molti tool per coloro che hanno accesso alla vostra rete (o a Internet, se lo usate per accedere al vostro sistema) per "fiutare" o individuare la vostra password, registrando tutti i dati trasferiti sulla rete e analizzandoli in modo da individuare istruzioni di login comuni. Questo metodo può essere utilizzato per trovare *qualsiasi* informazione inviata in modo non cifrato, perfino la password di root. È dunque necessario l'utilizzo di tool come Kerberos 5 e OpenSSH per impedire che le password o altri dati importanti vengano inviati senza crittografia. Se, per qualsiasi ragione, questi strumenti non possono essere utilizzati sul vostro sistema, non collegatevi mai come utente root, a meno che non siate alla console.
- *con un attacco frontale* — gli attacchi Denial of Service (letteralmente "negazione di servizio") e simili possono danneggiare perfino un sistema sicuro inondandolo di richieste errate che lo "opprimono" o creando processi che mettono a rischio il sistema e i dati, ma anche altri sistemi in comunicazione con il vostro. Esistono numerose protezioni per bloccare l'attacco e ridurne i danni, tra cui i firewall con il filtro di pacchetti. Comunque, gli attacchi frontali possono essere gestiti meglio dando uno sguardo ai modi in cui un sistema non affidabile comunica con il vostro sistema fidato, se inserite barriere di protezione tra i due e sviluppate un modo per rispondere velocemente a ogni evento, limitate al massimo i possibili danni.
- *approfittando di un bug o di un buco nella sicurezza* — a volte nei software vengono individuati dei bug che, se sfruttati, possono danneggiare seriamente un sistema non protetto. Per questa ragione, eseguite il minor numero di processi come utente root. Utilizzate inoltre i vari tool disponibili, per esempio Red Hat Network, per ottenere informazioni sugli aggiornamenti e sui problemi di sicurezza individuati di recente. Assicuratevi quindi che non vengano caricati programmi inutili all'avvio del sistema. Meno programmi vengono avviati, minori sono le possibilità di essere colpiti da bug della sicurezza.

7.7 Risorse aggiuntive

Le informazioni sulla sicurezza cambiano di continuo e i siti Web forniscono un modo semplice per avere le ultime notizie. Per ricevere informazioni sempre recenti relative alla sicurezza di un sistema Red Hat Linux o per scoprirne di più, visitate regolarmente il sito Web di Linux. Se poi vi occorre aiuto per sviluppare una politica di sicurezza solida che tenga conto delle particolari esigenze del vostro sistema, utilizzate un buon libro sulla sicurezza.

7.7.1 Siti Web utili

- http://www.redhat.com/support/errata — per avere notizie sulla sicurezza e sugli aggiornamenti per ogni versione di Red Hat Linux prodotta da Red Hat.
- http://www.cert.org — il sito CERT offre una lista aggiornata degli eventi a forte impatto sulla sicurezza e comprende informazioni dettagliate su come ripristinare un sistema dopo essere stato compromesso.
- http://www.sans.org — il sito Web del System Administration, Networking and Security Institute (SANS) fornisce avvisi sulla sicurezza in forma riassunta e link utili per gli RPM aggiornati (se disponibili).
- http://www.linuxsecurity.com — il sito Web di Linux specifico per la sicurezza offre una serie di link correlati al problema della sicurezza, alla documentazione e a molto altro.
- http://www.securityportal.com — questo sito contiene novità recenti sulla sicurezza, problemi specifici di Linux, documentazione per creare modelli e politiche di sicurezza migliori.

7.7.2 Libri correlati

- *Securing and Optimizing Linux: Red Hat Edition* di Gerhard Mourani, OpenNA — questo libro può essere scaricato gratuitamente in formato PDF all'indirizzo http://www.openna.com.
- *Secrets & Lies* di Bruce Schneier, John Wiley & Sons, Inc. — un'analisi esaustiva e pragmatica dei temi più attuali sulla sicurezza del sistema.

8 Moduli di autenticazione PAM

I programmi che forniscono privilegi devono essere in grado di autenticare gli utenti. Quando entrate in un sistema, una volta inserite la vostra login e la vostra password, il processo login utilizzerà questi dati per autenticare la vostra connessione — verificherà la vostra identità. Sono possibili altre forme di autenticazione oltre alle password ed è possibile memorizzare le password in modi differenti.

I PAM (pluggable authentication modules) permettono all'amministratore di sistema di creare un procedimento di autenticazione senza dover ricompilare i programmi che si occupano dell'autenticazione. I PAM vi consentono di gestire i moduli di autenticazione, modificando i relativi file di configurazione che si trovano nella directory `/etc/pam.d`.

La maggior parte degli utenti di Red Hat Linux non avrà mai bisogno di modificare questo file di configurazione. Quando usate l'RPM per installare i programmi che richiedono un'autenticazione, vengono effettuate automaticamente le modifiche necessarie per l'autenticazione delle password. Tuttavia, potreste voler personalizzare la vostra configurazione, in tal caso è necessario conoscere la struttura dei file di configurazione PAM. Maggiori informazioni sono disponibili nella Sezione 8.2.2, *Moduli PAM*.

8.1 I vantaggi di PAM

Se usati correttamente, i PAM sono di grande aiuto all'amministratore di sistema poiché forniscono vantaggi quali:

- Uno schema di autenticazione comune che può essere usato con molte applicazioni diverse.
- I PAM possono essere implementati con varie applicazioni che non devono essere ricompilate per poterli supportare.
- Elevato controllo e grande flessibilità di autenticazione per l'amministratore e lo sviluppatore di applicazioni.
- Gli sviluppatori non devono adattare i propri programmi affinché utilizzino uno schema di autenticazione particolare. Possono così concentrarsi sui loro programmi.

8.2 File di configurazione PAM

I file di configurazione PAM sono contenuti nella directory `/etc/pam.d`. Nelle versioni precedenti di PAM tali file erano invece contenuti in `/etc/pam.conf`. Il file `pam.conf` viene letto se la directory `/etc/pam.d/` non è presente sul sistema, ma il suo utilizzo è sconsigliato.

Ogni applicazione (o *servizio*, nome solitamente attribuito alle applicazioni utilizzate da molti utenti) ha un suo proprio file. Ogni file contiene cinque elementi diversi: **nome del servizio**, **tipo di modulo**, **indicatore di controllo**, **percorso di modulo** e **argomenti**.

8.2.1 Nomi di servizio PAM

Il nome di servizio di ogni applicazione basata su PAM corrisponde al nome del suo file di configurazione contenuto in `/etc/pam.d`. Ogni programma che utilizza PAM definisce il proprio nome di servizio.

Per esempio il programma `login` definisce il nome di servizio `login`, `ftpd` determina il nome di servizio `ftp` e così via.

In generale, il nome di servizio corrisponde al nome del programma usato per *accedere* al servizio, non al programma usato per *fornire* il servizio.

8.2.2 Moduli PAM

PAM fornisce quattro tipi diversi di moduli che permettono di controllare l'accesso a particolari servizi:

- Il modulo `auth` fornisce l'effettiva autenticazione (forse richiedendo e controllando una password) e fornisce "credenziali" quali l'appartenenza al gruppo o i "ticket" di Kerberos.
- Il modulo `account` esegue un controllo per assicurarsi che l'autenticazione sia possibile (se l'account non è scaduto, se l'utente ha il permesso di accedere a quest'ora del giorno, ecc).
- Il modulo `password` viene usato per configurare le password.
- Il modulo `session` viene chiamato in causa una volta che l'autenticazione di un utente è stata eseguita per rendere possibile l'uso dell'account, magari montando la sua directory home o rendendo disponibile la mailbox.

Questi moduli possono essere inseriti nello *stack* o impilati in modo da poter essere utilizzati contemporaneamente. L'ordine del modulo stack è molto importante nel processo di autenticazione, poiché facilita all'amministratore il compito di richiedere la verifica di determinate condizioni prima di autorizzare l'autenticazione dell'utente.

Per esempio, `rlogin` utilizza normalmente almeno quattro metodi di autenticazione tramite stack, come dimostra il suo file di configurazione PAM:

```
auth       required     /lib/security/pam_nologin.so
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_env.so
auth       sufficient   /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_stack.so service=system-auth
```

```
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

Prima che qualcuno possa usare il comando `rlogin`, PAM verifica se esiste `/etc/nologin`, se si sta provando a effettuare un collegamento in modo remoto come root e se possono essere caricate tutte le variabili d'ambiente. Viene poi eseguita un'autenticazione `rhosts`. Se l'autenticazione `rhosts` non va a buon fine, viene effettuatata un'autenticazione standard della password.

Nuovi moduli possono essere aggiunti in ogni momento e le applicazioni compatibili con PAM possono utilizzarli. Per esempio, se create un nuovo sistema di calcolo della password e scrivete un modulo PAM per supportarlo, i programmi compatibili con PAM possono immeditamente usare il nuovo modulo e la nuova password senza dover essere ricompilati o modificati. Ciò permette di abbinare e verificare molto velocemente i metodi di autenticazione con diversi programmi senza doverli ricompilare.

Una documentazione sulla scrittura dei moduli è disponibile in `/usr/share/doc/pam-<`*`numero versione`*`>`.

8.2.3 Opzioni PAM

Quando vengono controllati, tutti i moduli PAM generano un risultato positivo o negativo. Le opzioni indicano a PAM cosa fare con il risultato del controllo. Poiché i moduli possono essere ordinati in determinati modi, le opzioni permettono di stabilire l'importanza di un modulo rispetto ai moduli successivi.

Considerate il file di configurazione PAM `rlogin`:

```
auth       required     /lib/security/pam_nologin.so
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_env.so
auth       sufficient   /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_stack.so service=system-auth
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

Una volta specificato il tipo di modulo, gli indicatori di controllo decidono quanta importanza deve essergli attribuita rispetto all'accesso di tale utente al programma.

Lo standard PAM determina quattro tipi di opzioni di controllo:

- I moduli con opzione `required` devono superare il controllo perché l'autenticazione sia autorizzata. Se il controllo di un modulo `required` fallisce, l'utente non ne viene avvisato finché tutti gli altri moduli dello stesso tipo non sono stati controllati.

- I moduli con opzione `requisite` devono anch'essi superare la verifica perché l'autenticazione vada a buon fine. Tuttavia, se la verifica di un modulo `requisite` fallisce, l'utente ne viene immediatamente avvisato tramite un messaggio che richiama il primo modulo `requisite` *o* `required` che non ha superato la verifica.
- Le verifiche dei moduli `sufficient` vengono ignorate se falliscono. Tuttavia, se un modulo con opzione `sufficient` supera la verifica così come tutti i moduli `required` che lo precedono, nessun altro modulo di questo tipo viene controllato.
- I moduli con opzione `optional` non rivestono un ruolo cruciale per il superamento o il fallimento dell'autenticazione di questo tipo di modulo. Rivestono un ruolo importante solo se nessun modulo dello stesso tipo ha superato o non ha superato la verifica. In tal caso, il superamento o il fallimento della verifica di un modulo con opzione `optional` determina l'autenticazione di tutti i moduli dello stesso tipo.

Adesso è disponibile una nuova sintassi di controllo ancora più efficace per PAM. Per maggiori informazioni, consultate la documentazione su PAM contenuta in `/usr/share/doc/pam–`*<numero versione>*.

8.2.4 Percorsi dei moduli PAM

I percorsi dei moduli indicano a PAM dove trovare il modulo inseribile da usare con il tipo di modulo specificato. Solitamente viene fornito l'intero percorso al modulo, quale `/lib/security/pam_stack.so`. Tuttavia, se non viene indicato tutto il percorso (in altre parole, se il percorso non inizia con `/`), allora si suppone che il modulo indicato si trovi in `/lib/security`, la posizione di default dei moduli PAM.

8.2.5 Argomenti PAM

PAM utilizza degli argomenti per passare informazioni a un modulo inseribile durante l'autenticazione di un tipo particolare di modulo. Tali argomenti permettono ai file di configurazione PAM di usare un modulo PAM comune ma in modi differenti per un programma particolare.

Per esempio il modulo `pam_userdb.so` utilizza dei file nascosti del Berkeley DB per autenticare l'utente. (Il Berkeley DB è un database open source concepito per essere incorporato in varie applicazioni al fine di seguire determinati tipi di informazioni). Il modulo prende un argomento `db`, specificando il file Berkeley DB da usare, che può variare in funzione del servizio.

La linea `pam_userdb.so` in un file di configurazione PAM è simile a:

```
auth       required  /lib/security/pam_userdb.so db=path/to/file
```

Gli argomenti non validi vengono ignorati e non influenzano il superamento né il fallimento del modulo PAM. Quando viene passato un argomento non valido, viene solitamente inviato un errore a

`/var/log/messages`. Tuttavia, poiché il metodo di reporting è controllato dal modulo PAM, è compito del modulo rilevare l'errore.

8.2.6 Esempi di file di configurazione PAM

Un file di configurazione PAM di esempio è simile a:

```
#%PAM-1.0
auth      required  /lib/security/pam_securetty.so
auth      required  /lib/security/pam_unix.so shadow nullok
auth      required  /lib/security/pam_nologin.so
account   required  /lib/security/pam_unix.so
password  required  /lib/security/pam_cracklib.so
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
session   required  /lib/security/pam_unix.so
```

La prima riga è un commento (tutte le righe che iniziano con # sono un commento). Le righe da due a quattro contengono tre moduli da usare per l'autenticazione della login.

```
auth      required  /lib/security/pam_securetty.so
```

La seconda riga si assicura che *se* l'utente sta provando a collegarsi come root, la tty su cui sta provando a collegarsi è elencata nel file `/etc/securetty`, *se* tale file esiste.

```
auth      required  /lib/security/pam_unix.so shadow nullok
```

La terza riga chiede all'utente una password e controlla tale password.

```
auth      required  /lib/security/pam_nologin.so
```

La quarta riga controlla se il file `/etc/nologin` esiste. Se `/etc/nologin` esiste e l'utente non è root, l'autenticazione non va a buon fine.

Tutti e tre i moduli `auth` vengono controllati, *anche se il primo modulo `auth` non supera la verifica*. Questa strategia impedisce all'utente di sapere perché l'autenticazione non è permessa. Se fosse al corrente del motivo, l'utente riuscirebbe a infrangere l'autenticazione. Potete modificare questo comportamento sostituendo `required` con `requisite`. Se uno dei moduli `requisite` non supera la verifica, PAM non va a buon fine e non chiama altri moduli.

```
account   required  /lib/security/pam_unix.so
```

La quinta riga effettua, se necessario, una verifica dell'account. Per esempio se le password shadow sono state attivate, il modulo `pam_unix.so` verifica se l'account è scaduto o se l'utente non ha modificato la password nel periodo stabilito.

```
password  required  /lib/security/pam_cracklib.so
```

La sesta riga controlla se una password appena modificata può essere indovinata da un programma illegale per la ricostruzione delle password.

```
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
```

La settima riga specifica che se il programma `login` cambia la password dell'utente, dovrebbe utilizzare il modulo `pam_unix.so` per farlo. (Succede solo se un modulo `auth` ha stabilito che la password deve essere cambiata — per esempio se una password shadow è scaduta.)

```
session   required  /lib/security/pam_unix.so
```

L'ottava e ultima riga specifica che il modulo `pam_unix.so` viene usato per gestire la sessione. Attualmente questo modulo non compie nessuna operazione, e può essere sostituito con qualsiasi modulo necessario.

L'ordine delle righe all'interno del file è importante. Sebbene non sia fondamentale in che ordine sono chiamati i moduli `required`, esistono altre opzioni di controllo. Mentre `optional` è usato raramente, `sufficient` e `requisite` rendono importante l'ordine con cui sono inserirti.

Diamo un'occhiata alla configurazione `auth` per `rlogin`:

```
#%PAM-1.0
auth      required    /lib/security/pam_nologin.so
auth      required    /lib/security/pam_securetty.so
auth      required    /lib/security/pam_env.so
auth      sufficient  /lib/security/pam_rhosts_auth.so
auth      required    /lib/security/pam_stack.so service=system-auth
```

Per prima cosa, `pam_nologin.so` verifica se `/etc/nologin` esiste. In caso positivo, può collegarsi solo root.

```
auth      required    /lib/security/pam_securetty.so
```

In secondo luogo, `pam_securetty.so` evita gli accessi di root su terminali insicuri. Se volete che siano accettati (in tal caso vi raccomandiamo di non essere connessi a Internet o dietro un firewall), consultate la Sezione 8.4, *Utilizzo di `rlogin`, `rsh` e `rexec` con PAM*.

```
auth      required    /lib/security/pam_env.so
```

In terzo luogo, il modulo `pam_env.so` carica le variabili di ambiente specificate in `/etc/security/pam_env.conf`.

```
auth      sufficient  /lib/security/pam_rhosts_auth.so
```

Poi, se `pam_rhosts_auth.so` autentica l'utente usando `.rhosts` nella sua directory home, PAM attiva subito `rlogin` senza attuare nessun controllo della password tramite `pam_stack.so`. Se `pam_rhosts_auth.so` non riesce ad autenticare l'utente, l'autenticazione fallita viene ignorata.

```
auth      required    /lib/security/pam_stack.so service=system-auth
```

Infine, se `pam_rhosts_auth.so` non è riuscito ad autenticare l'utente, il modulo `pam_stack.so` esegue una normale autenticazione della password e riceve l'argomento `service=system-auth`.

Nota Bene

Se non volete che venga visualizzato il prompt per inserire la password quando `securetty` fallisce e determina che l'utente sta provando a collegarsi come root in modo remoto, potete cambiare il modulo `pam_securetty.so` da `required` a `requisite`. Altrimenti, se volete autorizzare i collegamenti root remoti (ve lo sconsigliamo), potete commentare questa riga.

8.3 Password shadow

Se usate le password shadow, `pam_unix.so` se ne accorge automaticamente e usa tali password per autenticare l'utente.

Consultate la Sezione 12.1, *Utility shadow* per maggiori informazioni sulle password shadow.

8.4 Utilizzo di `rlogin`, `rsh` e `rexec` con PAM

Per ragioni di sicurezza `rexec`, `rsh` e `rlogin` non sono attivati per default in Red Hat Linux 7.1. Dovete usare la raccolta di tool OpenSSH. Per informazioni su OpenSSH, consultate il Capitolo 11, *Protocollo SSH* e la *Official Red Hat Linux Customization Guide*.

Se dovete usare `rexec`, `rsh` e `rlogin` come root, apportate alcune modifiche al file `/etc/securetty`. Tutti questi tool contengono file di configurazione PAM che richiedono il modulo PAM `pam_securetty.so`, modificate quindi `/etc/securetty` per autorizzare l'accesso a root.

Prima di potervi collegare come root è necessario impostare questi tool. Installate l'RPM `rsh-server`, che non è fornito con Red Hat Linux 7.1. Consultate la *Official Red Hat Linux Customization Guide* per maggiori informazioni sull'utilizzo di RPM.

Quindi eseguite `ntsysv` e attivate `rexec`, `rsh` e `rlogin`. Per maggiori informazioni sull'utilizzo di questi tool, consultate la pagina man di `ntsysv`.

Infine, riavviate `xinetd` con `/sbin/service xinetd restart` per attivare le modifiche `ntsysv`. A questo punto, tutti gli utenti tranne root possono usare `rexec`, `rsh` e `rlogin`.

Per permettere a root di usare questi tool, aggiungete i nomi dei tool desiderati a `/etc/securetty`. Per attivare il collegamento root usando `rexec`, `rsh` e `rlogin`, aggiungete le righe seguenti a `/etc/securetty`:

```
rexec
rsh
rlogin
```

Per permettere a root di effettuare i login usando questi tool via `telnet` (una pessima idea, ma necessaria in alcuni ambienti), aggiungete le righe seguenti:

```
pts/0
pts/1
```

8.5 Risorse aggiuntive

Sono disponibili numerose fonti di informazioni su PAM molto utili per la configurazione e l'utilizzo di PAM sul sistema.

8.5.1 Documentazione installata

- Pagina man `pam` — Buone informazioni introduttive su PAM, tra cui la struttura e lo scopo dei file di configurazione PAM.
- `/usr/share/doc/pam-<numero versione>` — contiene un'ottima documentazione HTML su PAM, nonché i manuali *System Administrators' Guide*, *Module Writers' Manual* e *Application Developers' Manual*. Contiene inoltre una copia dello standard PAM, DCE-RFC 86.0.

8.5.2 Siti Web utili

- http://www.kernel.org/pub/linux/libs/pam — il primo sito Web di distribuzione del progetto Linux-PAM, contenente informazioni su vari moduli e applicazioni PAM, le relative FAQ e una documentazione aggiuntiva su PAM.

Quando iniziate a usare PAM, oltre a queste fonti vi suggeriamo di leggere il maggior numero possibile di esempi di file di configurazione. Molti siti Web offrono esempi di codici, sia per gli amministratori che vogliono modificare la configurazione di default sia per gli sviluppatori di applicazioni che desiderano usare PAM con i loro programmi.

9 Kerberos 5 su Red Hat Linux

Kerberos è un sistema di sicurezza per l'autenticazione dei servizi di rete. Per autenticazione si intende:

- verificare l'identità delle entità sulla rete
- controllare se il traffico sulla rete proviene da chi sostiene di averlo inviato

Kerberos usa le password per verificare l'identità degli utenti. Le password comunque sono inviate sempre in forma cifrata lungo la rete.

9.1 Perché usare Kerberos?

La maggior parte dei sistemi di rete usa uno schema di autenticazione basato sulle password. Quando un utente ha bisogno di essere autenticato per accedere a un server di rete, digita la sua password, che viene inviata via rete e in questo modo il server verifica l'identità dell'utente.

Trasmettere la password in chiaro lungo la rete riduce drasticamente il livello di sicurezza del sistema. Qualunque utente che ha accesso alla rete e che può utilizzare un analizzatore di pacchetti di rete (solitamente chiamato packet sniffer) può intercettare le password che attraversano la rete.

Lo scopo principale di Kerberos è di assicurare che le password *non* siano mai inviate in chiaro e preferibilmente che non siano mai inviate lungo la rete. L'uso corretto di Kerberos elimina ogni pericolo di intercettazione delle password sulla rete.

9.2 Perché non usare Kerberos?

Tramite Kerberos si riesce a proteggere la rete dagli attacchi più comuni. Allora perché non viene usato su ogni sistema di rete? Kerberos potrebbe risultare complesso da implementare per varie ragioni:

- Non esiste nessuna soluzione rapida per la migrazione delle password dal database delle password di UNIX (per esempio `/etc/passwd` o `/etc/shadow`) al database della password di Kerberos. La migrazione è tecnicamente possibile ma esula lo scopo di questo capitolo. Per stabilire se ha senso una migrazione delle password per l'installazione di Kerberos, consultate le FAQ al sito http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html oppure fate riferimento alle informazioni più dettagliate contenute nella Sezione 9.8, *Risorse aggiuntive*.
- Kerberos è solo in parte compatibile con il sistema PAM (Pluggable Authentication Modules) usato dalla maggior parte dei server Red Hat Linux. Per maggiori informazioni, consultate la Sezione 9.8, *Risorse aggiuntive*.
- Affinché una applicazione di rete possa usare Kerberos, è necessario modificare il suo codice sorgente per effettuare le chiamate alle librerie Kerberos. Per alcune applicazioni occorre molta

programmazione, per altre invece vanno effettuate modifiche al protocollo usato tra i server e i client di rete. Anche in questo caso potrebbe esserci bisogno di una programmazione lunga. Inoltre potrebbe risultare impossibile far funzionare Kerberos su alcune applicazioni a "sorgente chiusa".

- Kerberos parte dal presupposto che stiate usando host fidati su una rete non sicura. Il suo obiettivo principale è di impedire che le password in chiaro vengano inviate lungo questa rete. Tuttavia, se qualcuno diverso dall'utente effettivo ha accesso fisico a uno degli host, specialmente quello che emette i ticket usati per l'autenticazione, l'intero sistema di autenticazione è a rischio.
- Infine, se decidete di utilizzare Kerberos sulla rete, dovete adottarlo per ogni tipo di servizio. Se anche *un solo* servizio invia ancora la password in chiaro, il sistema di autenticazione risulta compromesso e non otterrete alcun beneficio dal sistema Kerberos. Perciò per migliorare il livello di sicurezza è necessario **kerberizzare** (ossia far funzionare con Kerberos) *tutte* le applicazioni di rete che inviano password in chiaro oppure smettere di usare sulla rete queste applicazioni poco sicure.

9.3 Terminologia Kerberos

Come per ogni altro sistema, anche Kerberos ha la sua terminologia. Prima di descriverne il funzionamento, vi elenchiamo i termini utilizzati:

chiave

insieme di dati, usati per cifrare e decifrare le informazioni. Le informazioni cifrate non possono essere decifrate senza la chiave corretta.

ciphertext

dati cifrati

client

un'entità sulla rete (un utente, un host o un'applicazione) che riceve un ticket da Kerberos

credential cache o file dei ticket

un file che contiene le chiavi per la comunicazione cifrata fra un utente e vari servizi di rete. Kerberos 5 fornisce l'architettura per altri tipi di cache (come per esempio la memoria condivisa), ma i file sono supportati meglio.

Key Distribution Center (KDC)

un servizio che distribuisce i ticket Kerberos, eseguito di solito sullo stesso host del Ticket Granting Server.

keytab o tabella delle chiavi

un file che contiene un elenco non cifrato delle chiavi. I server recuperano le chiavi dal file keytab invece di utilizzare il comando `kinit`. Il file keytab di default è `/etc/krb5.keytab`. `kadmind` è l'unico servizio che usa un altro file, normalmente il file `/var/kerberos/krb5kdc/kadm5.keytab`.

plaintext

informazioni non cifrate, in chiaro

principal

un utente o un servizio che si possono autenticare tramite Kerberos. Il nome di un principal ha la seguente forma "*root*[/*instance*]*@REALM*". Per un utente standard, *root* è lo stesso dell'ID di login. *instance* è opzionale. Se il principal ha un'istanza, è separato dalla root con "/". La stringa vuota è una istanza valida (che differisce da quella di default che è una istanza *NULLA*). Tutti i principal hanno la loro *chiave*, derivata dalle loro password (per gli utenti) o da un insieme casuale (per i servizi).

realm

una rete basata su Kerberos, formata da uno o più server (anche chiamati KDC) e da un insieme di client.

servizio

un programma o un computer accessibile via rete

ticket

una serie di credenziali elettroniche temporanee che verificano l'identità di un client per un particolare servizio

Ticket Granting Ticket (TGT)

un ticket speciale che permette ai client di ottenere dei ticket aggiuntivi senza richiederli al KDC

9.4 Funzionamento di Kerberos

Su una rete "tradizionale" in cui l'autenticazione degli utenti avviene tramite password, ogni volta che un utente deve essere autenticato per accedere a un servizio, è necessario digitare la password, che viene inviata in chiaro via rete e viene così autorizzato l'accesso al servizio di rete.

Come già sottolineato in precedenza, il problema principale risolto da Kerberos riguarda l'uso delle password per autenticare l'utente senza la necessità di inviarle via rete. Il database di Kerberos contiene le chiavi per tutti i servizi di rete.

Quando un utente si collega alla propria workstation collegata a una rete Kerberos, il suo principal viene inviato al KDC sotto forma di richiesta TGT. Questa richiesta può essere inviata dal programma di login (in modo trasparente) o dal programma `kinit` una volta che l'utente si è collegato.

Il KDC controlla il principal nel suo database. Se viene trovato, crea un TGT, lo cifra usando la chiave dell'utente e lo invia come risposta.

Il programma di login o `kinit` decifra il TGT utilizzando la chiave dell'utente. Il TGT, che scade dopo un periodo predefinito, viene immagazzinato nella cache delle credenziali. Per ogni TGT viene impostato un tempo limite di utilizzo per migliorare il livello di sicurezza. Di solito questo limite è di otto ore.

Quando un utente deve accedere a un servizio di rete, il client utilizza il TGT per richiedere un ticket per il servizio al Ticket Granting Service (TGS), in esecuzione sul KDC. Il TGS rilascia un ticket che viene usato per autenticare l'utente.

Probabilmente vi sarete resi conto che la spiegazione riportata sopra è stata semplificata. Se desiderate approfondire l'argomento, consultate la Sezione 9.8, *Risorse aggiuntive*

Nota Bene

Kerberos dipende da alcuni servizi di rete per poter funzionare correttamente. Prima di tutto è necessario che gli orologi dei vari calcolatori siano sincronizzati. Inoltre alcuni aspetti di Kerberos si basano sul servizio DNS (Domain Name Service), perciò accertatevi che il DNS sia configurato in modo corretto. Per maggiori informazioni, potete consultare la *Kerberos V5 System Administrator's Guide* presente nella directory `/usr/share/doc/krb5-server-<numeroversione>` nei formati HTML e PostScript.

9.5 Configurazione di un server Kerberos 5 su Red Hat Linux 7.1

Prima di tutto è necessario installare un calcolatore server in cui sia presente il software per Kerberos. Se state configurando un server slave, troverete maggiori dettagli nella *Kerberos 5 Installation Guide* (presente nella directory `/usr/share/doc/krb5-server-<numeroversione>`).

Per installare un server Kerberos:

1. Prima di installare Kerberos 5, assicuratevi che il vostro orologio di sistema sia sincronizzato e che il DNS funzioni. Prestate particolare attenzione alla sincronizzazione dell'ora tra il server Kerberos e i vari client. Infatti se gli orologi del server e dei client hanno una differenza superiore

a 5 minuti (tempo predefinito in Kerberos 5), i client non potranno autenticarsi al server. La sincronizzazione degli orologi è necessaria per impedire un attacco in cui si cerca di usare un vecchio metodo di autenticazione per mascherarsi da utente valido.

Dovreste configurare una rete client/server NTP (Network Time Protocol) compatibile usando Red Hat Linux, anche se non state usando Kerberos. Red Hat Linux 7.1 contiene il pacchetto `ntp` per un'installazione semplice. Per maggiori informazioni sull'NTP, consultate l'indirizzo http://www.eecis.udel.edu/~ntp

2. Installate i pacchetti `krb5-libs`, `krb5-server`, e `krb5-workstation` sul server KDC. Questa macchina deve essere il più possibile sicura, perciò non installate altri servizi.

   Se preferite utilizzare l'interfaccia grafica (GUI) per amministrare il server Kerberos, installate il pacchetto `gnome-kerberos`. Contiene il tool grafico `krb5`, per la gestione dei ticket e del sistema Kerberos.

3. Modificate i file di configurazione `/etc/krb5.conf` e `/var/kerberos/krb5kdc/kdc.conf` indicando le informazioni per la vostra rete. Sostituite le stringhe *EXAMPLE.COM* e *example.com* con il nome del vostro dominio mantenendo le lettere minuscole e maiuscole come indicato. Infine sostituite *kerberos.example.com* con il nome del server Kerberos. Per maggiori informazioni sul formato di questi file, consultate le rispettive pagine man.

4. Create il database utilizzando l'utility `kdb5_util` al prompt della shell digitate quanto segue:

   ```
   /usr/kerberos/sbin/kdb5_util create -s
   ```

   Il comando `create` crea il database per la memorizzazione delle chiavi. L'opzione `-s` obbliga la creazione di un file **stash**, in cui viene immagazzinato il server master. Se non esiste alcun file stash da cui leggere la chiave, il server Kerberos (`krb5kdc`) richiede all'utente la password del server master (che può essere utilizzata per ricreare la chiave) a ogni avvio del programma.

5. Modificate il file `/var/kerberos/krb5kdc/kadm5.acl`. Il programma `kadmind` usa questo file per determinare quali principal hanno accesso al database Kerberos. Nella maggior parte dei casi si può inserire la riga seguente:

   ```
   */admin@EXAMPLE.COM  *
   ```

   La maggior parte degli utenti saranno rappresentati nel database da un singolo principal (per esempio con una istanza *NULL* e *joe@EXAMPLE.COM*). Con questa configurazione gli utenti con un secondo principal e con un'istanza *admin* (per esempio *joe/admin@EXAMPLE.COM*) avranno pieni poteri sul database di Kerberos.

   Dopo aver attivato `kadmind` sul server, ogni utente potrà accedere ai servizi eseguendo `kadmin` o `gkadmin` su ogni client o server. Comunque solo gli utenti elencati nel file `kadm5.acl` potranno modificare il database.

Nota Bene

Le utility `kadmin` e `gkadmin` comunicano con il programma `kadmind` in esecuzione sul server via rete. Naturalmente dovrete creare un principal prima di connettervi al server via rete per amministrarlo. Create il primo principal con il comando `kadmin.local`, ideato per essere usato sullo stesso host di KDC e per non utilizzare Kerberos.

Per creare il primo principal, digitate il comando `kadmin.local` sul terminale di KDC:

```
/usr/kerberos/sbin/kadmin.local -q "addprinc nomeutente/admin"
```

6. Attivate Kerberos tramite il comando:

```
krb5kdc start
kadmin start
krb524 start
```

7. Aggiungete i principal per i vostri utenti tramite l'opzione `addprinc` di `kadmin` o tramite il menu **Principale** => **Aggiungi** di `gkadmin`. `kadmin` (e `kadmin.local` sul KDC master) è un'interfaccia a linea di comando per il sistema di amministrazione di Kerberos. Molti comandi sono disponibili dopo aver lanciato il programma `kadmin`. Per maggiori informazioni su questo programma, consultate la relativa pagina man.

8. Verificate che il vostro server rilasci i ticket. Prima di tutto, eseguite `kinit` per ottenere i ticket e memorizzatelo nel file della cache. Utilizzate il comando `klist` per visualizzare il contenuto della cache e il comando `kdestroy` per cancellarlo.

Nota Bene

Per default, `kinit` prova ad autenticarvi con la login utilizzata per collegarsi. Se l'utente non corrisponde a un principal presente nel database Kerberos, riceverete un messaggio di errore. In tal caso fornite a `kinit` il nome del vostro principal come argomento sulla linea di comando.

Una volta terminati i passi precedenti, il vostro server Kerberos dovrebbe essere in esecuzione. È necessario configurare i client di Kerberos.

9.6 Configurazione di un client Kerberos 5 su Red Hat Linux 7.1

La configurazione di un client di Kerberos 5 è più semplice di quella del server. È necessario installare i pacchetti client e modificare il file di configurazione `krb5.conf`. Le versioni "kerberizzate" di `rsh` e di `rlogin` richiedono qualche modifica nella configurazione.

1. Assicuratevi che l'ora tra il client kerberos e KDC sia sincronizzata. Per maggiori informazioni consultate la Sezione 9.5, *Configurazione di un server Kerberos 5 su Red Hat Linux 7.1*. Inoltre il DNS deve funzionare correttamente sul client Kerberos prima di installare i programmi.

2. Installate i pacchetti `krb5-libs` e `krb5-workstation` su ogni client della vostra rete. Inoltre modificate il file `/etc/krb5.conf` in ogni workstation client. Di solito è sufficiente usare il file `krb5.conf` del KDC.

3. Prima che un utente possa collegarsi tramite la versione "kerberizzata" di `rsh` o di `rlogin`, deve essere installato il pacchetto `xinetd`. Inoltre i programmi server `kshd` e `klogind` devono poter accedere alle chiavi del loro servizio principal.

   Tramite il programma `kadmin`, aggiungete un host principale per la workstation. Poiché non sarà mai necessario introdurre la password per questo principal, potete usare l'opzione `-randkey` del comando `addprinc` di kadmin per creare il principal e per assegnare una chiave casuale:

   ```
   addprinc -randkey host/blah.example.com
   ```

   Dopo aver creato il principal, estraete le chiavi per la workstation eseguendo il comando `ktadd` di `kadmin`.

   ```
   ktadd -k /etc/krb5.keytab host/blah.example.com
   ```

   Per poter usare la versione "kerberizzata" di `rsh` e di `rlogin`, usate `ntsysv` o `chkconfig` per abilitare `klogin`, `eklogin` e `kshell`.

4. Per gli altri servizi di rete va modificata la configurazione. Per usare la versione "kerberizzata" di `telnet`, dovete abilitare krb5-telnet. Utilizzate i programmi `ntsysv` o `chkconfig` affinché il servizio `krb5-telnet` venga attivato all'avvio del sistema.

   Se volete fornire un accesso FTP, dovete creare ed estrarre una chiave per un principal con una root di ftp e impostare il nome dell'host del server FTP. Utilizzate `ntsysv` o `chkconfig` per abilitare `gssftp`.

   Il server IMAP incluso nel pacchetto `imap` usa l'autenticazione GSS-API basata su Kerberos 5 nel caso sia presente il file `/etc/krb5.keytab`. La root per il principal deve essere imap. Il gserver CVS usa un principal con una root di `cvs` ed è identico al `pserver`.

Questa è la configurazione di base per una rete Kerberos semplice.

9.7 Kerberos e PAM

Attualmente, i servizi "kerberizzati" non utilizzano il sistema PAM — il server "kerberizzato" evita completamente il sistema PAM. Le applicazioni che usano PAM possono utilizzare il sistema Kerberos per il controllo della password se il modulo pam_krb5 è installato (è fornito nel pacchetto `pam_krb5`). Il pacchetto `pam_krb5` contiene un file d'esempio per la configurazione dei servizi `login` e `gdm`. Se l'accesso al server di rete è effettuato sempre tramite servizi kerberizzati (o servizi che utilizzano GSS-API, come IMAP), la rete può essere considerata sufficientemente sicura.

Un amministratore di sistema esperto non aggiunge il controllo delle password per i servizi di rete, poiché la maggior parte dei protocolli usati da questi servizi non cifrano la password prima di inviarla lungo la rete.

9.8 Risorse aggiuntive

Kerberos può rappresentare una sfida per i nuovi utenti, è infatti piuttosto complesso da capire, installare e configurare. Se desiderate maggiori esempi e informazioni sull'uso di Kerberos, consultate le seguenti fonti:

9.8.1 Documentazione installata

- `/usr/share/doc/krb5-server-<`*`numero-versione`*`>` — la *Kerberos V5 Installation Guide* e la *Kerberos V5 System Administrator's Guide*, viene installata nei formati PostScript e HTML dall'RPM `krb5-server`.
- `/usr/share/doc/krb5-workstation-<`*`numero-versione`*`>` — la *Kerberos V5 UNIX User's Guide*, vengono installate in formato PostScript e HTML dall'RPM `krb5-workstation`.

9.8.2 Siti Web utili

- http://web.mit.edu/kerberos/www — home page di Kerberos sul sito MIT
- http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html — FAQ su Kerberos
- ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS — link a una versione in Postscript del libro intitolato *Kerberos: An Authentication Service for Open Network Systems* di Jennifer G. Steiner, Clifford Neuman e Jeffrey I. Schiller. Si tratta della prima documentazione prodotta su Kerberos.
- http://web.mit.edu/kerberos/www/dialogue.html — *Designing an Authentication System: a Dialogue in Four Scenes* creato da Bill Bryant nel 1988, modificato da Theodore Ts'o nel 1997. Racconta di una conversazione tra due programmatori che stanno progettando di creare un sistema di autenticazione Kerberos. Lo stile informale della discussione agevola coloro che non conoscono assolutamente Kerberos.

- http://www.ornl.gov/~jar/HowToKerb.html — consigli pratici su come "kerberizzare" la vostra rete.

10 Installazione e configurazione di Tripwire

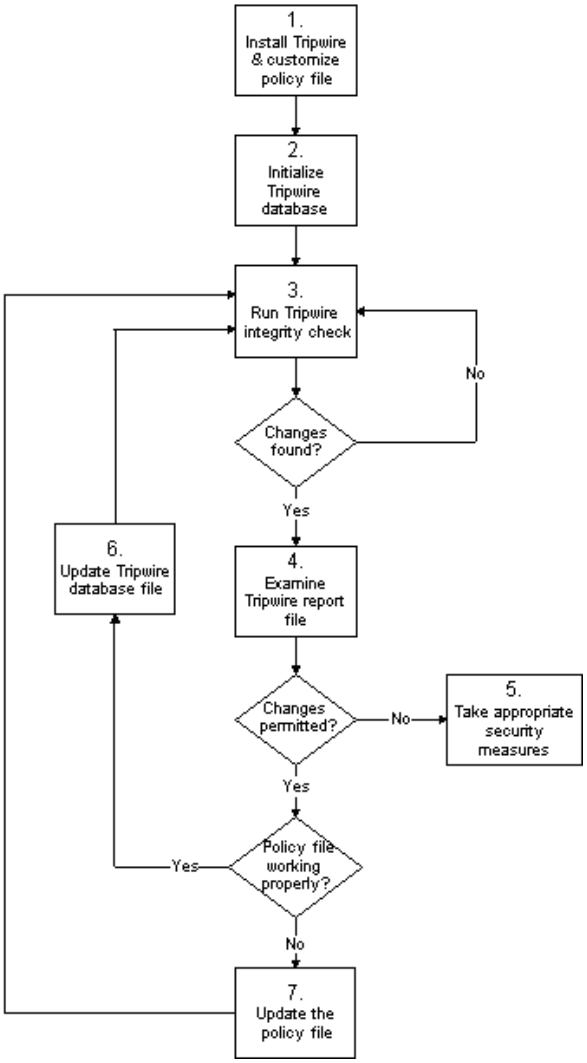
Il software Tripwire può aiutarvi a garantire l'integrità dei file e delle directory di sistema più importanti rilevando tutte le modifiche effettuate a tali file. Le opzioni di configurazione di Tripwire comprendono la possibilità di inviare messaggi di avvertimento via e-mail nel caso in cui vengano modificati dei file particolari. L'uso di Tripwire per rilevare le intrusioni e stabilire i danni può essere utile per aiutarvi a individuare le modifiche apportate al sistema e può rendere più veloce il ripristino dopo l'intrusione, riducendo il numero di file da ripristinare per riparare il sistema.

Tripwire confronta i file e le directory con un database fondamentale contenente le posizioni dei file, le date modificate e altri dati. Viene creato facendo una "fotografia" di file e directory specifici in uno stato "sicuro". (Per una maggiore sicurezza Tripwire dovrebbe essere installato prima che si presenti il rischio di un'intrusione nel sistema). Dopo aver creato il database, Tripwire paragona il sistema attuale con il database e segnala tutte le modifiche, aggiunte o cancellazioni avvenute.

10.1 Come usare Tripwire

Il seguente diagramma di flusso illustra il modo in cui Tripwire va utilizzato:

Figura 10–1 Come utilizzare Tripwire



Per installare e usare correttamente Tripwire eseguite quanto illustrato qui di seguito:

1. *Installazione di Tripwire e personalizzazione del file di policy* — se non lo avete già fatto, installate l'RPM di `tripwire` (consultate la Sezione 10.2.1, *Istruzioni per l'installazione dell'RPM*). In seguito personalizzate i file di configurazione (`/etc/tripwire/twcfg.txt`) e di policy (`/etc/tripwire/twpol.txt`). Eseguite quindi lo script di configurazione (`/etc/tripwire/twinstall.sh`). Per maggiori informazioni, consultate la Sezione 10.2.2, *Istruzioni post-installazione*.
2. *Inizializzazione del database di Tripwire* — create un database contenente i file di sistema più importanti e basato sui contenuti del nuovo file di policy di Tripwire (`/etc/tripwire/tw.pol`). Per maggiori informazioni, consultate la Sezione 10.7, *Inizializzazione del database*.
3. *Controllo dell'integrità di Tripwire* — paragonate il database appena creato con i file di sistema attuali e cercate i file mancanti o modificati. Per maggiori informazioni, consultate la Sezione 10.8, *Controllo dell'integrità*.
4. *Controllo del file di report di Tripwire* — visualizzate il file report di Tripwire utilizzando `twprint` per evidenziare violazioni dell'integrità. Per maggiori informazioni, consultate la Sezione 10.9, *Visualizzazione dei report*.
5. *Misure di sicurezza idonee* — se i file controllati sono stati modificati impropriamente, potete sostituire gli originali con i backup o reinstallare il programma.
6. *Aggiornamento del file database di Tripwire* — se le violazioni dell'integrità sono autorizzate e valide, perché per esempio avete modificato intenzionalmente un file o sostituito un particolare programma, è necessario specificare al file database di Tripwire di non segnalare tali modifiche come violazioni. Per maggiori informazioni, consultate la Sezione 10.10, *Aggiornamento del database dopo un controllo dell'integrità*.
7. *Aggiornamento del file di policy di Tripwire* — se dovete modificare l'elenco dei file da controllare o il modo in cui gestire le violazioni dell'integrità, occorre aggiornare il vostro file di policy (`/etc/tripwire/twpol.txt`), ricreare una copia firmata (`/etc/tripwire/tw.pol`) e aggiornare il database. Per maggiori informazioni, consultate la Sezione 10.11, *Aggiornamento del file di policy*.

Per informazioni più dettagliate, fate riferimento alle relative sezioni contenute in questo capitolo.

10.2 Istruzioni per l'installazione

Una volta installato, è necessario inizializzare Tripwire correttamente per poter controllare i file. Queste sezioni spiegano in dettaglio come installare il programma e poi come inizializzare il database.

10.2.1 Istruzioni per l'installazione dell'RPM

Per installare Tripwire più facilmente, installate prima l'RPM di `tripwire` durante il processo di installazione di Red Hat Linux 7.1. Se invece avete già installato Red Hat Linux 7.1, l'RPM di Tripwire può essere installato, utilizzando Gnome-RPM, o Kpackage, contenuti nei CD-ROM di Red Hat Linux 7.1, per installare l'RPM di Tripwire:

1. Individuate la directory `RedHat/RPMS` sul CD-ROM di Red Hat Linux.
2. Individuate l'RPM binario di `tripwire`, digitando `ls -l tripwire*` nella directory `RedHat/RPMS`.
3. Digitate `rpm -Uvh <nome>` (`<nome>` va sostituito con il nome dell'RPM di Tripwire individuato al punto 2)
4. Dopo aver installato l'RPM di `tripwire`, seguite le istruzioni post-installazione delineate qui sotto.

Nota Bene

Le release notes e il file `README` si trovano in `/usr/share/doc/tripwire-<numero-versione>`. Questi documenti contengono informazioni importanti relative al file di policy predefinito e ad altri temi.

10.2.2 Istruzioni post-installazione

L'RPM di `tripwire` installa i file dei programmi necessari per eseguire il software. Dopo aver installato Tripwire, configurate il vostro sistema nel modo illustrato qui di seguito:

1. Se sapete già di dover apportare numerose modifiche al file di configurazione (`/etc/tripwire/twcfg.txt`) e al file di policy (`/etc/tripwire/twpol.txt`), modificate questi file ora.

Nota Bene

La modifica dei file di configurazione e di policy consente di personalizzare Tripwire in base alle vostre esigenze, tuttavia non è necessario modificare tali file, se volete semplicemente utilizzare Tripwire. Nel caso intendiate modificare questi file, è necessario attuare tali modifiche prima di eseguire lo script di configurazione (`/etc/tripwire/twinstall.sh`). Se modificate i file di configurazione e di policy dopo aver eseguito lo script di configurazione, rieseguite lo script prima di inizializzare il file del database. Ricordate che *è possibile* modificare i file di configurazione e policy dopo aver inizializzato il file del database e aver eseguito un controllo dell'integrità.

---

2. Collegatevi come root, digitate `/etc/tripwire/twinstall.sh` sulla linea di comando e premete [Invio] per eseguire lo script di configurazione. Lo script `twinstall.sh` vi consente di impostare i codici, di generare chiavi cifrate per proteggere i file di configurazione e di policy e permette di firmare questi file. Per maggiori informazioni, consultate la Sezione 10.6, *Scelta delle chiavi*.

Nota Bene

Si consiglia di non rinominare o spostare i file (`/etc/tripwire/tw.cfg`) e (`/etc/tripwire/tw.pol`) generati dallo script `/etc/tripwire/twinstall.sh`, dopo averli cifrati e firmati.

---

3. Inizializzate il file del database eseguendo il comando `/usr/sbin/tripwire --init` sulla linea di comando.

4. Eseguite il primo controllo dell'integrità paragonando il database di Tripwire con i vostri file di sistema digitando `/usr/sbin/tripwire --check` sulla linea di comando e cercando eventuali errori nel report generato.

A questo punto, se avete effettuato con successo quanto descritto sopra, Tripwire possiede una "fotografia" dei file più importanti per il vostro sistema. Questa "immagine" gli consente di controllare se sono avvenute modifiche a tali file. Inoltre l'RPM di `tripwire` aggiunge un file chiamato `tripwire-check` alla directory `/etc/cron.daily` che eseguirà in modo automatico un controllo giornaliero dell'integrità.

10.3 Posizione dei file

Prima di utilizzare Tripwire, dovreste sapere dove sono collocati i file importanti per questa applicazione. Tripwire memorizza i suoi file in diversi posti, in funzione del loro ruolo:

- La directory `/usr/sbin` memorizza i programmi `tripwire`, `twadmin` e `twprint`.
- La directory `/etc/tripwire` contiene le chiavi del sito e locali (i file `*.key`), lo script di inizializzazione (`twinstall.sh`) e i file di configurazione e di policy (esempi ed effettivi).
- La directory `/var/lib/tripwire` contiene il database dei file di sistema (`*.twd`) e una directory `report` dove sono memorizzati i report di Tripwire. Questi report, chiamati *`nome_host-data_del_report-ora_del_report`*`.twr`, elencano in dettaglio le differenze rilevate tra il database di Tripwire e i file di sistema attuali.

10.4 Componenti di Tripwire

Il file di policy è, un file di testo contenente i commenti, le regole, le direttive e le variabili. Questo file determina il modo in cui Tripwire controlla il vostro sistema. Ogni regola nel file di policy specifica un oggetto di sistema da controllare. Le regole descrivono inoltre quali modifiche segnalare e quali ignorare.

Gli oggetti di sistema sono i file e le directory che desiderate controllare. Ogni oggetto è contraddistinto da un nome. Una proprietà si riferisce a una sola caratteristica di un oggetto che il sotware Tripwire può controllare. Le direttive controllano l'elaborazione condizionale di regole in un file di policy. Durante l'installazione, il file di policy in formato testo (`/etc/tripwire/twpol.txt`) viene cifrato e rinominato, diventando un file di policy attivo (`/etc/tripwire/tw.pol`).

Dopo l'inizializzazione Tripwire utilizza le regole del file di policy firmato per creare il file del database (`/var/lib/tripwire/`*`nome_host`*`.twd`). Il file del database è costituito da una fotografia del sistema in uno stato "sicuro". Tripwire confronta questa fotografia con il sistema attuale per individuare le modifiche avvenute. Questo paragone è definito **controllo dell'integrità**.

Quando eseguite un controllo dell'integrità, Tripwire crea dei file di report nella directory `/var/lib/tripwire/report`. I file di report elencano tutte le modifiche apportate ai file che violano le regole del file di policy.

Il file di configurazione Tripwire (`/etc/tripwire/tw.cfg`) memorizza informazioni specifiche per il sistema, come per esempio la posizione dei file di dati. Tripwire genera le informazioni necessarie per il file di configurazione durante l'installazione, ma l'amministratore del sistema può sempre modificare i parametri nel file della configurazione, dopo questa fase. Il file di configurazione modificato deve essere firmato come il file di policy per poter essere utilizzato di default.

Le variabili del file di configurazione **POLFILE**, **DBFILE**, **REPORTFILE**, **SITEKEYFILE** e **LOCALKEYFILE** specificano le posizioni dei file di policy, database, report e dei file con le chiavi locali e

del sito. Queste variabili sono definite per default al momento dell'installazione. Se modificate il file di configurazione e non definite le variabili descritte sopra, il file non viene considerato valido da Tripwire. Questo provoca un errore nell'esecuzione di `tripwire` e siete costretti a uscire dal programma.

Il file di configurazione deve essere firmato come il file di policy per poter essere usato da Tripwire. Per maggiori informazioni al riguardo, consultate la Sezione 10.11.1, *Firma del file di configurazione*.

10.5 Modifica del file di policy

È possibile specificare il modo in cui Tripwire controlla il vostro sistema modificando il file di policy Tripwire (`twpol.txt`). Modificando il file di policy in base alle vostre esigenze specifiche, potrete aumentare l'utilità dei report di Tripwire, riducendo i falsi allarmi per file o programmi che non usate ma che Tripwire continua a segnalare come mancanti o modificati.

Posizionate il file di policy predefinito nella directory `/etc/tripwire/twpol.txt`. Potete trovare un file di policy di esempio in `/usr/share/doc/tripwire-<`*`numero-versione`*`>/policyguide.txt`. Questo esempio vi aiuta a imparare il linguaggio di policy. Leggete questo file per sapere come modificare il file di policy predefinito.

Se modificate il file di policy subito dopo aver installato il pacchetto `tripwire`, assicuratevi di digitare `/etc/tripwire/twinstall.sh` per eseguire lo script di configurazione. Questo script firma il file di policy modificato e lo rinomina in `tw.pol`. Viene così creato il file di policy attivo utilizzato dal programma `tripwire` al momento dell'esecuzione.

Se modificate il file di policy d'esempio dopo aver eseguito lo script di configurazione, consultate la Sezione 10.11, *Aggiornamento del file di policy*, dove troverete le istruzioni su come effettuare la firma e trasformarlo nel file `tw.pol`.

Nota Bene

Se modificate il file di policy d'esempio, Tripwire non potrà usarlo finché non verrà firmato, cifrato e trasformato nel nuovo file `/etc/tripwire/tw.pol` (vedere la Sezione 10.11, *Aggiornamento del file di policy*).

10.6 Scelta delle chiavi

I file di Tripwire sono firmati e cifrati tramite le chiavi del sito e locali, che impediscono la visualizzazione o modifica dei file di configurazione, policy, database e report da parte di utenti non autorizzati. Ciò significa che anche se un intruso riesce a ottenere l'accesso di root al vostro sistema, non sarà comunque in grado di modificare i file di Tripwire per nascondere le proprie tracce, a meno che non

conosca le chiavi. Nel scegliere le chiavi dovete utilizzare almeno otto caratteri alfanumerici/simboli per ogni chiave. La lunghezza massima consentita è di 1023 caratteri, si consiglia di non usare le virgolette. Assicuratevi inoltre che le chiavi siano completamente diverse dalla password di root per il sistema.

Le chiavi locali e del sito dovrebbero essere univoche. La chiave del sito consente di firmare i file di configurazione e di policy, mentre la chiave locale firma i file di database e report.

Memorizzate le chiavi in un posto sicuro. *Se dimenticate la password non sarà possibile decifrare un file firmato.* Nel caso dimentichiate le password delle chiavi, i file non saranno utilizzabili e dovrete rieseguire lo script di configurazione, che inizializza di nuovo il database di Tripwire.

10.7 Inizializzazione del database

Durante l'inizializzazione del database, Tripwire crea una serie di oggetti filesystem basati sulle regole contenute nel file di policy. Questo database è fondamentale per eseguire i controlli dell'integrità.

Per inizializzare il database di Tripwire, utilizzate il seguente comando:

```
/usr/sbin/tripwire --init
```

L'esecuzione di tale comando potrebbe richiedere qualche minuto.

10.8 Controllo dell'integrità

Durante il controllo dell'integrità, Tripwire paragona gli oggetti filesystem attuali con le proprietà registrate nel database. Tutte le violazioni vengono visualizzate e salvate in un file di report a cui si può accedere in seguito tramite il comando `twprint`. Per maggiori informazioni su come visualizzare i report di Tripwire, consultate la Sezione 10.9, *Visualizzazione dei report*.

Nel file di policy esiste un'opzione per la configurazione della posta elettronica che consente di farvi ricevere a determinati indirizzi e-mail dei messaggi di avviso qualora si verifichino delle violazioni all'integrità. Per maggiori informazioni a riguardo, consultate la Sezione 10.12, *Tripwire e la posta elettronica*.

Per eseguire un controllo dell'integrità utilizzate i seguenti comandi:

```
/usr/sbin/tripwire --check
```

L'esecuzione di questo comando potrebbe richiedere qualche minuto, a seconda del numero di file da controllare.

10.9 Visualizzazione dei report

Con il comando `twprint -m r` potete visualizzare i contenuti in chiaro di un report. È necessario specificare a `twprint` il file di report da visualizzare.

Ecco un esempio del comando `twprint` (digitate tutto su una riga):

```
/usr/sbin/twprint -m r --twrfile
          /var/lib/tripwire/report/<nome>.twr
```

L'opzione `-m r` indica a `twprint` di decodificare un report di Tripwire. L'opzione `--twrfile` indica a `twprint` di utilizzare un file di report specifico.

Il nome del report che desiderate visualizzare comprende il nome dell'host usato da Tripwire per generare il report, la data e l'ora di creazione. Potete visualizzare i report salvati in passato quando volete. Digitate semplicemente `ls /var/lib/tripwire/report` per visualizzare una lista dei report di Tripwire.

I report di Tripwire possono essere piuttosto lunghi, a seconda del numero di violazioni individuate o di errori generati. Ecco un esempio di record:

```
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            Fri Jan 12 04:04:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================================
Report Summary:
===============================================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --check

===============================================================================
Rule Summary:
===============================================================================
-------------------------------------------------------------------------------
Section: Unix File System
```

```
-------------------------------------------------------------------
  Rule Name                Severity Level    Added    Removed  Modified
  ---------                --------------    -----    -------  --------
  Invariant Directories    69                0        0        0
  Temporary directories    33                0        0        0
* Tripwire Data Files      100               1        0        0
  Critical devices         100               0        0        0
  User binaries            69                0        0        0
  Tripwire Binaries        100               0        0        0
```

10.9.1 Uso di `twprint` per visualizzare il database di Tripwire

Potete usare il comando `twprint` anche per visualizzare l'intero database o le informazioni dei file selezionati. Ciò è senz'altro utile per visualizzare quante informazioni sta controllando Tripwire sul vostro sistema.

Per visualizzare il database completo di Tripwire, digitate questo comando:

```
/usr/sbin/twprint -m d --print-dbfile | less
```

Verranno visualizzate moltissime informazioni, le prime righe saranno simili all'esempio qui fornito:

```
Tripwire(R) 2.3.0 Database

Database generated by:        root
Database generated on:        Tue Jan  9 13:56:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================
Database Summary:
===============================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --init

===============================================================
Object Summary:
===============================================================
---------------------------------------------------------------
# Section: Unix File System
---------------------------------------------------------------
```

```
    Mode        UID          Size       Modify Time
    ------      ----------   ---------- ----------
/
    drwxr-xr-x  root (0)     XXX        XXXXXXXXXXXXXXXX
/bin
    drwxr-xr-x  root (0)     4096       Mon Jan  8 08:20:45 2001
/bin/arch
    -rwxr-xr-x  root (0)     2844       Tue Dec 12 05:51:35 2000
/bin/ash
    -rwxr-xr-x  root (0)     64860      Thu Dec  7 22:35:05 2000
/bin/ash.static
    -rwxr-xr-x  root (0)     405576     Thu Dec  7 22:35:05 2000
```

Per visualizzare le informazioni su un file particolare, per es.: `/etc/hosts`, digitate un comando `twprint` differente:

```
/usr/sbin/twprint -m d --print-dbfile /etc/hosts
```

Il risultato sarà simile al seguente:

```
Object name:  /etc/hosts

Property:               Value:
-------------           -----------
Object Type             Regular File
Device Number           773
Inode Number            216991
Mode                    -rw-r--r--
Num Links               1
UID                     root (0)
GID                     root (0)
```

Per visualizzare altre opzioni, consultate la pagina man di `twprint`.

10.10 Aggiornamento del database dopo un controllo dell'integrità

Se eseguite un controllo dell'integrità e riscontrate delle violazioni, determinate innanzitutto se tali violazioni sono davvero delle "falle" nella sicurezza oppure se sono modifiche autorizzate. Se di recente avete installato un'applicazione o modificato dei file di sistema importanti, Tripwire segnalerà (in modo corretto) tutte le violazioni dell'integrità. In questo caso dovrete aggiornare il vostro database, in modo tale che le modifiche apportate non vengano più segnalate come violazioni. Se tuttavia vengono effettuate modifiche a file di sistema che provocano violazioni dell'integrità, ripristinate i file originali con una copia di backup o reinstallate il programma.

Per aggiornare il database di Tripwire, specificate il report che desiderate utilizzare per l'aggiornamento. Nell'eseguire il comando per integrare le violazioni "valide" nel database, assicuratevi di usare il report più recente. Digitate il seguente comando (tutto su una riga), sostituendo *nome* con il nome del report da utilizzare:

```
/usr/sbin/tripwire --update --twrfile
          /var/lib/tripwire/report/<nome>.twr
```

Tripwire visualizza il report utilizzando l'editor predefinito (specificato nel file di configurazione Tripwire sulla riga **EDITOR**). A questo punto potete deselezionare i file che non desiderate aggiornare nel database Tripwire. È importante modificare solo le violazioni dell'integrità autorizzate.

Tutti gli aggiornamenti proposti per il database di Tripwire hanno una `[x]` che precede il nome del file. Se non volete aggiungere una violazione valida al database di Tripwire, rimuovete la `x` dalle parentesi. Per accettare tutti i file con `x`, scrivete il file nell'editor e poi uscite dal programma. In questo modo indicate a Tripwire di modificare il database e di non segnalare questi file come violazioni.

Per esempio, l'editor di testo predefinito per Tripwire è `vi`. Per scrivere il file con `vi` ed effettuare le modifiche al database di Tripwire quando aggiornate un report specifico, digitate `:wq` nella modalità di comando `vi` e premete [Invio]. Vi verrà chiesto di inserire la password della chiave. A questo punto viene scritto un nuovo database che include le violazioni valide.

Dopo aver scritto un nuovo database di Tripwire, le violazioni autorizzate non vengono più segnalate al controllo dell'integrità successivo.

10.11 Aggiornamento del file di policy

Se desiderate modificare i file di record nel database di Tripwire oppure la "severità" per la verifica delle violazioni, modificate il file di policy Tripwire.

Innanzitutto, effettuate tutte le modifiche necessarie al file di policy d'esempio (`/etc/tripwire/twpol.txt`). Una modifica che di solito viene apportata è il commento a tutti i file non esistenti sul sistema. In questo modo non verrà visualizzato il messaggio di errore `file non trovato` nei report di Tripwire. Per esempio, se sul vostro sistema non è presente un file chiamato `/etc/smb.conf`, specificate a Tripwire di non cercarlo, commentando la riga nel file `twpol.txt`:

```
#     /etc/smb.conf                     -> $(SEC_CONFIG) ;
```

È poi necessario indicare a Tripwire di creare un nuovo file `/etc/tripwire/tw.pol` firmato e di generare un file del database aggiornato in base a queste informazioni di policy. Ponendo il caso che `/etc/tripwire/twpol.txt` sia il file di policy modificato, usate questo comando:

```
/usr/sbin/twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt
```

Vi verrà richiesta la password per la chiave del sito. A questo punto il file `twpol.txt` viene analizzato e firmato.

È importante aggiornare il database di Tripwire, dopo aver creato un nuovo file `/etc/tripwire/tw.pol`. Il modo più affidabile per farlo è cancellare il database di Tripwire e creare un nuovo database utilizzando un nuovo file di policy.

Se il file del database di Tripwire si chiama `wilbur.domain.com.twd`, digitate questo comando:

```
rm /var/lib/tripwire/wilbur.domain.com.twd
```

Digitate poi il comando per creare un nuovo database:

```
/usr/sbin/tripwire --init
```

Il nuovo database viene creato in base alle istruzioni contenute nel file di policy. Per assicurarvi che il database sia stato modificato in modo corretto, eseguite manualmente il primo controllo dell'integrità e visualizzate i contenuti del report risultante. Per istruzioni specifiche relative a questi punti, consultate la Sezione 10.8, *Controllo dell'integrità* e la Sezione 10.9, *Visualizzazione dei report*.

10.11.1 Firma del file di configurazione

Il file di testo con le modifiche del file di configurazione (di solito `/etc/tripwire/twcfg.txt`) deve essere firmato per sostituire `/etc/tripwire/tw.cfg` e per essere usato da Tripwire durante il controllo dell'integrità. Tripwire non riconosce le modifiche nella configurazione fino a quando il file di testo della configurazione non viene firmato correttamente e utilizzato per sostituire il file `/etc/tripwire/tw.pol`.

Se il file di configurazione è `/etc/tripwire/twcfg.txt`, digitate questo comando per firmarlo e per sostituire l'attuale file `/etc/tripwire/tw.pol`:

```
/usr/sbin/twadmin --create-cfgfile -S site.key /etc/tripwire/twcfg.txt
```

Poiché il file di configurazione non modifica i file di Tripwire rilevati dall'applicazione, non è necessario rigenerare il database dei file di sistema controllati.

10.12 Tripwire e la posta elettronica

Tripwire può inviare un messaggio e-mail, qualora venga violata una specifica regola nel file di policy. Per configurare questa funzionalità di Tripwire, occorre prima l'indirizzo e-mail della persona da contattare se avviene una violazione dell'integrità e il nome della regola che volete controllare. Per i grandi sistemi con più amministratori, è possibile inviare messaggi di avvertimento a più persone in presenza di un certo tipo di infrazione oppure non inviare nessun messaggio in caso di violazioni minori.

Una volta determinato a chi inviare il messaggio e cosa notificare, aggiungete una linea **emailto=** alla sezione della direttiva di ogni regola. Per farlo, inserite una virgola alla fine della riga **severity=** e digitate **emailto=** all'inizio della riga seguente. Inserite poi gli indirizzi e-mail delle persone a cui inviare i report delle violazioni alla regola specificata. Se indicate più di un indirizzo e-mail, separato da punto e virgola, verranno inviate altrettante e-mail.

Se desiderate che due amministratori di sistema (per esempio, Tullio e Cesare) ricevano una notifica via e-mail nel caso in cui venga modificato il programma di networking, cambiate la direttiva della regola "Networking Programs" nel modo seguente:

```
(
  rulename = "Networking Programs",
  severity = $(SIG_HI),
  emailto = tullio@domain.com;cesare@domain.com
)
```

Dopo aver trasformato il file `/etc/tripwire/twpol.txt` in un nuovo file di policy firmato, agli indirizzi e-mail verranno notificate le violazioni a quella particolare regola. Per le istruzioni sulla firma del file di policy, consultate la Sezione 10.11, *Aggiornamento del file di policy*.

10.12.1 Invio di messaggi e-mail di prova

Per garantire che la configurazione delle notifiche e-mail di Tripwire permetta di inviare in modo corretto le e-mail, utilizzate il seguente comando:

```
/usr/sbin/tripwire --test --email vostro@indirizzo.email
```

Il programma `tripwire` provvede immediatamente a inviare una e-mail di notifica all'indirizzo specificato.

10.13 Risorse aggiuntive

Le funzioni di Tripwire sono molto più numerose di quelle trattate in questo capito. Per maggiori informazioni su Tripwire consultate la seguente documentazione:

10.13.1 Documentazione installata

- `/usr/share/doc/tripwire-<numero-versione->` — un eccellente punto di partenza per imparare come personalizzare i file di configurazione e di policy nella directory `/etc/tripwire`.
- Potete inoltre fare riferimento alle pagine man inerenti i comandi `tripwire`, `twadmin` e `twprint`.

10.13.2 Siti Web utili

- http://www.tripwire.org — la pagina principale del progetto open source di Tripwire dove potete trovare le ultime novità sulle applicazioni, tra cui una lista delle FAQ più frequenti.

11 Protocollo SSH

Questo capitolo illustra i vantaggi del protocollo SSH™, la sequenza di eventi che si susseguono quando viene stabilita una connessione a un sistema remoto, i diversi livelli di SSH e i metodi per garantire che SSH sia usato dagli utenti che si connettono al vostro sistema.

I metodi più diffusi per collegarsi in modo remoto a un altro sistema (tramite `telnet`, `rlogin` o `rsh`) oppure per copiare i file tra host (`ftp` o `rcp`) sono insicuri e andrebbero evitati. Dovreste invece connettervi a un host remoto usando una shell sicura o una rete virtuale privata e cifrata. L'uso di metodi sicuri per collegarsi ad altri sistemi in modo remoto diminuisce i rischi per la sicurezza di entrambi i sistemi (il vostro e quello remoto).

11.1 Introduzione

SSH (o *S*ecure *SH*ell) è un protocollo che vi consente di stabilire connessioni sicure tra due sistemi. Il calcolatore client avvia una connessione con un calcolatore server e SSH fornisce le seguenti misure di protezione:

- Dopo una connessione iniziale, il client riesce a identificare lo stesso server a cui si connette, durante sessioni successive.
- Il client trasmette le proprie informazioni di autenticazione al server, per esempio il nome utente e la password, in forma cifrata.
- Tutti i dati inviati e ricevuti durante la connessione vengono trasferiti utilizzando una cifratura complessa, in questo modo è estremamente complesso decifrarli e leggerli.
- Il client può utilizzare le applicazioni X11[1]lanciate dal prompt della shell. Viene così fornita un'interfaccia grafica e sicura (chiamata **X11 forwarding**).

Anche il server può approfittare di SSH, specialmente se esegue numerosi servizi. Se usate **port forwarding**, potete cifrare protocolli insicuri (per esempio POP) per stabilire una comunicazione sicura con le macchine remote. SSH facilita la cifratura di diversi tipi di comunicazione normalmente inviati in modo poco sicuro tramite le reti pubbliche.

Red Hat Linux 7.1 comprende i pacchetti Openssh server (`openssh-server`), client (`openssh-clients`) e il pacchetto generico. Per attivare questi pacchetti è necessario installare anche il pacchetto generico OpenSSH (`openssh`). Per le istruzioni sull'installazione e l'implementazione di OpenSSH, consultate la *Official Red Hat Linux Customization Guide*.

[1] X11 si riferisce al sistema di visualizzazione a finestre di X11R6, abbreviato con X. Red Hat Linux comprende XFree86, sistema X Window molto diffuso e basato su X11R6.

I pacchetti OpenSSH richiedono l'installazione di `openssl`, che comprende numerose librerie cifrate per consentire a OpenSSH di fornire comunicazioni cifrate. `Openssl` va installato prima dei pacchetti OpenSSH.

Molti programmi client e server possono utilizzare il protocollo SSH, tra cui molte applicazioni open source disponibili gratuitamente. Esistono varie versioni del client SSH per quasi tutti i maggiori sistemi operativi in uso. Anche se gli utenti che si connettono al vostro sistema non possiedono Red Hat Linux possono comunque trovare e utilizzare un client SSH nativo per il proprio sistema operativo.

11.1.1 Perché usare SSH?

Tra le minacce al traffico di rete vi sono la rilevazione dei pacchetti, falsi DNS e IP[2]e la diffuzione di informazioni di instradamento contraffatte. In termini generali queste minacce possono essere raggruppate in due categorie:

- *Intercettazione delle comunicazioni tra due sistemi* — questo scenario prevede l'esistenza di una terza parte in qualche punto della rete tra le due entità in comunicazione. Questa terza parte esegue una copia delle informazioni trasmesse tra i due sistemi, per conservarle o inviarle modificate al destinatario originale.
- *Imitazione di un host particolare* — con questa strategia, un sistema intercettante finge di essere il destinatario di un messaggio. Se la strategia funziona, il client non si accorge dell'inganno e continua a comunicare con il sistema intercettante come se il proprio traffico raggiungesse con successo la destinazione desiderata.

Entrambe le tecniche descritte sopra possono intercettare le informazioni e molto probabilmente con scopi ostili. I risultati potrebbero essere disastrosi, se gli intercettatori riescono a rilevare tutti i pacchetti su una LAN oppure se un server DNS

Se SSH viene utilizzato per i login con la shella remota e per la copia dei file, è possibile ridurre notevolmente queste minacce. Una firma digitale di un server fornisce la verifica per la propria identità. L'intera comunicazione tra i sistemi client e server non possono essere utilizzati se intercettati, perché ogni pacchetto è cifrato. I tentativi di assumere l'identità di uno dei due sistemi comunicanti non funzioneranno, poiché ogni pacchetto è cifrato con un codice conosciuto solo dai sistemi locali e remoti.

11.2 Sequenza degli eventi di una connessione SSH

Una serie di eventi contribuisce a salvaguardare l'integrità di una comunicazione SSH tra due host.

Innanzitutto viene creato un **livello di trasporto** sicuro, in modo che il client sappia che sta comunicando con il server corretto. Poi viene cifrata la comunicazione tra il client e il server con l'uso di un cifratore simmetrico.

2 Per "falso" s'intende spacciarsi per un particolare sistema e in realtà non esserlo.

In seguito, il client si autentifica al server senza preoccuparsi che le informazioni di autenticazione vengano compromesse. OpenSSH su Red Hat Linux utilizza le chiavi DSA o RSA e la versione 2.0 del protocollo SSH per l'autenticazione.

Infine, quando il client si è autenticato al server, è possibile utilizzare in modo sicuro i vari servizi usati tramite connessione, per esempio una sessione interattiva della shell, le applicazioni X11 e le porte TCP/IP immesse in un tunnel.

L'intero processo di connessione avviene con poco lavoro aggiuntivo necessario sul sistema locale. Infatti, in molti sensi, SSH funziona bene perché è conosciuto dagli utenti abituati a metodi di connessione meno sicuri.

Nell'esempio che segue, user1 inizializza sul sistema client una connessione SSH a un server, L'indirizzo IP del server è 10.0.0.2, ma si potrebbe usare anche il nome del dominio. Il nome di login di user1 sul server è user2. Il comando `ssh` è scritto nel seguente modo:

```
[user1@machine1 user1]$ ssh user2@10.0.0.2
```

Il client OpenSSH richiede la chiave privata dell'utente per l'autenticazione. Comunque tale chiave non viene inviata tramite la connessione sicura tra il client e il server. Viene invece usata per aprire il file `id_dsa` e generare una firma, inviata poi al server. Se il server ha una copia della chiave pubblica che può essere utilizzata per la verifica della firma, l'utente viene autenticato.

In questo esempio, l'utente utilizza una chiave DSA (si possono usare anche le chiavi RSA) e vede il prompt seguente:

```
Enter passphrase for DSA key '/home/user1/.ssh/id_dsa':
```

Se l'autenticazione della chiave pubblica fallisce per qualsiasi ragione (se per esempio la chiave è inserita in modo scorretto o le informazioni di autenticazione non sono presenti sul sul server) viene provato un'altro tipo di autenticazione. Nel nostro esempio il server OpenSSH consente a user1 di autenticarsi utilizzando la password di user2 perché la firma inviata non coincide con la chiave pubblica memorizzata da user2:

```
user2@machine2's password:
```

Con l'inserimento di una password corretta, compare il prompt della shell. Naturalmente user2 deve già avere un account sulla macchina 10.0.0.2, affinché l'autenticazione della password funzioni.

```
Last login: Mon Apr 15 13:27:43 2001 from machine1
[user2@machine2 user2]$
```

A questo punto l'utente interagisce con la shell come con `telnet` o `rsh`, l'unica differenza consiste nel fatto che la comunicazione è cifrata.

Altri tool SSH, come `scp` e `sftp`, funzionano in modo simile a `rcp` e `ftp`. Per maggiori informazioni ed esempi sull'uso di questi e altri comandi SSH, consultate la *Official Red Hat Linux Customization Guide*.

11.3 Livelli di sicurezza SSH

Il protocollo SSH consente a ogni programma client e server creato in base alle specifiche del protocollo di comunicare in modo sicuro e di essere utilizzato in modo interscambiabile.

Attualmente esistono due diverse varietà di SSH. La versione 1 contiene diversi algoritmi di cifratura brevettati (comunque molti brevetti sono scaduti) e una "falla" nella sicurezza che potenzialmente permette di inserire informazioni nel flusso di dati. È consigliabile utilizzare i server e client compatibili con la versione 2, se possibile.

OpenSSH comprende un supporto per la versione 2 (e chiavi di cifratura DSA disponibili gratutitamente). OpenSSH e le librerie di cifratura OpenSSL forniscono una serie completa di funzionalità per la sicurezza.

Entrambe le versioni del protocollo SSH (1 e 2) utilizzano livelli di sicurezza simili per consolidare l'integrità delle comunicazioni da diversi sistemi. Ogni livello fornisce il proprio tipo di protezione, che, se usato insieme agli altri, rafforza l'intero sistema di sicurezza per le comunicazioni.

11.3.1 Livello di trasporto

Lo scopo principale del livello di trasporto è facilitare una comunicazione sicura tra due host al momento dell'autenticazione e subito dopo. Il livello di trasporto, che utilizza di solito il protocollo TCP/IP, cerca di raggiungere tale scopo cifrando e decifrando i dati, verificando che il server corrisponda alla macchina corretta per l'autenticazione e fornendo la protezione integrale di pacchetti di dati durante la trasmissione e la ricezione. Inoltre il livello di trasporto può fornire la compressione dei dati, aumentando la velocità di trasferimento delle informazioni.

Quando un client contatta un server utilizzando un protocollo SSH, vengono "negoziati" diversi punti importanti, in modo che i due sistemi possano creare correttamente il livello di trasporto:

- Scambio delle chiavi
- Algoritmo della chiave pubblica
- Algoritmo della cifratura simmetrica
- Algoritmo per l'autenticazione del messaggio
- Algoritmo hash

Durante lo scambio delle chiavi il server si fa riconoscere dal client tramite una **chiave host**. Naturalmente, se questo client non ha mai comunicato con questo particolare server, non sarà in grado di riconoscere la chiave del server. OpenSSH aggira questo problema autorizzando il client ad accettare la chiave host del server la prima volta che avviene una connessione SSH. Nelle connessioni successive, la chiave host del server può essere verificata con una versione salvata sul client, in modo che il client sia "sicuro" di comunicare con il server corretto.

Il metodo di verifica della chiave host usato da OpenSSH non è perfetto. Un malintenzionato potrebbe "mascherarsi" da server durante il contatto iniziale, poiché il sistema non conosce necessariamente la differenza tra il server corretto e quello "mascherato". Purtroppo, finché non si diffonderà un metodo di distribuzione delle chiavi host migliore, questo metodo insicuro è comunque meglio di niente.

SSH è stato ideato per funzionare con quasi ogni tipo di algoritmo per le chiavi pubbliche o di formato in codice. Lo scambio iniziale delle chiavi genera due valori (un valore hash, usato per gli scambi e un valore segreto condiviso) e i due sistemi iniziano immediatamente a calcolare nuove chiavi e algoritmi per proteggere l'autenticazione e i dati futuri inviati tramite la connessione.

11.3.2 Autenticazione

Dopo aver costruito un tunnel sicuro per inviare le informazioni da un sistema all'altro, il server indica al client i diversi metodi di autenticazione supportati, come per esempio una firma privata codificata o la digitazione di una password. Il client poi tenta di autenticarsi al server tramite uno dei metodi supportati.

Poiché i server possono essere configurati per autorizzare diversi tipi di autenticazione, questo metodo offre un ottimo controllo da entrambe le parti. Il server stabilisce i metodi di cifratura supportati e il client può scegliere l'ordine dei metodi di autenticazione da utilizzare. Grazie alla sicurezza del livello di trasporto SSH, è possibile utilizzare senza problemi perfino metodi di autenticazione apparentemente non sicuri, come l'autenticazione basata sull'host,

La maggior parte degli utenti che richiedono una shell sicura utilizzano una password per l'autenticazione. A differenza di altri schemi di autenticazione per la sicurezza, la password viene trasmessa al server in chiaro. Comunque, dal momento che l'intera password è cifrata quando si sposta sul livello di trasporto, può essere inviata in modo sicuro attraverso qualsiasi rete.

11.3.3 Connessione

Ad autenticazione avvenuta, vengono aperti dei **canali** multipli selezionando [3]la singola connessione tra i due sistemi. Ognuno di questi canali gestisce la comunicazione per una diversa sessione di terminale, le informazioni di X11 inviate oppure ogni altro servizio che cerca di utilizzare la conessione SSH.

[3] Una connessione "multiplata" è costituita da diversi segnali inviati tramite un supporto condiviso. Con SSH, canali differenti vengono inviati tramite una connessione comune sicura.

Entrambi i client e i server possono creare un nuovo canale, assegnandogli un numero diverso a ogni estremità. Quando una parte tenta di aprire un nuovo canale, viene inviato insieme alla richiesta il suo numero per il canale. Questa informazione viene memorizzata dall'altra parte e utilizzata per indirizzare una particolare comunicazione di servizio per il canale. In questo modo i diversi tipi di sessione non si disturbano a vicenda e i canali possono essere chiusi senza interrompere la connessione primaria SSH tra i due sistemi.

I canali supportano inoltre il controllo del flusso, che gli consente di inviare e ricevere i dati ordinatamente. In questo modo i dati non sono inviati attraverso il canale finché l'host non riceve il messaggio che il canale è in grado di ricevere.

I canali sono particolarmente utili con X11 forwarding e TCP/IP port forwarding (SSH). È possibile configurare in modo diverso canali separati, forse per usare una dimensione del pacchetto massima differente oppure per trasferire un tipo particolare di dati. Ciò consente a SSH una gestione flessibile dei diversi tipi di connessioni remote, come per esempio tramite reti pubbliche o collegamenti LAN ad alta velocità, senza dover modificare l'infrastruttura fondamentale del protocollo. Il client e il server stabiliscono la configurazione di ogni canale entro la connessione SSH in modo automatico.

11.4 File di configurazione OpenSSH

OpenSSH possiede due diversi tipi di file per la configurazione, uno per i programmi client (`ssh`, `scp` e `sftp`) e l'altro per il servizio del server (`sshd`) posizionato in due aree diverse.

Le informazioni di configurazione SSH sono memorizzate nella directory `/etc/ssh`:

- `primes` — contiene gruppi Diffie-Hellman usati per lo scambio delle chiavi. In sostanza, questo scambio crea un valore segreto condiviso che non può essere determinato da una singola parte e viene usato per fornire l'autenticazione dell'host. Questo file è fondamentale per creare un livello di trasporto sicuro.
- `ssh_config` — il file di configurazione del client SSH, utilizzato per indirizzare il client SSH. Se un utente ha a disposizione il proprio file di configurazione nella directory home (`~/.ssh/config`), i valori di questo file hanno la priorità sui valori memorizzati in `/etc/ssh/ssh_config`.
- `sshd_config` — il file di configurazione per `sshd`.
- `ssh_host_dsa_key` — la chiave privata DSA utilizzata da `sshd`.
- `ssh_host_dsa_key.pub` — la chiave pubblicata DSA usata da `sshd`.
- `ssh_host_key` — la chiave privata RSA utilizzata da `sshd` per la versione 1 del protocollo SSH.
- `ssh_host_key.pub` — la chiave pubblica RSA usata da `sshd` per la versione 1 del protocollo SSH.

- `ssh_host_rsa_key` — la chiave privata RSA usata da `sshd` per la versione 2 del protocollo SSH.
- `ssh_host_rsa_key.pub` — la chiave pubblica RSA utilizzato da `sshd` per la versione 2 del protocollo SSH.

Le informazioni di configurazione SSH specifiche dell'utente sono memorizzate nella directory home dell'utente all'interno della sottodirectory `.ssh`:

- `authorized_keys2` — il file che contiene una lista delle chiavi pubbliche "autorizzate". Se un utente che si sta connettendo può provare di conoscere la chiave privata che corrisponde a una delle chiavi pubbliche, viene autenticato. Tuttavia questo è un metodo di autenticazione opzionale.
- `id_dsa` — contiene l'identità di autenticazione DSA dell'utente.
- `id_dsa.pub` — la chiave pubblica DSA dell'utente.
- `known_hosts2` — memorizza le chiavi host DSA dei server a cui l'utente si collega tramite SSH. Se un server possiede delle chiavi host modificate in modo autorizzato, in caso di reinstallazione di Red Hat Linux, all'utente viene notificato che la chiave host, memorizzata nel file `known_hosts2` e relativa a questo host non corrisponde. A questo punto l'utente deve cancellare la chiave dell'host in `known_hosts` per memorizzare la nuova chiave host per questo sistema. Il file `known_hosts2` è fondamentale per garantire che il client si connetta al server corretto. Se la chiave dell'host è stata modificata e non sapete perché, contattate l'amministratore di sistema dell'host per assicurarvi che l'host non sia stato compromesso.

Per informazioni inerenti le diverse direttive disponibili nei file di configurazione SSH, consultate le pagine man per `ssh` e `sshd`.

11.5 Più di una Secure Shell

Un'interfaccia a linea di comando sicura è solo uno dei tanti modi in cui una SSH può essere utilizzata. Considerata la quantità esatta della larghezza di banda, le sessioni X11 possono essere indirizzate tramite un canale SSH. Oppure, utilizzando il TCP/IP forwarding, le connessioni di porta tra i sistemi, un tempo insicure, possono essere mappate per canali SSH specifici.

11.5.1 X11 Forwarding

Aprire una sessione X11 tramite una connessione SSH stabilita è facile quanto avviare un programma X quando un client esegue già X sul vostro host. Quando un programma X viene lanciato dal prompt della secure shell, il client e il server SSH creano un nuovo canale sicuro all'interno dell'attuale connessione SSH e i dati del programma X vengono inviati tramite questo canale alla vostra macchina client come se foste connessi al server X mediante un terminale locale.

Come potrete immaginare X11 forwarding può essere molto utile. Per esempio, potete usarlo per creare una sessione sicura e interattiva con l'interfaccia grafica utente `up2date` sul server per aggiornare in modo selettivo i pacchetti (se avete installato sul vostro server i pacchetti Red Hat Network necessari). Per farlo, connettetevi semplicemente al server utilizzando `ssh` e digitate:

```
up2date
```

Vi viene richiesto di inserire la password di root per il server. Compare ora il Red Hat Update Agent e potete così aggiornare i vostri pacchetti sul server proprio come se foste seduti davanti alla macchina.

Sia i dati di elaborazione richiesti per cifrare e decifrare le informazioni sicure inviate tramite il canale che la larghezza di banda aggiuntiva necessaria per inviare dati cifrati dell'applicazione X potrebbero essere importanti. È importante effettuare dei test adeguati per assicurarsi che il programma X sia ancora utilizzabile, in base alle condizioni del vostro hardware e della larghezza di banda.

11.5.2 TCP/IP forwarding

TCP/IP forwarding funziona con il client SSH, il quale richiede che una porta particolare sul client o sul server venga mappata tramite la connessione SSH esistente.

Per mappare una porta locale sul client verso una porta remota sul server, dovete innazitutto conoscere i numeri delle porte di entrambe le macchine. È persino possibile mappare due porte diverse e non standard.

Per creare un canale TCP/IP forwarding che attenda le connessioni sull'host locale, utilizzate il seguente comando (tutto su una riga):

```
ssh -L <porta-locale>:<nomehost-remoto>:<porta-remota>
        <nomeutente>@<nomeutente>
```

Nota Bene

Per impostare TCP/IP forwarding e avviare servizi su porte inferiori alla 1024 è necessario l'accesso di root.

Se per esempio desiderate controllare la vostra posta su un server chiamato mail.domain.com utilizzando il protocollo POP e se il server ha a disposizione SSH, potete utilizzare il comando seguente per configurare TCP/IP forwarding:

```
ssh -L 1100:mail.domain.com:110 mail.domain.com
```

Dopo aver posizionato TCP/IP tra le due macchine, potete indirizzare il vostro client di posta POP per utilizzare l'host locale come server POP e indicare la porta 110 per il controllo di posta nuova. Qualsiasi richiesta inviata alla porta 1100 sul vostro sistema sarà indirizzata in modo sicuro al server mail.domain.com.

Se sul server mail.domain.com non è in esecuzione un demone server SSH ma potete collegarvi tramite SSH a una macchina vicina, potete ancora utilizzare SSH, forse tramite un firewall, per rendere sicura quella parte della connessione POP avvenuta tramite reti pubbliche. È necessario un comando leggermente diverso:

```
ssh -L 1100:mail.domain.com:110 other.domain.com
```

In questo esempio, inviate la vostra richiesta POP dalla porta 1100 sulla vostra macchina tramite la connessione SSH a other.domain.com sulla porta 22. A questo punto other.domain.com si connette alla porta 110 su mail.domain.com per permettervi di controllare l'arrivo di nuova posta. Solo la connessione tra il vostro sistema e other.domain.com è sicura, ma in molte situazioni, ciò è sufficiente per trasmettere e ricevere informazioni in modo sicuro attraverso reti pubbliche garantendo una sicurezza mai avuta prima.

Naturalmente negli esempi descritti sopra, dovete essere in grado di autenticarvi al server SSH per eseguire il TCP/IP forwarding. Assicuratevi di poter eseguire i comandi SSH normali prima di tentare la configurazione di TCP/IP forwarding.

TCP/IP forwarding può risultare particolarmente utile per ricevere informazioni in modo sicuro tramite i firewall di rete. Se il firewall è configurato per consentire il traffico SSH tramite la porta standard (22), ma blocca l'accesso tramite le altre porte, una connesssione tra due host che usano porte bloccate è comunque possibile se si reindirizza la comunicazione tramite una connessione SSH tra i due host.

Nota Bene

Questa operazione può rivelarsi molto pericolosa. L'utilizzo di un TCP/IP forwarding per inoltrare connessioni in questo modo consente a qualsiasi utente sul sistema client di connettersi al servizio a cui state inviando le connessioni. Tutto ciò può essere rischioso se il sistema client viene compromesso.

Prima di usare il TCP/IP forwarding, consultate l'amministratore dei firewall. Gli amministratori di sistema che si occupano di TCP/IP forwarding possono disabilitare questa funzione sul server specificando il parametro `No` per la riga **AllowTcpForwarding** nel file `/etc/ssh/sshd_config` e riavviando il servizio `sshd`.

11.6 SSH per le connessioni remote

Per rendere SSH davvero efficace nel proteggere le vostre connessioni di rete, è necessario smettere di utilizzare tutti i protocolli di connessione non sicuri, come `telnet` e `rsh`. Altrimenti una password protetta tramite `ssh` può essere individuata alla prima connessione via `telnet`.

Per disabilitare i metodi di connessione poco sicuri utilizzate il comando `ntsysv` o `chkconfig` per garantire che questi servizi non vengano attivati all'avvio del sistema. Se volete utilizzare `ntsysv` per configurare i servizi che si avviano ai runlevel 2, 3 e 5, digitate il comando:

```
/usr/sbin/ntsysv 235
```

All'interno di `ntsysv` potete impedire l'attivazione dei servizi deselezionandoli. La [Barra spaziatrice] consente di attivare o disattivare tali servizi. È consigliabile deselezionare almeno `telnet`, `rsh`, `ftp` e `rlogin`. Alla fine fate clic sul pulsante **OK** per salvare le modifiche. Per ulteriori informazioni sull'uso di questa utility, consultate la relativa pagina man.

Le modifiche effettuate con `ntsysv` verranno applicate solo riavviando il sistema o cambiando il runlevel. Se disabilitate i servizi usati con `xinetd`, occorre riavviare quest'ultimo. `rlogin`, `rsh` e `telnet` sono controllati per default da `xinetd`. Per riavviare `xinetd`, digitate:

```
/sbin/service xinetd restart
```

I servizi non utilizzati con `xinetd` vanno disattivati manualmente, a meno che il sistema non venga riavviato dopo l'uso di `ntsysv`. Per interrompere un servizio, userete probabilmente un comando simile al seguente:

```
/sbin/service <nome-servizio> stop
```

Dopo il riavvio di `xinetd` e la disattivazione di ogni altro servizio, i metodi di connessione disabilitati non saranno più accettati dal vostro sistema. Se disabilitate tutti i metodi di connessione remoti diversi dal demone `sshd`, gli utenti dovranno usare un'applicazione client SSH per connettersi al server.

12 Controllo degli accessi e dei privilegi

Secondo una politica di sicurezza corrente, la sicurezza del sistema si basa sull'incapacità di gruppi o utenti di fare più di quel che dovrebbero. La maggior parte dei cambiamenti quotidiani riguardano il controllo degli accessi e dei privilegi concessi a gruppi e utenti, (vedere il Capitolo 2, *Utenti e gruppi* per maggiori informazioni sulla creazione e la configurazione corrette di gruppi e utenti).

Tuttavia, molte organizzazioni che utilizzano Red Hat Linux richiedono maggiore sicurezza o particolari configurazioni che permettono di ottenere un accesso più o meno elevato alle applicazioni o ai dispositivi di sistema. Questa sezione fornisce alcuni metodi per ottenere un livello di accesso e di privilegi adeguato alle proprie necessità.

12.1 Utility shadow

Se siete in un ambiente multi-utente e non usate né PAM né Kerberos, dovreste considerare l'utilizzo delle utility shadow (chiamate anche **password shadow**) per l'alto livello di protezione che offrono ai file di autenticazione del sistema. Durante l'installazione di Red Hat Linux, la protezione del sistema fornita dalle password shadow è attivata per default, così come lo sono le **password MD5** (metodo indiscutibilmente più sicuro della cifratura per immagazzinare le password sul sistema).

Rispetto al metodo standard usato per immagazzinare le password sui sistemi UNIX e Linux, le password shadow offrono alcuni vantaggi quali:

- Un metodo che permette di migliorare la sicurezza del sistema spostando le password cifrate da `/etc/passwd` verso `/etc/shadow`, leggibile solo da root.
- Informazioni relative all'invecchiamento della password (quanto tempo è trascorso dall'ultima volta che la password è stata modificata).
- Un controllo sulla durata di validità della password (quando l'utente la deve modificare).
- La possibilità di usare il file `/etc/login.defs` per rafforzare una regola di sicurezza, specialmente relativa all'invecchiamento della password.

Il pacchetto `shadow-utils` contiene alcune utility che supportano:

- La conversione di password normali in password shadow e viceversa (`pwconv`, `pwunconv`).
- La verifica della password, del gruppo e dei file shadow associati (`pwck`, `grpck`).
- Metodi standard per aggiungere, cancellare e modificare gli account utenti (`useradd`, `usermod` e `userdel`).
- Metodi standard per aggiungere, cancellare e modificare i gruppi utenti (`groupadd`, `groupmod` e `groupdel`).

- Metodi standard di amministrazione del file `/etc/group` tramite il comando `gpasswd`.

Nota Bene

Queste utility offrono altri vantaggi:

- Le utility funzionano correttamente indipendentemente dallo stato di attivazione/disattivazione dello shadowing.
- Le utility sono state leggermente modificate per supportare lo schema del gruppo privato utente di Red Hat. Per una descrizione delle modifiche, consultate la pagina man `useradd`. Per maggiori informazioni sui gruppi privati utente, consultate la Sezione 2.4, *Gruppi privati utente*.
- Lo script `adduser` è stato sostituito con il collegamento simbolico a `/usr/sbin/useradd`.
- I tool contenuti nel pacchetto `shadow-utils` non sono compatibili né con Kerberos né con LDAP. I nuovi utenti saranno solo locali. Per maggiori informazioni su Kerberos e LDAP, consultate il Capitolo 9, *Kerberos 5 su Red Hat Linux* e il Capitolo 4, *LDAP (Lightweight Directory Access Protocol)*.

12.2 Configurazione dell’accesso alla console

Quando gli utenti standard (non root) si collegano a un computer in modo locale, ricevono due tipi di autorizzazione speciale:

1. Eseguono alcuni programmi che non possono eseguire in altro modo.
2. Accedono ad alcuni file (solitamente file device usati per accedere a dischetti, CD-ROM ecc.) a cui non possono accedere in altro modo.

Poiché su un unico computer ci sono più console e più utenti si possono collegare contemporaneamente in modo locale, uno degli utenti deve "vincere" la gara per accedere ai file. Il primo utente che si collega alla console diventa proprietario dei file. Una volta che il primo utente si è scollegato, il secondo utente che si collega diventa proprietario dei file.

Invece, *ogni* utente che si collega alla console è autorizzato a lanciare programmi che eseguono task normalmente riservati all’utente root. Se X Window è in esecuzione, queste azioni possono essere incluse come voci di menu in un’interfaccia utente grafica. Alla consegna, i programmi accessibili dalla console includono `halt`, `poweroff` e `reboot`.

12.2.1 Disattivazione di Shutdown tramite Ctrl-Alt-Canc

`/etc/inittab` specifica per default che il sistema è impostato in modo da fermarsi e riavviarsi tramite la combinazione di tasti [Ctrl]-[Alt]-[Canc]. Se desiderate disattivare completamente questa funzione, commentate il link seguente in `/etc/inittab`:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Altrimenti potete decidere di dare solo ad alcuni utenti non root l'autorizzazione di fermare il sistema dalla console usando la combinazione di tasti [Ctrl]-[Alt]-[Canc]. Per limitare questo privilegio ad alcuni utenti, seguite questa procedura:

1. Aggiungete l'opzione `-a` alla linea `/etc/inittab`:

   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```

   `-a` chiede a `shutdown` di cercare il file `/etc/shutdown.allow`, creato nel prossimo punto.

2. Create un file chiamato `shutdown.allow` in `/etc`. Il file `shutdown.allow` deve elencare i nomi utente di tutti gli utenti che possono fermare il sistema con la combinazione di tasti [Ctrl]-[Alt]-[Canc]. Il file `/etc/shutdown.allow` è un elenco di nomi utente posizionati uno per riga:

   ```
   stefano
   giacomo
   sofia
   ```

Nel file `shutdown.allow` di esempio, Stefano, Giacomo e Sofia possono fermare il sistema dalla console usando la combinazione di tasti [Ctrl]-[Alt]-[Canc]. Quando viene usata questa combinazione di tasti, il file `shutdown -a` in `/etc/inittab` verifica se qualche utente in `/etc/shutdown.allow` (o root) è collegato a una console virtuale. In caso positivo, l'arresto del sistema prosegue, in caso negativo, un messaggio di errore viene trasmesso alla console del sistema.

Per maggiori informazioni, consultate la pagina man di `shutdown`.

12.2.2 Disattivazione dell'accesso ai programmi della console

Per disattivare l'accesso degli utenti ai programmi della console, eseguite questo comando come root:

```
rm -f /etc/security/console.apps/*
```

In ambienti dove la console è protetta in altro modo (le password BIOS e LILO sono impostate, la combinazione di tasti [Ctrl]-[Alt]-[Canc] è disattivata, i pulsanti di accensione e di reset sono disabilitati ecc.), non è raccomandabile autorizzare l'accesso di utenti alla console dove possono eseguire `poweroff`, `halt` e `reboot`, accessibili dalla console per default.

Per annullare queste funzioni, eseguite questo comando come root:

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

12.2.3 Disattivazione di qualsiasi accesso alla console

Il modulo PAM `pam_console.so` gestisce l'autenticazione e le autorizzazioni dei file della console (vedere il Capitolo 8, *Moduli di autenticazione PAM* per maggiori informazioni sulla configurazione di PAM). Se desiderate disattivare qualsiasi accesso alla console, compreso ai programmi e ai file, commentate tutte le righe che si riferiscono a `pam_console.so` nella directory `/etc/pam.d` seguendo questo script:

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

12.2.4 Configurazione della console

Il modulo `pam_console.so` utilizza il file `/etc/security/console.perms` per determinare le autorizzazioni di accesso alla console degli utenti. La sintassi del file è molto flessibile; potete modificare il file affinché queste istruzioni non vengano più applicate. Tuttavia, il file di default contiene una riga simile a:

```
 <console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

Quando gli utenti effettuano il log in, sono collegati a una specie di terminale, un server X chiamato `:0` o `mymachine.example.com:1.0` oppure un dispositivo come `/dev/ttyS0` o `/dev/pts/2`. Per default conviene determinare quali console virtuali e server X saranno considerati locali, ma se volete configurare il terminale seriale vicino a voi sulla porta `/dev/ttyS1` affinché sia anch'esso locale, modificate la riga nel modo seguente:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

12.2.5 Rendere i file accessibili dalla console

`/etc/security/console.perms` contiene una sezione simile a:

```
<floppy>=/dev/fd[0-1]* \
    /dev/floppy/*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
    /dev/mixer* /dev/sequencer \
    /dev/sound/*
<cdrom>=/dev/cdrom* /dev/cdwriter*
```

Se necessario potete aggiungere delle righe. Assicuratevi che le linee che aggiungete si riferiscano ai dispositivi corretti. Per esempio, potete aggiungere:

```
<scanner>=/dev/sga
```

Assicuratevi ovviamente che `/dev/sga` corrisponda veramente al vostro scanner e non, per esempio, al vostro disco fisso.

Questo è il primo passo. Nel secondo passo dovete decidere dell'"avvenire" di questi file. Esaminate l'ultima sezione di `/etc/security/console.perms`:

```
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound>  0640 root
<console> 0600 <cdrom>  0600 root.disk
```

e aggiungete una riga:

```
<console> 0600 <scanner> 0600 root
```

In seguito, quando vi collegherete alla console, riceverete la proprietà del dispositivo `/dev/sga` e le vostre autorizzazioni saranno 0600 (leggibili e scrivibili solo da voi). Quando vi scollegherete, il dispositivo sarà di proprietà del root il quale disporrà ancora delle autorizzazioni 0600 (leggibili e scrivibili solo da root).

12.2.6 Attivazione dell'accesso alla console per altre applicazioni

Se volete rendere altre applicazioni accessibili agli utenti della console, dovete semplicemente lavorare un pò di più.

Per prima cosa, l'accesso alla console *solo* funziona per le applicazioni che si trovano in `/sbin` o `/usr/sbin`, perciò l'applicazione che volete eseguire si deve trovare anch'essa lì. Dopo esservene accertati, seguite questa procedura:

1. Create un link fra il nome della vostra applicazione, come il nostro programma di esempio *`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 PAM per il servizio *foo* in `/etc/pam.d/`. Vi consigliamo di iniziare con una copia del servizio di arresto del file di configurazione PAM e di modificare il file se volete modificarne il comportamento:

```
cp /etc/pam.d/halt /etc/pam.d/foo
```

D'ora in poi l'esecuzione di `/usr/bin/`*foo* richiamerà `consolehelper` che, con l'aiuto di `/usr/sbin/userhelper`, autenticherà l'utente chiedendo la password utente se `/etc/pam.d/`*foo* è una copia di `/etc/pam.d/halt` (nel caso contrario, farà esattamente ciò che è specificato in `/etc/pam.d/`*foo*), quindi esegue `/usr/sbin/`*foo* con delle autorizzazioni root.

12.3 Gruppo `floppy`

Se, per qualche motivo, l'accesso alla console non è adeguato alle vostre esigenze e se dovete dare a utenti non root l'accesso al lettore floppy del vostro sistema, potete farlo tramite il gruppo `floppy`. Aggiungete gli utenti al gruppo `floppy` usando il tool che preferite. Ecco un esempio di come `gpasswd` può essere usato per aggiungere l'utente Gianni al gruppo `floppy`:

```
[root@bigdog root]# gpasswd -a gianni floppy
Adding user Gianni to group floppy
[root@bigdog root]#
```

Adesso l'utente Gianni può accedere al lettore floppy del sistema.

Parte III Apache

13 Utilizzo di Apache come server Web sicuro

13.1 Introduzione

Questo capitolo fornisce informazioni di base sull'installazione del server Apache World Wide Web (WWW o Web) con il modulo mod_ssl e la libreria e il toolkit OpenSSL. La combinazione di questi tre elementi forniti con Red Hat Linux sarà chiamata server Web sicuro o semplicemente server sicuro.

I server Web forniscono pagine Web ai browser. Netscape Navigator e Microsoft Internet Explorer sono esempi di browser conosciuti. In termini più tecnici, i server e i browser comunicano usando il protocollo HTTP, lo standard Internet per le comunicazioni Web. Quando l'utente fa clic su una pagina Web, viene inoltrata una richiesta HTTP a un server Web, che riceve la richiesta e fornisce il contenuto, per es. una pagina HTML, uno script CGI o una pagina Web generata in modo dinamico da un database. Se il server Web non può rispondere alla richiesta, invia un messaggio di errore. Apache, il server presente in Red Hat Linux, è il server Web più usato su Internet (vedere la pagina Web http://www.netcraft.net/survey).

Apache ha una struttura modulare, è infatti composto da vari "pezzi" di codice separati che corrispondono a diversi aspetti o funzionalità del server Web. L'aspetto modulare è stato progettato in modo che qualsiasi sviluppatore potesse scrivere il proprio pezzo di codice. I codici degli sviluppatori, chiamati moduli, possono facilmente essere integrati nel server Apache.

Il modulo mod_ssl è un modulo per la sicurezza di Apache. Utilizza i tool forniti dal progetto OpenSSL per aggiungere una funzione molto importante ad Apache: la possibilità di cifrare le comunicazioni. Tuttavia, utilizzando il protocollo "standard" HTTP le comunicazioni tra il browser e il server Web vengono gestite in chiaro, perciò le informazioni trasferite via rete possono venire intercettate.

Il progetto OpenSSL include un toolkit che implementa i protocolli Secure Sockets Layer (SSL) e Transport Layer Security (TLS). Il protocollo SSL viene utilizzato per rendere sicure le trasmissioni su internet. Il protocollo TLS è ormai uno standard per le comunicazioni private e sicure su Internet. I tool OpenSSL vengono utilizzati dal modulo mod_ssl per garantire la sicurezza nelle comunicazioni Web.

Questo capitolo non fornisce una documentazione completa ed esaustiva per ciascuno di questi programmi. Quando possibile, questa guida vi indicherà dove trovare documentazione più tecnica in merito a questi soggetti.

Questo capitolo vi mostra come installare questi programmi. Imparerete inoltre a generare una richiesta di chiave privata e di certificato, a creare il certificato da voi firmato e a installare un certificato da usare con il vostro server Web sicuro.

13.2 Ringraziamenti

Il server Web sicuro include:

- Un software sviluppato dal gruppo di Apache per l'utilizzo nel progetto Apache HTTP (http://httpd.apache.org)
- Il modulo per la sicurezza mod_ssl sviluppato da Ralf S. Engelschall (http://www.modssl.org)
- Il toolkit OpenSSL, sviluppato da Mark J. Cox, Ralf S. Engelschall, Dr. Stephen Henson e Ben Laurie (http://www.openssl.org)
- Un software basato sul server HTTP Apache-SSL sviluppato da Ben Laurie (http://www.apache-ssl.org)
- Un software basato sulla cifratura SSLeay scritto da Eric Young e Tim Hudson.

Red Hat ringrazia tutti per la collaborazione.

13.3 Panoramica sui pacchetti relativi alla sicurezza

Per installare il server sicuro occorrono almeno tre pacchetti.

`apache`

Il pacchetto `apache` contiene il demone `httpd` e le utility, i file di configurazione, i moduli Apache, le pagine man e altri file usati dal server Apache.

`mod_ssl`

Il pacchetto `mod_ssl` include il modulo mod_ssl, che fornisce il supporto per la cifratura per il server Web Apache tramite i protocolli Secure Sockets Layer (SSL) e Transport Layer Security (TLS).

`openssl`

Il pacchetto `openssl` contiene il toolkit OpenSSL. Questo pacchetto implementa i protocolli SSL e TLS e include una libreria per la cifratura.

Red Hat Linux contiene inoltre dei pacchetti che aggiungono funzionalità al vostro server sicuro:

`apache-devel`

Il pacchetto `apache-devel` contiene i file Apache include, i file header a l'utility APXS, necessari per caricare moduli extra non forniti in questo prodotto. Per maggiori informazioni sul caricamento dei moduli nel server Web sicuro tramite la funzionalità DSO di Apache, consultate la Sezione 14.3, *Aggiungere moduli al server*.

Se non volete caricare altri moduli nel server Web sicuro, non installate questo pacchetto.

apache-manual

Il pacchetto apache-manual contiene la *Apache 1.3 User's Guide* in formato HTML. Questo manuale è anche disponibile via Web al sito http://httpd.apache.org/docs/.

Pacchetti OpenSSH

I pacchetti OpenSSH forniscono una serie di tool per le connessioni di rete e per effettuare login remoti. I tool OpenSSH cifrano tutto il traffico (comprese le password) e impediscono attacchi e intrusioni esterne.

Il pacchetto openssh include i file fondamentali richiesti dai programmi client OpenSSH e dal server OpenSSH. Il pacchetto openssh contiene anche scp, un valido sostituto per rcp (per copiare file fra macchine diverse) e ftp (per trasferire file fra macchine diverse).

Il pacchetto openssh-askpass supporta il display di una finestra di dialogo che richiede una password durante l'utilizzo dell'agente OpenSSH con autenticazione RSA.

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 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, ssh, un valido sostituito per rsh, slogin, un valido sostituto per rlogin (per il login remoto) e telnet (per comunicare con un altro host tramite il protocollo TELNET).

Per maggiori informazioni su OpenSSH, consultate il Capitolo 11, *Protocollo SSH* 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 necessari alla compilazione di applicazioni contenenti un supporto per vari algoritimi 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 Stunnel SSL. 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 sorgente del demone.

La Tabella 13–1, *Pacchetti di sicurezza* visualizza la posizione dei pacchetti del server sicuro e altri pacchetti relativi alla sicurezza contenuti in Red Hat Linux. Questa tabella indica se i pacchetti sono opzionali per l'installazione di un server sicuro.

Tabella 13–1 Pacchetti di sicurezza

Nome del pacchetto	Contenuto nel gruppo	Opzionale?
`apache`	Ambiente di sistema/Demoni	no
`mod_ssl`	Ambiente di sistema/Demoni	no
`openssl`	Ambiente di sistema/Librerie	no
`apache-devel`	Sviluppo/Librerie	sì
`apache-manual`	Documentazione	sì
`openssh`	Applicazioni/Internet	sì
`openssh-askpass`	Applicazioni/Internet	sì
`openssh-askpass-gnome`	Applicazioni/Internet	sì
`openssh-clients`	Applicazioni/Internet	sì
`openssh-server`	Ambiente di sistema/Demoni	sì
`openssl-devel`	Sviluppo/Librerie	sì
`stunnel`	Applicazioni/Internet	sì

13.4 Installazione del server sicuro

Per installare il server Web sicuro seguite una di queste procedure:

- *Durante l'installazione di Red Hat Linux* — Poiché il server Web sicuro è incluso nel sistema operativo Red Hat Linux, il metodo di installazione più semplice è durante l'installazione di Red Hat Linux. Per maggiori informazioni, consultate la Sezione 13.5, *Installazione del server sicuro con Red Hat Linux*.
- *Durante l'aggiornamento di Red Hat Linux tramite il programma di installazione* — se avete già una versione precedente di Red Hat Linux e volete aggiornarla alla Red Hat Linux 7.1, potete installare i pacchetti del server sicuro durante il processo di aggiornamento. Per maggiori informazioni, consultate la Sezione 13.6, *Aggiornamento da una versione precedente di Red Hat Linux*.

- *Installazione del server sicuro dopo l'installazione di Red Hat Linux 7.1* — se avete già installato Red Hat Linux 7.1, ma non avete installato i pacchetti per la funzionalità server sicuro, potete utilizzare la tecnologia RPM, Gnome-RPM o Kpackage per installare i pacchetti del server sicuro dal CD di Red Hat Linux. Per maggiori informazioni, consultate la Sezione 13.7, *Installazione del server sicuro dopo l'installazione di Red Hat Linux*.

Aggiornamento di Apache

Se volete aggiornare il server Web sicuro a partire da una versione precedente di Apache (incluso qualsiasi prodotto server sicuro di Red Hat) dovete prima capire alcuni punti relativi al processo di aggiornamento di Apache. Prima di iniziare l'aggiornamento, consultate la Sezione 13.8, *Aggiornamento da una versione precedente di Apache*.

13.5 Installazione del server sicuro con Red Hat Linux

Se volete installare il server sicuro durante l'installazione di Red Hat Linux, seguite le instruzioni contenute nel manuale di installazione corrispondente al vostro sistema. Se intendete usare il sistema Red Hat Linux come server sicuro, vi consigliamo di eseguire un'installazione Server o Personalizzata.

- Se scegliete un'installazione di classe Server, i pacchetti `apache`, `mod_ssl` e `openssl` vengono selezionati automaticamente. I pacchetti `stunnel` e `openssh`, che forniscono funzioni relative alla sicurezza, vengono anch'essi selezionati.
- Se scegliete un'installazione di classe Workstation (o Laptop, se disponibile per il vostro sistema), i pacchetti del server sicuro e quelli relativi alla sicurezza non vengono selezionati automaticamente, ma potete scegliere di installarli durante il processo personalizzato di selezione dei pacchetti.
- Se scegliete un'installazione di classe Personalizzata, dato che avete il controllo sui pacchetti da installare, dovete selezionare i pacchetti del server sicuro e quelli relativi alla sicurezza che desiderate installare.

Quando avete scelto la classe d'installazione, seguite le istruzioni e configurate il sistema. Arrivati alla sezione dedicata alla selezione dei gruppi di pacchetti, selezionate il gruppo **Server Web**. Questo gruppo include i pacchetti `apache` e `mod_ssl` che dovete installare per utilizzare il secure server. Poiché `openssl` dipende dal pacchetto `mod_ssl`, devono essere entrambi selezionati.

Se volete installare anche gli altri pacchetti legati alla sicurezza descritti nella Sezione 13.3, *Panoramica sui pacchetti relativi alla sicurezza* avrete bisogno di selezionarli. Scegliete **Selezione individuale dei pacchetti** nella schermata **Selezione dei gruppi di pacchetti**.

Selezionate i pacchetti relativi alla sicurezza che volete installare. La Tabella 13–1, *Pacchetti di sicurezza* contiene riferimenti che vi aiuteranno a trovarli.

Accertatevi di aver selezionato i pacchetti necessari e continuate con il processo di installazione. Terminata l'installazione, consultate la Sezione 13.9, *Panoramica sui certificati e la sicurezza*.

13.6 Aggiornamento da una versione precedente di Red Hat Linux

Se avete già una versione precedente di Red Hat Linux sul vostro sistema dovete aggiornarlo alla Red Hat Linux 7.1 anziché eseguire un'installazione completa. Selezionate **Aggiornamento** e seguite le istruzioni contenute nella guida di installazione. Durante l'aggiornamento assicuratevi che i pacchetti del server sicuro siano selezionati.

Quando eseguite un aggiornamento del vostro sistema Red Hat Linux il programma di installazione controlla quali pacchetti sono stati installati. Questi vengono automaticamente aggiornati alla versione Red Hat Linux 7.1 durante il processo di installazione. Ovviamente se non avete un pacchetto già installato il programma di installazione non lo installa, a meno che non personalizziate la scelta.

Se state aggiornando la versione Red Hat Linux 7.0 o una versione successiva e avete installato i pacchetti del server sicuro, il processo di aggiornamento aggiornerà, anche i pacchetti del server sicuro. Se invece non avete installato i pacchetti del server sicuro, selezionate i pacchetti `apache`, `mod_ssl` e `openssl` durante la personalizzazione dei pacchetti. Per istruzioni su come trovare i pacchetti, consultate la Sezione 13.6.1, *Personalizzazione dell'aggiornamento per installare il server sicuro*.

Se state aggiornando una versione Professional di Red Hat Linux per il mercato US/Canada dovete selezionare i pacchetti relativi al server sicuro. Probabilmente avete installato `apache` ma non `mod_ssl` né `openssl` poiché non erano inclusi in Red Hat Linux prima della Red Hat Linux 7.1. Personalizzate l'aggiornamento e scegliete `mod_ssl` e `openssl`. Per maggiori informazioni, consultate la Sezione 13.6.1, *Personalizzazione dell'aggiornamento per installare il server sicuro*.

Se aggiornate una versione internazionale di Red Hat Linux Professional e avete installato `apache`, `mod_ssl` e `openssl`, il programma di installazione seleziona e installa questi programmi automaticamente.

Se state aggiornando la versione internazionale di Red Hat Linux Professional ma non avete `apache`, né `mod_ssl` o `openssl`, personalizzate l'aggiornamento e selezionate questi pacchetti. Per informazioni su come trovare i pacchetti, consultate la Sezione 13.6.1, *Personalizzazione dell'aggiornamento per installare il server sicuro*.

13.6.1 Personalizzazione dell'aggiornamento per installare il server sicuro

Se avete bisogno di personalizzare il vostro processo di aggiornamento, seguite le istruzioni contenute nella guida di installazione. Scegliete **Aggiornamento** come **Tipo di installazione** e **Selezione dei pacchetti da aggiornare**. In seguito selezionate i pacchetti da installare, come spiegato nella guida di installazione. La Tabella 13–1, *Pacchetti di sicurezza* fornisce la posizione dei pacchetti relativi al server sicuro e indica se tali pacchetti sono opzionali.

Dopodiché, se state aggiornando anche una versione di Apache, consultate la Sezione 13.8, *Aggiornamento da una versione precedente di Apache*. Se non state effettuando un aggiornamento di Apache, proseguite con la Sezione 13.9, *Panoramica sui certificati e la sicurezza*.

13.7 Installazione del server sicuro dopo l'installazione di Red Hat Linux

Se avete installato Red Hat Linux 7.1 senza aver installato i pacchetti server sicuro, e poi successivamente avete deciso che volete installarli, potete farlo. Il modo più semplice prevede l'utilizzo dell'RPM, di Gnome-RPM o di Kpackage.

13.7.1 Arresto di tutti i processi attivi del server Web

Se avete un server Web attivo sul sistema, fermatelo prima di installare server Web sicuro;. Se avete un server Apache attivo, fermatelo digitando uno o entrambi i comandi seguenti:

```
/etc/rc.d/init.d/httpsd stop
/etc/rc.d/init.d/httpd stop
```

13.7.2 Utilizzo di Gnome-RPM o Kpackage

Se state utilizzando GNOME o KDE potete usare un programma grafico come Gnome-RPM o Kpackage per installare i pacchetti del server sicuro.

Maggiori informazioni sull'uso di Gnome-RPM sono contenute nella *Official Red Hat Linux Getting Started Guide*. Maggiori informazioni sull'uso di Kpackage sono riportate nella pagina Web *Kpackage Handbook* all'indirizzo http://www.general.uwa.edu.au/u/toivo/kpackage.

Una volta installati i pacchetti necessari, create la vostra chiave e richiedete un certificato seguendo le istruzioni contenute nella Sezione 13.9, *Panoramica sui certificati e la sicurezza*.

13.7.3 Utilizzo dell'RPM

I pacchetti del server Web sicuro sono in formato RPM, perciò potete installarli usando RPM. Per maggiori informazioni sull'RPM, consultate la *Official Red Hat Linux Customization Guide*. Se avete dubbi sui pacchetti da installare, consultate la Tabella 13–1, *Pacchetti di sicurezza*.

Una volta installati i pacchetti del server sicuro, consultate la Sezione 13.8, *Aggiornamento da una versione precedente di Apache* se state aggiornando una versione di Apache. Altrimenti, proseguite con la Sezione 13.9, *Panoramica sui certificati e la sicurezza*.

13.8 Aggiornamento da una versione precedente di Apache

Se durante l'installazione dei pacchetti del server sicuro aggiornate Apache, prestate attenzione a quanto segue:

- Nella versione di Apache fornita in Red Hat Linux 7.1, la `DocumentRoot` è `/var/www/html`.
- Se avete personalizzto il file di configurazione Apache (`httpd.conf`), vorrete sapere cosa ne sarà della vostra personalizzazione durante il processo di aggiornamento.

13.8.1 Dove si trova la DocumentRoot?

La `DocumentRoot` è la directory sul vostro sistema che ha al suo interno la maggior parte delle pagine Web fornite dal vostro server Apache. La `DocumentRoot` è impostata all'interno del file di configurazione Apache `httpd.conf`. Per maggiori informazioni sulla `DocumentRoot`, consultate la Sezione 14.2.28, *`DocumentRoot`* .

Nelle versioni precedenti Red Hat Linux 7.0, l'Apache fornita usava `/home/httpd/html` come `DocumentRoot`. Nella versione di default (non sicura) del file di configurazione Apache, la `DocumentRoot` è `/usr/local/apache/htdocs`. È inoltre possibile che abbiate usato una `DocumentRoot` completamente diversa. Tuttavia, in Red Hat Linux 7.1 la `DocumentRoot` di default è `/var/www/html`.

Tutte le pagine Web che non si trovano alla nuova `DocumentRoot` non verranno distribuite da Apache incluso in Red Hat Linux 7.1 nella sua configurazione di default. Dovete compiere uno dei seguenti passi:

Spostate tutti i file dalla vecchia `DocumentRoot` (`/home/httpd/html`, `/usr/local/apache/htdocs`) nella nuova `DocumentRoot` (`/var/www/html`).

oppure

Modificate il file di configurazione di Apache e riportate ogni riferimento della `DocumentRoot` alla vecchia directory.

La soluzione che avete scelto dipende dalla configurazione del vostro sistema. Generalmente se montate automaticamente la `/home` sul vostro sistema non avete bisogno di avere la `DocumentRoot` in `/home`. D'altro canto non avete spazio a sufficienza in `/var`, quindi non volete la `DocumentRoot` in `/var`. Dovete decidere per la soluzione migliore basandovi sulla configurazione del sistema e sulle necessità del server Web. La configurazione di default del server Web sicuro è stata concepita per ripondere alle necessità della maggior parte dei Webmaster. Sfortunatamente non possiamo configurarlo in funzione di ogni singola situazione.

13.8.2 Cosa succede al vecchio file di configurazione?

Se avete un'altra versione di Apache nel vostro sistema e avete personalizzato i file di configurazione, durante l'installazione di Apache i vecchi file di configurazione verranno salvati nella loro directory con l'estensione `.rpmsave`. Se avete un'altra versione di Apache, ma non avete modificato i file di configurazione, l'installazione li riscriverà.

Dopo aver installato il programma Apache, potete recuperare la vostra precedente configurazione dai vecchi file di configurazione Apache tramite un'operazione di copia e incolla e inserirla nel nuovo file `httpd.conf`. Se state per usare il Tool di configurazione di Apache, non modificate `httpd.conf` manualmente. Per maggiori informazioni sul Tool di configurazione di Apache, consultate la *Official Red Hat Linux Customization Guide*.

13.9 Panoramica sui certificati e la sicurezza

Il server Web sicuro fornisce una certa sicurezza grazie al protocollo Secure Sockets Layer (SSL) e, nella maggior parte dei casi, a un certificato digitale rilasciato da una Certificate Authority (CA). Il protocollo SSL gestisce le comunicazioni criptate e la mutua autenticazione fra i browser e il vostro server Web sicuro (la CA mette la sua reputazione dopo la certificazione della vostra organizzazione). Quando il vostro browser comunica tramite la cifratura SSL, il prefisso https:// compare all'inizio della 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 decodificarsi mutualmente le 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 comunica 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.

Impostate il server sicuro e usate 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 server sicuro.

Un server sicuro usa un certificato per identificarsi davanti ai browser Web. Potete generare da soli il vostro certificato (chiamato certificato "self-signed") oppure potete richiederne uno a una Certificate Authority o CA. Un certificato rilasciato da un CA riconosciuta garantisce che il sito Web venga associato a una particolare società o organizzazione.

Se decidete di creare voi stessi il certificato, sappiate che i certificati "self-signed" non dovrebbero essere usati in molti ambienti di produzione. Questi certificati non vengono automaticamente accettati 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 certificato rilasciati da una CA, consultate la Sezione 13.11, *Tipi di certificati*.

Una volta che avete creato o ottenuto il certificato, installatelo sul vostro server Web sicuro.

13.10 Utilizzo di chiavi e certificati pre-esistenti

Se disponete già di una chiave e di un certificato (per esempio se state installando il server Web sicuro come sostituzione per un altro server sicuro) potete probabilmente usare la vostra chiave e il vostro certificato con il server sicuro. Nelle due situazioni seguenti, non potete usare una chiave e un certificato pre-esistenti:

- *Se cambiate l'indirizzo IP o il nome di dominio* — non potete usare la vostra chiave e il vostro certificato se modificate l'indirizzo IP o il nome di dominio. I certificati sono rilasciati per un particolare indirizzo IP e nome di dominio. 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 lo potete usare per il vostro server Web sicuro. Tuttavia, non potete farlo poiché VeriSign rilascia certificati per un software server e una combinazione di indirizzo IP/nome dominio particolari.

  Se modificate uno di questi parametri (per esempio, se avete usato in precedenza un altro server sicuro e adesso volete usare il server Web sicuro), il certificato VeriSign che avete ottenuto per la precedente configurazione non funzionerà con quella nuova. Dovrete richiederne un altro.

Se avete una chiave e un certificato che potete usare, non dovete generare una nuova chiave né un nuovo certificato. Tuttavia, potreste dovere 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 vostro certificato in:

```
/etc/httpd/conf/ssl.crt/server.crt
```

Dopo averli spostati, andate alla Sezione 13.15, *Verifica del certificato*.

Se state effettuando un aggiornamento del server sicuro Red Hat versione 1.0 o 2.0, la vostra chiave (`httpsd.key`) e il vostro certificato (`httpsd.crt`) verranno posizionati in `/etc/httpd/conf/`. Dovete spostarli e rinominarli affinché il server sicuro possa usarli. 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 server Web sicuro come descritto nella Sezione 14.1, *Avvio e chiusura di* `httpd`. Se state aggiornando un versione precedente del server sicuro non dovete ottenere un nuovo certificato.

13.11 Tipi di certificati

Se avete installato il server Web sicuro usando il programma di installazione di Red Hat Linux, una chiave e un certicicato di test vengono generati e inseriti nelle directory appropriate. Prima di iniziare a usare il server sicuro, dovete tuttavia generare la vostra chiave e ottenere un certificato che identifichi correttamente il vostro server.

Per usare il server sicuro dovete avere una chiave e un certificato — il che significa che potete generare un certificato "self-signed" oppure acquistare un certificato da una CA. Quali sono le differenza fra questi due certificati?

Un certificato rilasciato da una CA fornisce due aspetti importanti per il 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 fornisce le pagine Web al browser.

Se il vostro server sicuro è accessibile al pubblico in generale, 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 ciò 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 server sicuro, ma sappiate che un certificato di questo tipo non fornisce funzionalità diverse rispetto ai certificati rilasciati dalle CA. Infatti, un certificato "self-signed" non viene automaticamente riconosciuto dai browser degli utenti e non fornisce alcuna garanzia sull'identità dell'organizzazione. Se il vostro server sicuro 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.

   Per visualizzare un elenco delle CA, fate clic sul pulsante **Sicurezza** sulla barra degli strumenti di Navigator oppure sul lucchetto posto in basso a sinistra dello schermo, quindi fate clic su **Signers** per visualizzare un elenco dei firmatari di certificati dai quali il vostro browser accetta certificati. Informazioni sulle CA sono presenti anche sul Web. Se avete 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, ed effettivamente siete chi dite di essere, vi spedisce un certificato digitale.
5. Installate il certificato sul vostro server Web. Adesso potete inziare 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 13.12, *Creazione di una chiave*.

13.12 Creazione di una chiave

Innanzitutto, andate alla directory `/etc/httpd/conf` usando il comando `cd`. 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 create la vostra chiave di accesso digitando il comando:

```
make genkey
```

Il sistema visualizza un messaggio simile a:

```
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 riconosce le lettere minuscole da quelle maiuscole.

Nota Bene

La password deve essere inserita ogni volta che avviate il vostro server sicuro, 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 `server.key`.

Se non volete digitare la password ogni volta che avviate il server Web sicuro, non usate `make genkey` per creare la chiave, ma i due comandi seguenti. Entrambi i comandi devono essere digitati in modo da creare un'unica riga.

Digitate:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

per creare la chiave. Quindi usate questo comando:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

perché le autorizzazioni siano impostate correttamente nella chiave.

Se usate questi comandi per creare la chiave, non dovete usare la password per avviare il server Web sicuro.

La disattivazione della password è vivamente SCONSIGLIATA per motivi di sicurezza.

I problemi associati all'assenza di password sono direttamente collegati 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 server Web.

Se le regole di sicurezza UNIX vengono rigorosamente rispettate sul computer host (tutte le patch 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 server

sicuro 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, andate alla Sezione 13.13, *Come richiedere un certificato a una CA*. Se invece volete creare voi stessi il certificato, andate alla Sezione 13.14, *Creazione di un certificato "self-signed"*.

13.13 Come richiedere un certificato a una CA

Una volta creata la chiave dovete formulare una richiesta di certificato da inviare a una CA. 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 alcune 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) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:Durham
Organization Name (eg, company) [Internet Widgits]:Test Company
```

```
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.mydomain.com
Email Address []:admin@mydomain.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) [AU]:
```

La risposta di default, fra parentesi, è **AU**. Per accettarla, premete [Invio], altrimenti digitate le lettere corrispondenti al vostro paese.

Adesso inserite le altre informazioni (`State or Province Name`, `Locality Name`, `Organization Name`, `Organizational Unit Name`, `Common Name`, e `Email address`). Per farlo, seguite le istruzioni riportate qui di seguito:

- 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.
- In `Common Name`, assicuratevi di inserire il *vero* nome del vostro server sicuro (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 niente in questi campi, premete [Invio].

Quando avete finito di fornire le informazioni richieste, viene creato un file `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 corrispondente Web. La CA vi dice come inviare la richiesta, se sono necessari altri documenti e quanto dovete pagare.

Il certificato viene solitamente spedito dalla CA via e-mail. Salvate o copiate e incollate il certificato con il nome `/etc/httpd/conf/ssl.crt/server.crt`.

13.14 Creazione di un certificato "self-signed"

Potete creare voi stessi il certificato. Osservate che un certificato self-signed non fornisce le stesse garanzie di sicurezza di un certificato CA. Per maggiori informazioni, consultate la Sezione 13.11, *Tipi di certificati*.

Per creare un certificato è necessario prima creare una chiave di accesso seguendo le istruzioni fornite nella Sezione 13.12, *Creazione di una chiave*. Una volta creata la chiave, 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, 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) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:Durham
Organization Name (eg, company) [Internet Widgits]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.mydomain.com
Email Address []:myemail@mydomain.com
```

Dopodiché, viene creato un certificato self-signed, il quale verrà posizionato in `/etc/httpd/conf/ssl.crt/server.crt`. A questo punto riavviate il server sicuro. Per maggiori informazioni, consultate la Sezione 14.1, *Avvio e chiusura di* `httpd`.

13.15 Verifica del certificato

Quando il server sicuro viene installato dal programma di installazione di Red Hat Linux, vengono installati, a scopo di verifica, una chiave di accesso e un certificato generico. Non vi potete connettere al server sicuro usando questo certificato. Dovete infatti ottenere un certificato CA o crearne uno. Per maggiori informazioni sui tipi di certiticati disponibili, consultate la Sezione 13.11, *Tipi di certificati*.

Se avete un certificato CA o self-signed, di sicuro avete un file chiamato `/etc/httpd/conf/ssl.key/server.key` contenente la vostra chiave e un file chiamato `/etc/httpd/conf/ssl.crt/server.crt` contenente il vostro certificato. Se la vostra chiave e il vostro certificato si trovano in un altro posto, spostateli in queste directory. Se avete modificato le posizioni di default o i nomi di file del server sicuro nel file di configurazione Apache, spostate questi due file nelle directory appropriate in funzione delle modifiche apportate.

A questo punto, arrestate e riavviate il server come descritto nella Sezione 14.1, *Avvio e chiusura di* `httpd`. Se il file della chiave è cifrato, vi viene chiesto di inserire la password.

Puntate il vostro browser sulla home page del vostro server. La URL per accedere al vostro server sicuro; è:

```
https://your_domain
```

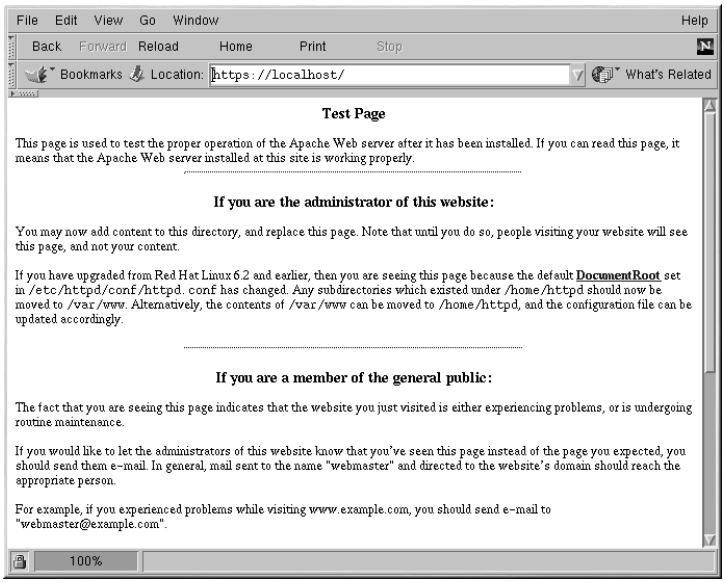
Nota Bene

Osservate la "s" dopo "http." Il prefisso https: è usato per le transazioni HTTP sicure.

Se usate un certificato rilasciato da una CA famosa, il vostro browser accetta automaticamente il certificato e stabilisce la connessione sicura. Il vostro browser non riconosce automaticamente un certificato di prova o self-signed. Se non usate un certificato CA, seguite le istruzioni fornite dal vostro browser per accettare il certificato. Per accettare le impostazioni di default, fate clic su **Avanti** finché non compaiono diverse finestre di dialogo.

Una volta che il browser ha accettato il certificato, il vostro server Web sicuro visualizza una home page come spiegato nella Figura 13–1, *La home page di default*.

Figura 13–1 La home page di default



13.16 Accesso al server sicuro

Per accedere al vostro server sicuro, usate l'URL seguente:

```
https://your_domain
```

Le URL per il collegamento al vostro server sicuro devono iniziare con l'indicatore di protocollo https: anziché con http:.

Le URL per il collegamento al vostro server non sicuro possono iniziare con:

```
http://your_domain
```

La porta standard per le comunicazioni Web sicure è la numero 443. La porta standard per le comunicazioni Web non sicure è la numero 80. La configurazione di default del server Web sicuro si collega a entrambe le porte standard. Per questo motivo non dovete specificare il numero di porta nella URL (il numero di porta è sottointeso).

Tuttavia, se configurate il vostro server perché si colleghi a una porta non standard (un numero vicino a 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 modo 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 server Web non sicuro impostato sulla porta 12331:

```
http://your_domain:12331
```

È possibile che alcune delle URL di esempio usate in questo manuale debbano essere modificate, a seconda che vi stiate collegando al vostro server Web sicuro o a quello non sicuro. Considerate tutte le URL di questo manuale come semplici esempi generali.

13.17 Risorse aggiuntive

Se avete seguito i passi descritti nel Capitolo 13, *Utilizzo di Apache come server Web sicuro*, ma avete riscontrato dei problemi, consultate la sezione "Errata" del sito Web di Red Hat all'indirizzo http://www.redhat.com/support/errata.

Se avete acquistato un prodotto Red Hat ufficiale e la relativa assistenza, registratevi alla pagina Web dedicata al supporto all'indirizzo http://www.redhat.com/support.

Se volete registrarvi alla mailing list dedicata al server sicuro di Red Hat, visitate la pagina Web http://www.redhat.com/mailing-lists.

Potete inoltre iscrivervi alla mailing list dedicata al server sicuro inviando un'e-mail all'indirizzo `redhat-secure-server-request@redhat.com` e indicando la parola "subscribe" (senza le virgolette) nell'oggetto.

13.17.1 Documentazione installata

Se avete installato il pacchetto `apache-manual`, potete accedere alla documentazione Apache in formato HTML disponibile all'indirizzo http://localhost/manual/.

La documentazione relativa a mod_ssl è disponibile all'indirizzo http://localhost/manual/mod/mod_ssl/.

13.17.2 Siti Web utili

Consigli, risposte a domande ricorrenti e documenti HOWTO sono disponibili all'indirizzo http://www.redhat.com/support/docs/howto.

L'Apache Centralized Knowledgebase di Red Hat Linux è disponibile all'indirizzo http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html.

Il sito Web di Apache fornisce una completa documentazione per il server Web Apache. Per accedervi, collegatevi all'indirizzo http://httpd.apache.org/docs.

Il sito di mod_ssl (http://www.modssl.org) è la fonte di informazione più completa su mod_ssl. Il sito comprende una ricca documentazione tra cui uno *User Manual*. Per accedervi, collegatevi all'indirizzo http://www.modssl.org/docs.

13.17.3 Libri correlati

Apache: The Definitive Guide, 2a edizione, di Ben Laurie e Peter Laurie, O'Reilly & Associates, Inc.

14 Direttive e moduli Apache

La configurazione predefinita di Apache è adatta per la maggior parte degli utenti. Si consiglia di non cambiare mai le direttive di configurazione. Se intendete modificare le opzioni della configurazione predefinita, è necessario sapere quali sono le opzioni e dove si trovano. Questo capitolo descrive le opzioni di configurazione disponibili.

AVVERTIMENTO

Se intendete utilizzare il Tool di configurazione di Apache, un'utility grafica fornita con Red Hat Linux, non dovete modificare `httpd.conf`, il file di configurazione del server Web Apache. Viceversa, se desiderate modificare `httpd.conf` manualmente, non utilizzate il Tool di configurazione di Apache.

Per maggiori informazioni sul Tool di configurazione di Apache, consultate la *Official Red Hat Linux Customization Guide*.

Terminata l'installazione del pacchetto `apache`, la documentazione di Apache è disponibile all'indirizzo http://your_domain/manual/ o al sito http://httpd.apache.org/docs/. La documentazione del server Web Apache contiene l'elenco e la descrizione di tutte le direttive di configurazione della versione di Apache fornite con Red Hat Linux.

Nel leggere il file di configurazione del vostro server Web, tenete presente che include sia un server Web "non sicuro" che "sicuro. Il server Web sicuro funziona come host virtuale ed è configurato nel file `httpd.conf`. Per maggiori informazioni relative agli host virtuali, consultate la Sezione 14.4, *L'uso degli host virtuali*.

Nota Bene

L'estensione FrontPage non è inclusa, poiché la licenza Microsoft(TM) proibisce l'inserimento delle estensioni in prodotti di terzi.

14.1 Avvio e chiusura di `httpd`

Durante il processo di installazione è stato salvato in `/etc/rc.d/init.d` uno script della Bourne shell chiamato `httpd`. Per avviare e chiudere manualmente il vostro server, eseguite `httpd` con l'argomento `stop` o `start`.

Per avviare il server, digitate il comando:

```
/etc/rc.d/init.d/httpd start
```

Se state eseguendo Apache come server sicuro, vi viene richiesto l'inserimento di una password, il server si avvierà dopo averla digitata.

Per chiudere il server, digitate il comando:

```
/etc/rc.d/init.d/httpd stop
```

Il comando `restart` offre un modo veloce per chiudere e avviare nuovamente il server. Al riavvio del server vi viene richiesta la password, (se state eseguendo Apache come server sicuro). Il comando `restart` è simile all'esempio seguente:

```
/etc/rc.d/init.d/httpd restart
```

Dopo ogni modifica del file `httpd.conf`, non è necessario chiudere e riavviare il server, potete invece utilizzare il comando `reload`, che non richiede alcuna password, perché rimane memorizzata durante il ricaricamento, ma non tra una chiusura e un riavvio. Il comando `reload` è simile all'esempio seguente:

```
/etc/rc.d/init.d/httpd reload
```

Il processo `httpd` parte automaticamente all'avvio del sistema. Se eseguite Apache come server sicuro, vi viene richiesta una password dopo l'avvio del sistema, a meno che non abbiate creato una chiave per il server senza la protezione di una password.

14.2 Direttive di configurazione in `httpd.conf`

Il file di configurazione del server Web Apache si chiama `/etc/httpd/conf/httpd.conf`. Si tratta di un file abbastanza comune e la sua configurazione di default si adatta a molti, dunque probabilmente non ci sarà bisogno di modificare le direttive in `httpd.conf`. Forse, però, desiderate approfondire le opzioni di configurazione più importanti.

Anche i file vuoti `srm.conf` e `access.conf` sono contenuti nella directory `/etc/httpd/conf`. Questi file erano utilizzati insieme a `httpd.conf` come file di configurazione per Apache.

Se vi occorre configurare Apache, modificate `httpd.conf` e ricaricate o spegnete e riavviate il processo `httpd`. Per saperne di più su come ricaricare, chiudere e avviare Apache, consultate la Sezione 14.1, *Avvio e chiusura di `httpd`*.

Prima di modificare `httpd.conf`, si consiglia di copiare il file originale, chiamandolo, per esempio, `httpd.confold`. In questo modo, se doveste commettere un errore durante la modifica del file, avrete comunque una copia di backup.

Se il vostro server Web non funziona in modo corretto, la prima cosa da fare è verificare le modifiche appena effettuate nel file `httpd.conf`. Assicuratevi che non vi siano errori di battitura. Dopodiché controllate il file di log del vostro server Web (`/var/log/httpd/error_log`). Il file di log degli errori non è facile da interpretare, in genere però gli ultimi inserimenti nel log degli errori dovrebbero aiutarvi a individuare la causa del problema.

I prossimi paragrafi presentano una descrizione delle direttive contenute nel file `httpd.conf`, nella sequenza in cui le trovate nel file. Queste descrizioni sono abbastanza succinte, quindi se vi occorre un approfondimento, consultate la documentazione di Apache in formato HTML disponibile all'indirizzo http://*vostro_dominio*/manual/ o nel sito Apache all'indirizzo http://www.apache.org/docs/. Per maggiori informazioni sulle direttive di mod_ssl, consultate la documentazione disponibile all'indirizzo http://*vostro_dominio*/manual/mod/mod_ssl/ in formato HTML o lo *User's Manual* di mod-ssl all'indirizzo http://www.modssl.org/docs/2.7/.

14.2.1 `ServerType`

`ServerType` può essere impostato come `inetd` o `standalone`. L'impostazione di default del vostro server Web è `ServerType standalone`.

La direttiva `ServerType standalone` attiva il server Web una volta sola, il quale gestisce tutte le connessioni. Invece, la direttiva `ServerType inetd` indica che per ogni connessione HTTP viene avviata una nuova istanza del server. Ogni istanza gestisce un'unica connessione e termina appena viene chiusa. Come probabilmente avrete capito, l'uso di `inetd` non è molto efficace. Inoltre capita che `inetd` non funzioni in modo corretto, a seconda del gruppo di Apache. Infine, considerato che Red Hat Linux 7.1 usa `xinetd`, è necessaria una configurazione aggiuntiva affinché `xinetd` attivi il server. Per queste ragioni, è consigliabile lasciare il `ServerType` del server Web impostato come `standalone`.

14.2.2 `ServerRoot`

`ServerRoot` è la directory di livello superiore che contiene i file del server. Entrambi i server (sicuro e non sicuro) sono impostati per utilizzare una `ServerRoot` di `/etc/httpd`.

14.2.3 `LockFile`

`LockFile` imposta il percorso per il file di blocco utilizzato dal server Apache se è stato compilato con `USE_FCNTL_SERIALIZED_ACCEPT` o `USE_FLOCK_SERIALIZED_ACCEPT`. È consigliabile lasciare `LockFile` al suo valore di default.

14.2.4 `PidFile`

`PidFile` è il file nel quale è memorizzato il pid (ID del processo) del server Web. Di solito è contenuto nella directory `/var/run/httpd.pid`.

14.2.5 ScoreBoardFile

`ScoreBoardFile` immagazzina le informazioni del processo server che sono usate per la comunicazione tra il processo padre e i processi figli. `ScoreBoardFile` è contenuto in `/var/run/httpd.scoreboard`.

14.2.6 ResourceConfig

La direttiva `ResourceConfig` comanda al server di leggere il file specificato. La direttiva `ResourceConfig` è commentata perché il vostro server Web utilizza solo il file `httpd.conf` per le direttive di configurazione.

14.2.7 AccessConfig

La direttiva di configurazione `AccessConfig` indica al server di leggere il file specificato per caricare altre direttive, dopo aver letto il file indicato da `ResourceConfig`. La direttiva `AccessConfig` è commentata poiché la configurazione del server Web usa solamente il file `httpd.conf` per le direttive di configurazione.

14.2.8 Timeout

`Timeout` definisce il tempo espresso in secondi che il server aspetta per la ricezione e la trasmissione durante la comunicazione. In particolare, definisce quanto tempo il server aspetta per ricevere una richiesta GET, per ricevere pacchetti TCP su richiesta POST o PUT e che aspetta la risposta degli ACK ai pacchetti TCP. Il `Timeout` è impostato per attendere 300 secondi, ossia il tempo adeguato per la maggior parte delle situazioni.

14.2.9 KeepAlive

`KeepAlive` definisce se il server gestisce le connessioni persistenti (più di una richiesta per connessione). `KeepAlive` può essere usato per evitare che un client occupi troppe risorse del server. Per default `KeepAlive` è impostato su `on` in modo da autorizzare le connessioni persistenti. Per disabilitare tali connessioni, impostatelo su `off`. Se volete saperne di più su come limitare le richieste per ogni connessione, consultate la Sezione 14.2.10, *`MaxKeepAliveRequests`* .

14.2.10 MaxKeepAliveRequests

Questa direttiva imposta il numero massimo di richieste accettate su ogni connessione persistente. Il team di sviluppo di Apache consiglia di impostarlo su un valore alto per migliorare le prestazioni del server. `MaxKeepAliveRequests` è impostato per default su `100`.

14.2.11 `KeepAliveTimeout`

`KeepAliveTimeout` imposta il tempo (in secondi) durante il quale il server attende un'altra richiesta prima di chiudere la connessione. Una volta ricevuta la richiesta, si applica invece la direttiva `Timeout`.

14.2.12 `MinSpareServers` e `MaxSpareServers`

Il server Web Apache si adatta dinamicamente al carico di lavoro mantenendo un numero variabile di processi che gestiscono il carico di richieste. Il server principale controlla il numero di server in attesa di richiesta e li elimina se superano il valore di `MaxSpareServers` o li avvia se sono inferiori al valore di `MinSpareServers`.

Il valore di default di `MinSpareServers` è `5`, mentre il valore di default di `MaxSpareServers` è `20`. Si consiglia di non aumentare troppo il valore di `MinSpareServers` per evitare di sovraccaricare il server.

14.2.13 `StartServers`

`StartServers` imposta il numero di processi server che devono essere creati all'avvio del servizio. Poiché il server Web elimina o crea dinamicamente i processi server in funzione del traffico, non è necessario aumentare questo parametro. Il valore di default è otto.

14.2.14 `MaxClients`

`MaxClients` imposta un limite per il numero totale di processi server (e quindi anche di client connessi contemporaneamente) in esecuzione. Di solito il valore impostato è abbastanza alto (di default 150). Non è possibile impostare un valore superiore a 256 senza ricompilare Apache. La ragione principale per cui conviene limitare il numero di connessioni simultanee è di evitare di provocare un crash del sistema operativo.

14.2.15 `MaxRequestsPerChild`

`MaxRequestsPerChild` imposta il numero massimo di richieste che ogni figlio può gestire prima che il processo sia eliminato. Lo scopo principale di `MaxRequestsPerChild` è di evitare che un processo rimanga in esecuzione per molto tempo, occupando così troppa memoria. Il valore di default è `100`.

14.2.16 `Listen`

Il comando `Listen` specifica su quale porta il server Web riceve le richieste. Per default il server Web attende le richieste sulla porta 80 per la comunicazione Web non sicura e sulla porta 443 per la comunicazione sicura.

Se impostate Apache perché attenda su una porta inferiore alla 1024, dovete eseguire il processo `httpd` come root. Per le porte superiori alla 1024, potete eseguirlo come un qualsiasi utente.

`Listen` può inoltre essere usato per specificare particolari indirizzi IP dai quali il server accetta le connessioni.

14.2.17 BindAddress

`BindAddress` è un modo per specificare su quale indirizzo IP il server deve rimanere in attesa. Per attivare questa funzionalità usate la direttiva `Listen`. `BindAddress` non viene usata dal server Web, è infatti commentata per default in `httpd.conf`.

14.2.18 LoadModule

`LoadModule` è utilizzato per caricare i moduli Dynamic Shared Object (DSO, oggetti condivisi dinamicamente). Maggiori informazioni sono disponibili nella Sezione 14.3, *Aggiungere moduli al server*. L'ordine dei moduli è estremamente importante e non deve essere cambiato.

14.2.19 IfDefine

I tag `<IfDefine>` e `</IfDefine>` non utilizzano la configurazione specificata al loro interno se nel primo tag la definizione "test" risulta essere vera. Le direttive vengono ignorate se il test è falso.

Il test nei tag `<IfDefine>` è il nome di un parametro (per esempio, `HAVE_PERL`). Se il parametro è definito (ossia viene fornito come argomento dell'avvio del server Web), allora il test è "vero". In questo caso il server Web viene attivato e le direttive contenute nei tag `IfDefine` vengono applicate.

I tag `<IfDefine HAVE_SSL>` contengono per default la configurazione dell'host virtuale per il server Web sicuro. I tag `<IfDefine HAVE_SSL>` contengono le direttive `LoadModule` e `AddModule` per il modulo `ssl_module`.

14.2.20 ClearModuleList

`ClearModuleList` si trova prima della sezione relativa alle direttive `AddModule`. La direttiva `ClearModuleList` inizializza la lista integrata dei moduli attivi. Le direttive `AddModule` ricreano la lista dei moduli che devono essere caricati subito dopo `ClearModuleList`.

14.2.21 AddModule

`AddModule` è la direttiva usata per creare una lista dei moduli disponibili. Usate questa direttiva, se volete aggiungere altri moduli. Per maggiori informazioni sul caricamento dei moduli DSO, consultate la Sezione 14.3, *Aggiungere moduli al server*.

14.2.22 `ExtendedStatus`

La direttiva `ExtendedStatus` controlla se Apache genera le informazioni base (`off`) o dettagliate (`on`), quando viene chiamato il gestore `server-status` mediante il tag `Location`. Per maggiori informazioni consultate la Sezione 14.2.71, *`Location`* .

14.2.23 `Port`

In generale, `Port` definisce la porta sulla quale il server attende. Si tratta normalmente di diverse porte poiché viene usata anche la direttiva `Listen` (e quindi il server attende su tutte le porte). Per maggiori informazioni consultate la descrizione della direttiva `Listen`.

Il comando `Port` specifica inoltre il numero della porta per attribuire un nome canonico al server. Per maggiori informazioni, consultate la Sezione 14.2.39, *`UseCanonicalName`* .

14.2.24 `User`

La direttiva `User` imposta lo userid utilizzato dal server per rispondere alle richieste. Lo `User` impostato determina gli accessi ai file e i privilegi con i quali sono eseguiti i processi figli. Qualunque file non accessibile all'utente specificato non sarà distribuito via Web. L'utente di default è `apache`.

L'utente `User` dovrebbe avere i privilegi per accedere solamente ai file visibili via Web. I processi CGI vengono eseguiti con i diritti di `User`. L'utente `User` non dovrebbe essere autorizzato a eseguire qualunque altro codice che non sia in risposta alle richieste HTTP.

Nota Bene

Non impostate `User` come root. Se lo fate, potreste rendere il vostro server Web poco sicuro.

Il processo padre `httpd` viene eseguito con i diritti di root, ma tutti i processi che rispondono alle richieste HTTP sono eseguiti con i diritti dell'utente `User`. Il server principale deve essere eseguito con i diritti di root, se volete utilizzare le porte inferiori alla 1024 (la comunicazione standard WWW è sulla porta 80 mentre la comunicazione standard WWW sicura è sulla porta 443). Le porte sotto la 1024 sono riservate all'uso del sistema, perciò sono accessibili solo dall'utente root. Quando il server si è collegato alla propria porta, comunque, rinvia il processo a `User` prima di accettare qualsiasi richiesta di connessione.

14.2.25 `Group`

La direttiva `Group` è analoga alla direttiva `User`. `Group` imposta il gruppo per l'esecuzione dei processi figli. Il gruppo di default è `apache`.

14.2.26 ServerAdmin

`ServerAdmin` è l'indirizzo di posta elettronica dell'amministratore del server Web. Questo indirizzo di posta elettronica appare nei messaggi di errore nelle pagine Web generate dal server, in questo modo gli utenti possono riferire eventuali problemi inviando un'e-mail all'amministratore del server. `ServerAdmin` è impostato per default su `root@localhost`.

Normalmente alla direttiva `ServerAdmin` viene attribuito il valore `webmaster@your_domain.com`. Assegnate dunque un alias a `webmaster` per la persona responsabile del server Web nel file `/etc/aliases`. Infine eseguite `/usr/bin/newaliases` per aggiungere il nuovo alias.

14.2.27 ServerName

Potete usare la direttiva `ServerName` per impostare un hostname per il vostro server differente dal nome reale del calcolatore. Per esempio, potete usare www.your_domain.com se il nome del calcolatore è foo.your_domain.com. `ServerName` deve essere un nome valido per il vostro DNS (Domain Name Service) affinché tutto funzioni correttamente.

Se specificate un `ServerName`, accertatevi che nel file `/etc/hosts` esista la corrispondenza tra nome simbolico e indirizzo IP.

14.2.28 DocumentRoot

`DocumentRoot` è la directory che contiene i file HTML in risposta alle richieste. La directory di default per entrambi i server Web sicuro e non sicuro è `/var/www/html`. Per esempio, il server Web può ricevere una richiesta per il seguente documento:

```
http://vostro_dominio/foo.html
```

Il server cercherà il file nella directory di default:

```
/var/www/html/foo.html
```

Se desiderate modificare la direttiva `DocumentRoot` in modo che non sia condivisa dal server Web non sicuro e quello sicuro, consultate la Sezione 14.4, *L'uso degli host virtuali*.

14.2.29 Directory

I tag `<Directory /path/to/directory>` e `</Directory>` sono usati per raggruppare un insieme di direttive di configurazione da applicare solo a una directory e a tutte le sue sottodirectory. Tutte le direttive applicabili a una directory possono essere usate all'interno dei tag `<Directory>`. I tag `<File>` invece possono essere usati allo stesso modo dei file.

Per default, i parametri più restrittivi sono applicati alla directory root, tramite le direttive `Options` (vedere la Sezione 14.2.30, *`Options`*) e `AllowOverride` (vedere la Sezione 14.2.31, *`AllowOverride`*). Con questa configurazione, alle directory sul sistema che necessitano di impostazioni meno restrittive devono essere assegnate in modo esplicito tutte queste impostazioni.

Usando i tag `Directory`, la `DocumentRoot` avrà parametri meno restrittivi, in modo tale da poter effettuare le richieste HTTP.

La directory `cgi-bin` è impostata in modo da permette l'esecuzione dei programmi in essa contenuti, tramite l'opzione `ExecCGI`. Se dovete eseguire degli script CGI presenti in un'altra directory, impostate la direttiva `ExecCGI`. Per esempio, se la vostra directory `cgi-bin` è `/var/www/cgi-bin`, ma volete eseguire anche gli script CGI presenti in `/home/my_cgi_directory`, aggiungete una direttiva `ExecCGI` al file `httpd.conf` come avviene nell'esempio seguente:

```
<Directory /home/my_cgi_directory>
    Options +ExecCGI
</Directory>
```

Per poter eseguire gli script CGI presenti in `/home/my_cgi_directory`, sono necessarie ulteriori modifiche. Innanzitutto eliminate il commento dalla direttiva `AddHandler` per identificare i file con le estensioni `.cgi` come script CGI. Per maggiori informazioni, consultate la Sezione 14.2.65, *`AddHandler`* . I permessi per gli script CGI e l'intero percorso vanno impostati su 0755. Infine il proprietario del file deve essere lo stesso della directory.

14.2.30 `Options`

La direttiva `Options` controlla le caratteristiche del server disponibili in una particolare directory. Per esempio, con i parametri restrittivi specificati per la directory root, la direttiva `Options` è impostata solo per `FollowSymLinks`: quindi non sono autorizzate altre caratteristiche tranne quella che consente al server di seguire i link simbolici nella directory root.

Di default, nella directory `DocumentRoot`, `Options` è configurato per contenere `Indexes`, `Includes` e `FollowSymLinks`. `Indexes` permette al server di generare una lista di directory per una directory, se non è specificata alcuna `DirectoryIndex` (per esempio: `index.html`). `Includes` indica che sono autorizzati gli include del server. `FollowSymLinks` consente al server di seguire i link simbolici in questa directory.

È inoltre necessario inserire la direttiva `Options` per le directory dell'host virtuale, se desiderate che questo riconosca particolari caratteristiche.

Mediante la linea `Options Includes`, contenuta all'interno della sezione di direttive `<Directory "/var/www/html">`, gli include del server sono già abilitati. Tuttavia, se desiderate che un host virtuale riconosca che gli include del server siano autorizzati all'interno di `/var/www/html`, dovrete inserire una sezione nei tag del vostro host virtuale che sia simile alla seguente:

```
<Directory /var/www/html>
```

```
Options Includes
</Directory>
```

14.2.31 AllowOverride

La direttiva `AllowOverride` consente di stabilire se le `Options` possono essere ridefinite dalle dichiarazioni presenti nel file `.htaccess`. Per default, sia nella directory root che nella directory `DocumentRoot` non è permesso sovrascrivere il file `.htaccess`.

14.2.32 Order

La direttiva `Order` controlla l'ordine di valutazione delle direttive `allow` e `deny`. Il server è configurato per valutare prima la direttiva `deny` per la directory `DocumentRoot`.

14.2.33 Allow

`Allow` specifica quali richieste possono accedere a una directory. Il campo richiedente può essere `all`, un dominio, un indirizzo IP, una parte dell'indirizzo IP, la coppia rete/netmask, ecc. La directory `DocumentRoot` è configurata per permettere l'accesso da `all` (ossia da tutti i client).

14.2.34 Deny

`Deny` funziona in modo simile ad `allow`, ma specifica quali accessi negare. La vostra `DocumentRoot` non è configurata per negare alcuna richiesta.

14.2.35 UserDir

`UserDir` è il nome della sottodirectory contenente i file HTML personali dell'utente. Per default la sottodirectory si chiama `public_html` e deve essere presente nella directory home dell'utente. Per esempio, il server può ricevere la seguente richiesta:

```
http://vostro_dominio/~nome utente/foo.html
```

Il server cercherà il file:

```
/home/username/public_html/foo.html
```

Nell'esempio precedente, `/home/username` è la directory home dell'utente (ovviamente il percorso di default della directory home può essere differente sul vostro sistema).

Assicuratevi che i permessi della directory home dell'utente siano corretti, l'impostazione esatta è 0755. È necessario attivare i bit di lettura (r) e di esecuzione (x) nella directory `public_html` (0755 funziona correttamente). I file presenti in questa directory devono essere impostati almeno su 0644.

14.2.36 `DirectoryIndex`

La direttiva `DirectoryIndex` indica il nome della pagina di default che viene restituita al client quando un utente richiede un indice di una directory, specificando uno slash (/) dopo il nome della directory.

Quando un utente richiede la pagina http://*vostro_dominio*/*questa_directory*/, riceve o la pagina `DirectoryIndex`, se esistente o un elenco di directory generato dal server. La configurazione di default di `DirectoryIndex` è `index.html index.htm index.shtml index.php index.php4 index.php3 index.cgi`. Il server cerca di individuare uno di questi file e restituisce il primo file che trova. Se non trova nessun file e per questa directory è impostata la direttiva `Options Indexes`, il server genera e restituisce un elenco, in formato HTML, delle sottodirectory e dei file contenuti nella directory.

14.2.37 `AccessFileName`

`AccessFileName` attribuisce il nome al file che il server utilizza per accedere alle informazioni di controllo in ogni directory. In genere il server Web è impostato di default per utilizzare `.htaccess`, se esistente.

Immediatamente dopo la direttiva `AccessFileName`, un tag `Files` controlla l'accesso ai file che iniziano con `.ht`. Per ragioni di sicurezza questa direttiva nega l'accesso Web a qualunque file `.htaccess` (o a qualunque file che inizi con `.ht`).

14.2.38 `CacheNegotiatedDocs`

Per default, il server Web chiede ai server proxy di non conservare nella cache alcun documento trasmesso sulla base del contenuto (ciò significa che tali documenti potrebbero essere modificati dall'inserimento del richiedente). Eliminando il commento dalla direttiva `CacheNegotiatedDocs`, il server proxy è autorizzato a conservare i documenti nella cache.

14.2.39 `UseCanonicalName`

Per default `UseCanonicalName` è impostato su `on`. `UseCanonicalName` permette a un server di costruire un URL che faccia riferimento a sè stesso utilizzando `ServerName` e `Port`. Quando il server si riferisce a se stesso per rispondere a una richiesta di un client, utilizza questo URL. Se invece impostate `UseCanonicalName` su `off`, il server usa il valore inviato dal client per fare riferimento a sè stesso.

14.2.40 `TypesConfig`

`TypesConfig` definisce il nome del file che contiene i tipi MIME di default (le estensioni dei file per i tipi di contenuto). Il file `TypesConfig` di default è `/etc/mime.types`. Invece di modificare questo file, si consiglia di aggiungere i tipi MIME tramite la direttiva `AddType`.

14.2.41 DefaultType

`DefaultType` definisce il tipo MIME di default per i documenti che non sono riconosciuti. Secondo la configurazione di default, se il server Web non riconosce un tipo di file, lo considera come un file in formato testo.

14.2.42 IfModule

I tag `<IfModule>` e `</IfModule>` raggruppano le direttive condizionali. Le direttive presenti all'interno di `IfModule` sono elaborate solo se la condizione specificata è vera. Le direttive sono elaborate se il modulo specificato all'interno del tag `<IfModule>` è compilato nel server Apache. Se il simbolo "!" (punto esclamativo) è inserito prima del nome del modulo, le direttive vengono elaborate solo se il modulo non è compilato nel primo tag `<IfModule>`.

Il file `mod_mime_magic.c` è incluso nei tag `IfModule`. Questo file è simile al comando `file` di UNIX che legge i primi byte del file per determinarne il tipo e poi utilizza "numeri magici" e altre istruzioni per stabilire il tipo MIME del file.

Se il modulo mod_mime_magic viene compilato per Apache, i tag `IfModule` indicano al modulo dove si trova in questo caso il file con le istruzioni `/usr/share/magic`.

Il modulo mod_mime_magic non è compilato per default. Se desiderate utilizzarlo, consultate le informazioni su come aggiungere i moduli al vostro server contenute nella Sezione 14.3, *Aggiungere moduli al server*.

14.2.43 HostnameLookups

`HostnameLookups` può essere impostato su `on`, `off` oppure `double`. Autorizzando la direttiva `HostnameLookups` (impostandola su `on`), il vostro server risolve in modo automatico l'indirizzo IP per ogni connessione che richiede un documento dal server Web. Risolvere l'indirizzo IP significa che il vostro server si connette una o più volte al DNS per individuare il nome dell'host che corrisponde a un particolare indirizzo IP. Se impostate `HostnameLookups` su `double`, il server esegue un DNS inverso doppio. In altre parole, dopo un lookup inverso viene eseguito un lookup diritto. Almeno uno degli indirizzi IP nel lookup diritto deve coincidere con l'indirizzo derivante dal primo lookup inverso.

Normalmente dovreste lasciare `HostnameLookups` impostato su `off`, perché le richieste del DNS aggiungono un carico eccessivo che può causare un rallentamento del server. Se il server è occupato, gli effetti di `HostnameLookups` sono molto evidenti.

`HostnameLookups` coinvolge Internet in generale. Si sommano tutte le connessioni individuali create per cercare ogni hostname. Dunque per evitare problemi con il server Web e per il bene di Internet in generale, è consigliabile lasciare la direttiva `HostnameLookups` impostata su `off`.

14.2.44 `ErrorLog`

`ErrorLog` specifica il nome del file dove vengono registrati tutti gli errori del server. Per default il file di log errori è `/var/log/httpd/error_log`.

Il file di log degli errori è il miglior posto dove cercare se il server Web genera degli errori o per capire la causa dei malfunzionamenti.

14.2.45 `LogLevel`

`LogLevel` definisce il livello di "verbosità" dei messaggi d'errore registrati nel file di log. `LogLevel` può essere impostato su `emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` o `debug`. Per default è impostato su `warn` (valore medio di verbosità).

14.2.46 `LogFormat`

La direttiva `LogFormat` definisce il formato dei messaggi di accesso registrati nel file di log. Questo formato rende facilmente leggibile il file di log degli accessi.

14.2.47 `CustomLog`

`CustomLog` indica il file di log e il suo formato. Nella configurazione di default del vostro server Web, `CustomLog` definisce il file di log in cui sono registrati gli accessi al server Web: `/var/log/httpd/access_log`. Se desiderate generare delle statistiche di accesso al sito Web, dovete sapere dove è memorizzato questo file.

`CustomLog` definisce il formato dei file di log. Il formato standard è:

```
remotehost rfc931 authuser [date] "request" status bytes
```

`remotehost`

Contiene il nome dell'host remoto. Se il nome non è disponibile tramite il DNS oppure se `HostnameLookups` è impostato su `Off`, il campo *`remotehost`* contiene l'indirizzo IP dell'host remoto.

`rfc931`

Non è usato. In questo punto del file di log viene inserito il carattere `-`.

`authuser`

Se viene richiesta l'autenticazione, allora indica lo username che identifica l'utente. Di solito non viene usato ed è inserito il carattere `-`.

`[data]`

Data e ora della richiesta.

"richiesta"

Stringa contenente la stessa richiesta inviata dal browser o dal client.

stato

Codice dello stato HTTP restituito al browser o al client.

byte

Dimensione del documento.

Il comando `CustomLog` può essere utilizzato per configurare i file di log specifici per registrare i "referer" (l'URL per la pagina Web collegata a una pagina sul vostro server) e/o gli "agent" (i browser utilizzati per ricevere le pagine Web dal vostro server Web). Le linee rilevanti di `CustomLog` sono commentate come illustrato nell'esempio. Se desiderate i due file di log, eliminate i commenti:

```
#CustomLog /var/log/httpd/referer_log referer
#CustomLog /var/log/httpd/agent_log agent
```

In alternativa potete impostare la direttiva `CommonLog` in modo che utilizzi un log `combinato`:

```
#CustomLog /var/log/httpd/access_log combined
```

Un file di log `combinato` aggiunge i campi referer e agent al termine di ogni riga. Se desiderate usare un file di log `combinato`, eliminate il commento dalla direttiva `CustomLog` per impostare il log di accesso sul formato del file di log comune.

14.2.48 ServerSignature

La direttiva `ServerSignature` aggiunge una linea contenente la versione del server Apache e il `ServerName` alle pagine Web generate dal server (per esempio nelle pagine contenenti i messaggi di errore). Per default `ServerSignature` è impostato su `on`. Se non volete aggiungere queste informazioni impostatelo su `off`. Potete anche inserire il tag `EMail`. In tal caso nelle pagine Web generate dal server viene aggiunta la stringa `mailto:ServerAdmin`.

14.2.49 Alias

L'impostazione `Alias` consente alle directory di trovarsi fuori da `DocumentRoot`. Qualunque URL che termina con l'alias, viene automaticamente risolto nel percorso dell'alias. Nella configurazione di default è già presente un alias. Il server Web può accedere alla directory `icons` anche se si trova fuori della directory `DocumentRoot`. La directory `icons`, un alias, è in realtà `/var/www/icons/` e non `/var/www/html/icons/`.

14.2.50 `ScriptAlias`

La direttiva `ScriptAlias` definisce dove sono localizzati gli script CGI (o gli altri tipi di script). Normalmente non dovete lasciare gli script CGI all'interno di `DocumentRoot`, poiché potrebbero essere visualizzati come documenti di testo. Sebbene possa non interessarvi se qualcuno vede (e usa) i vostri script CGI, qualche malintenzionato potrebbe scoprire come funzionano e sfruttare eventuali "falle" negli script. La directory `cgi-bin` è di default uno `ScriptAlias` della directory `/cgi-bin/` e si trova in `/var/www/cgi-bin/`.

Per la directory `/var/www/cgi-bin` è stata impostata la direttiva `Options ExecCGI`, che abilita l'esecuzione degli script presenti nella directory.

Per maggiori informazioni sull'esecuzione di script CGI in directory diverse da `cgi-bin`, consultate la Sezione 14.2.65, *`AddHandler`* e la Sezione 14.2.29, *`Directory`* .

14.2.51 `Redirect`

Quando una pagina Web viene rimossa, la direttiva `Redirect` può essere utilizzata per rimappare il vecchio URL con quello nuovo. Il formato è il seguente:

```
Redirect /percorso/foo.html http://nuovo_dominio/percorso/foo.html
```

Se si riceve una richiesta HTTP per la pagina http://*vostro_domino*/*percorso*/foo.html, il server restituisce la pagina http://*nuovo_dominio*/*percorso*/foo.html. al client, che di solito cerca di richiamare il documento dal nuovo URL.

14.2.52 `IndexOptions`

`IndexOptions` controlla l'aspetto degli elenchi delle directory generati del server. Se è impostata la direttiva `Options Indexes` (vedere la Sezione 14.2.30, *`Options`*), il server Web genera l'elenco delle directory quando riceve una richiesta HTTP:

http://*vostro_dominio*/*questa_directory*/

Innanzitutto, il server Web cerca nella directory uno dei file specificati con la direttiva `DirectoryIndex` (per esempio `index.html`). Se i file non sono presenti, crea un file HTML contenente l'elenco dei file e delle directory. Potete modificare l'aspetto di queste pagine usando la direttiva `IndexOptions` (contenuta in `httpd.conf`).

La configurazione di default imposta `FancyIndexing` su on. Se `FancyIndexing` è attivato, facendo clic sull'intestazione della colonna potrete cambiare l'ordinamento dei file e delle directory. Con un altro clic sulla stessa intestazione, si inverte per esempio la sequenza da ordinamento ascendente a discendente. `FancyIndexing` visualizza un'icona per ogni tipo di file, in funzione dell'estensione. Se usate la direttiva `AddDescription` e attivate `FancyIndexing`, viene visualizzata una breve descrizione dei file nell'elenco delle directory generato dal server.

`IndexOptions` ha vari parametri per selezionare l'aspetto degli elenchi delle directory. I parametri possibili sono `IconHeight` e `IconWidth`, affinché il server includa i tag `HEIGHT` e `WIDTH` per le icone delle pagine Web generate dal server; `IconsAreLinks` per poter utilizzare le icone come link, insieme al nome del file.

14.2.53 AddIconByEncoding

Questa direttiva associa un'icona a un particolare tipo di file secondo la codifica MIME. Per esempio il server Web visualizza l'icona `compressed.gif` per i file di tipo x-compress e x-gzip.

14.2.54 AddIconByType

Questa direttiva specifica il nome dell'icona da visualizzare accanto al file con il tipo MIME negli elenchi delle directory generati dal server. Per esempio, il vostro server è impostato per visualizzare l'icona `text.gif` accanto al file con il tipo MIME "text".

14.2.55 AddIcon

`AddIcon` indica al server che icona visualizzare in funzione dell'estensione del file. Per esempio il server Web visualizza l'icona `binary.gif` per i file che hanno l'estensione `.bin` o `.exe`.

14.2.56 DefaultIcon

`DefaultIcon` specifica l'icona da visualizzare negli elenchi delle directory generati dal server per i file che non hanno altre icone specificate. La `DefaultIcon` per quei file è di default `unknown.gif`.

14.2.57 AddDescription

Potete utilizzare la direttiva `AddDescription` per visualizzare il testo che specifica certi file negli elenchi delle directory, generati dal server (inoltre dovrete abilitare `FancyIndexing` come una direttiva `IndexOptions`). Per specificare i file a cui questa direttiva deve essere applicata, potete nominare file specifici, espressioni con asterisco o estensioni di file. Per esempio potete utilizzare la seguente linea:

```
AddDescription "Un file che termina in .ni" .ni
```

In ogni elenco generato dal server Web, tutti i file con l'estensione `.ni` hanno la descrizione `Un file che termina in .ni` dopo il nome del file. È inoltre necessario attivare la direttiva `FancyIndexing`.

14.2.58 `ReadmeName`

`ReadmeName` definisce il nome del file (se esiste nella directory) che viene aggiunto alla fine dell'elenco. Nella configurazione di default, `ReadmeName` è impostato sul valore `README`.

14.2.59 `HeaderName`

`HeaderName` specifica il nome del file (se esiste nella directory) che viene inserito all'inizio degli elenchi delle directory generati dal server. Comer per `ReadmeName`, il server cerca di includere il file in formato HTML, se possibile, altrimenti in formato testo.

14.2.60 `IndexIgnore`

`IndexIgnore` può contenere estensioni di file, nomi di file parziali, espressioni con asterisco o nomi di file completi. Il server Web non individua i file che non corrispondono a nessuno dei parametri contenuti nell'elenco delle directory generato dal server.

14.2.61 `AddEncoding`

`AddEncoding` definisce le estensioni dei file che hanno una particolare codifica. `AddEncoding` può essere utilizzato per indicare al browser (non tutti) di decomprimere certi file mentre vengono scaricati.

14.2.62 `AddLanguage`

`AddLanguage` associa l'estensione di un file a una particolare lingua. Questa direttiva è utile se il server deve restituire i documenti HTML in base alla lingua del client specificata nel browser.

14.2.63 `LanguagePriority`

`LanguagePriority` vi permette di definire in che lingua trasmettere i file se nel browser non è stata specificata la lingua del client.

14.2.64 `AddType`

Usate la direttiva `AddType` per associare un tipo MIME a una estensione di file. Per esempio, se state utilizzando il linguaggio PHP4, dovete aggiungere la direttiva `AddType` affinché il server Web riconosca i file PHP come tipo MIME (di solito hanno l'estensione `.php4`, `.php3`, `.phtml` o `.php`).

La seguente linea indica al vostro server di riconoscere l'estensione `.shtml` (per gli include del server):

```
AddType text/html .shtml
```

Dovete includere la linea precedente all'interno dei tag dell'host virtuale, per ogni host virtuale che deve autorizzare gli include del server.

14.2.65 AddHandler

`AddHandler` mappa l'estensione di un file a gestori specifici. Per esempio, il gestore `cgi-script` può essere utilizzato per associare l'estensione `.cgi` a un file script CGI. Questo metodo funziona anche al di fuori della directory `ScriptAlias`, se seguite attentamente le istruzioni qui fornite.

Nel file `httpd.conf` è contenuta una riga `AddHandler` CGI:

```
AddHandler cgi-script .cgi
```

È necessario innanzitutto eliminare il commento dalla linea, dopodiché Apache eseguirà gli script CGI per i file che terminano in `.cgi`, anche se sono al di fuori di `ScriptAlias`, configurato per default per localizzare la vostra directory `/cgi-bin/` in `/var/www/cgi-bin/`.

Dovete inoltre configurare `ExecCGI` come `Options` per ogni directory che contiene uno script CGI. Consultate la Sezione 14.2.29, *`Directory`* per maggiori informazioni sulla configurazione della directory `ExecCGI`. Accertatevi che i permessi siano impostati correttamente per gli script CGI e per le directory che li contengono, normalmente su 0755. Infine il proprietario della directory e quello dei file devono coincidere.

`AddHandler` deve essere inserito nella configurazione del vostro `VirtualHost`, anche se gli script CGI sono al di fuori di `ScriptAlias`.

Oltre agli script CGI, il vostro server Web utilizza anche `AddHandler` per elaborare gli HTML e i file imagemap analizzati dal server.

14.2.66 Action

`Action` vi permette di specificare un contenuto MIME e uno script CGI. In questo modo, quando viene richiesto un file di un determinato tipo viene eseguito uno script CGI.

14.2.67 MetaDir

`MetaDir` specifica il nome della directory in cui il vostro server Web deve cercare i file che contengono meta informazioni (header HTTP extra) per includerle nella preparazione di documenti.

14.2.68 MetaSuffix

`MetaSuffix` specifica il suffisso del file che contiene meta informazioni (header HTTP extra), che dovrebbe trovarsi nella directory `MetaDir`.

14.2.69 `ErrorDocument`

Per default, in caso di problemi o errori, il vostro server Web mostra un messaggio di errore semplice (e di solito cifrato) al client richiedente. Invece di usare l'impostazione di default, potete utilizzare la direttiva `ErrorDocument` per personalizzare il messaggio da visualizzare in caso di errore o reindirizzare il client verso una URL locale o esterna. `ErrorDocument` associa il codice HTTP a una URL o a un messaggio che verrà restituito al client.

14.2.70 `BrowserMatch`

La direttiva `BrowserMatch` consente al server di definire le variabili d'ambiente e/o le azioni basate sul campo header HTTP User-Agent, che identifica il browser del client. Per default il vostro server Web utilizza `BrowserMatch` per negare le connessioni a determinati browser con problemi noti e anche per disabilitare i keepalive e i comandi di annullamento degli header HTTP per i browser che hanno problemi con queste azioni.

14.2.71 `Location`

I tag `<Location>` e `</Location>` vi permettono di specificare il controllo dell'accesso basato sull'URL.

`Location` può essere presente anche all'interno dei tag `IfModule mod_perl.c`. Questa configurazione è attivata solamente se il modulo DSO `mod_perl.so` viene caricato. Per maggiori informazioni relative all'aggiunta di moduli per Apache, consultate la Sezione 14.3, *Aggiungere moduli al server*.

I tag `Location` assegnano il nome alla directory `/var/www/perl` (un `Alias /perl`), ossia la directory dalla quale gli script perl vengono eseguiti. Se viene richiesto un documento con una URL contenente `/perl` nel suo percorso file, il vostro server Web controlla nella directory `/var/www/perl/` per eseguire lo script corretto.

Nel file `httpd.conf` sono commentati altri esempi delle opzioni `<Location>`. Se volete attivare queste opzioni eliminate il commento nella sezione corretta dalle direttive.

Subito dopo le direttive Perl discusse sopra, il vostro file `httpd.conf` comprende una sezione di direttive per abilitare HTTP PUT (usato da Netscape Gold per inviare pagine Web al server Web). Se desiderate abilitare HTTP PUT, eliminate il commento all'intera sezione:

```
#Alias /upload /tmp
#<Location /upload>
#    EnablePut On
#    AuthType Basic
#    AuthName Temporary
#    AuthUserFile /etc/httpd/conf/passwd
#    EnableDelete Off
```

```
#    umask 007
#    <Limit PUT>
#       require valid-user
#    </Limit>
#</Location>
```

Dovrete inoltre eliminare il commento dalle linee seguenti situate all'inizio del file `httpd.conf` in modo che il modulo mod_put venga caricato per Apache:

```
#LoadModule put_module          modules/mod_put.so
#AddModule mod_put.c
```

Se desiderate autorizzare delle persone a connettersi dal vostro dominio per vedere i report sullo stato del server, dovreste eliminare il commento dalla sezione di direttive elencata qui sotto:

```
#<Location /server-status>
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>
```

Dovete sostituire `.vostro_dominio.com` con il vostro nome di dominio di secondo livello.

Se volete fornire diverse configurazioni di report (tra cui i moduli installati e le direttive di configurazione) alle richieste dal vostro dominio, eliminate il commento dalle linee seguenti:

```
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>
```

Anche in questa sezione inserite il `.vostro_dominio.com`.

La prossima sezione utilizza i tag `Location` per permettere l'accesso alla documentazione presente nella directory `/usr/share/doc` selezionando l'indirizzo URL http://*vostro_dominio*/doc/qualsiasi.html. La direttiva permette l'accesso delle richieste provenienti dall'host locale.

`Location` può essere utilizzato per attivare una sezione che controlla gli attacchi al sito Web. Questi attacchi si servono di un vecchio bug precedente ad Apache 1.1. Se volete registrare queste richieste, eliminate il commento alle righe seguenti:

```
#<Location /cgi-bin/phf*>
#    Deny from all
#    ErrorDocument 403 http://phf.apache.org/phf_abuse_log.cgi
#</Location>
```

Se queste linee non sono commentate, il vostro server Web ridireziona le richieste che terminano in `/cgi-bin/phf*` allo script CGI di log eseguito dal team di sviluppo di Apache.

14.2.72 `ProxyRequests`

Se eliminate il commento dalla entry `IfModule` inserendo invece la `ProxyRequests`, il vostro server Apache si comporterà anche da server proxy. È inoltre necessario caricare il modulo `mod_proxy`. Per informazioni su come caricare i moduli, consultate la Sezione 14.3, *Aggiungere moduli al server*.

14.2.73 `ProxyVia`

Il comando `ProxyVia` controlla l'HTTP Via: la linea relativa all'header viene inviata con le richieste o le risposte attraverso il server proxy Apache. L'header Via: mostra il nome dell'host se `ProxyVia` è impostato su `On`, il nome dell'host e la versione di Apache, se è impostato il comando `Full`. Qualsiasi linea Via: viene trasmessa senza essere modificata se è impostato `Off` e viene rimossa se è impostato `Block`.

14.2.74 Direttive della cache

Una serie di direttive relative alla cache sono commentate nel proxy `IfModule` menzionato sopra. Se state utilizzando la funzionalità server proxy e desiderate inoltre abilitare la cache proxy, è necessario eliminare il commento dalla direttiva cache come descritto. La configurazione di default per le vostre direttive cache dovrebbe essere idonea per molte configurazioni.

La `CacheRoot` configura il nome della directory che contiene i file memorizzati nella cache. La `CacheRoot` di default è `/var/cache/httpd`.

La direttiva `CacheSize` specifica quanto spazio potete usare in KB. La dimensione predefinita è di `5` KB.

La `CacheGcInterval` indica un numero di ore, dopo le quali i file nella cache vengono cancellati se la cache utilizza più spazio di quanto configurato in `CacheSize`. Il valore di default è 4 ore.

I documenti in HTML rimangono nella cache (senza che venga effettuata una nuova richiesta) per un numero massimo di ore configurato in `CacheMaxExpire`. Il valore di default è `24` ore.

La entry `CacheLastModifiedFactor` impedisce che venga stabilita una data di scadenza per un documento privo di tale data. Il valore di default per `CacheLastModifiedFactor` è di `0.1`, questo significa che la data di scadenza per questi documenti è pari a 1/10 della quantità di tempo trascorso dall'ultima modifica.

La entry `CacheDefaultExpire` specifica la scadenza in ore per un documento ricevuto che utilizza un protocollo che non supporta la data di scadenza. La configurazione di default è 1 ora.

Ogni documento ricevuto da un host e/o un dominio conforme alla configurazione in `NoCache` non viene memorizzato nella cache. Se conoscete host o domini dai quali non volete memorizzare documenti, eliminate il commento dalla direttiva `NoCache` e inserite il nome degli host e dei domini.

14.2.75 `NameVirtualHost`

È necessario utilizzare la direttiva `NameVirtualHost` per un indirizzo IP (e un numero di porta se necessario) di ogni host virtuale che state configurando. La configurazione degli host virtuali basati sul nome viene utilizzata quando dovete configurare diversi virtual host per altrettanti domini, ma non potete (o non volete) usare indirizzi IP diversi per ogni host.

Nota Bene

Non potete usare un host virtuale basato sul nome con il vostro server "sicuro". Ogni host virtuale configurato avrà solo connessioni HTTP "non sicure".

Non potete usare gli host virtuali con il vostro server sicuro perché la handshake SSL (il momento in cui il browser accetta il certificato di autenticazione del server Web) si attiva prima della richiesta HTTP che identifica l'host virtuale corretto. In altre parole, l'autenticazione viene effettuata prima che ci sia qualunque identificazione di host virtuale basata sul nome. Se volete usare l'host virtuale con il server sicuro, è necessario usare l'host virtuale basato sull'indirizzo IP.

Se usate un host virtuale basato sul nome eliminate il commento dalla direttiva `NameVirtualHost` e aggiungete l'indirizzo IP corretto. Poi inserite le informazioni relative ai differenti domini utilizzando i tag `Virtual Host` vicino al `ServerName` per ogni host virtuale e per qualsiasi altra direttiva di configurazione applicabile solo a quell'host virtuale.

14.2.76 `VirtualHost`

I tag `<VirtualHost>` e `</VirtualHost>` si trovano accanto alle direttive di configurazione da applicare a un host virtuale. La maggior parte delle direttive di configurazione possono essere utilizzate all'interno dei tag degli host virtuali e poi vanno applicate solo a quel particolare host virtuale.

In alcune direttive di configurazione si trovano una serie di tag `VirtualHost`. Per maggiori informazioni sui virtual host, consultate la Sezione 14.4, *L'uso degli host virtuali*.

14.2.77 SetEnvIf

La direttiva di configurazione `SetEnvIf` è utilizzata per disabilitare i keepalive HTTP e per consentire al protocollo SSL di chiudere la connessione senza un messaggio di avvertimento da parte del browser client. Questa impostazione è necessaria per alcuni browser che non chiudono in modo affidabile la connessione SSL.

14.2.78 Direttive di configurazione per l'SSL

Le direttive SSL vengono incluse nel file `httpd.conf` del server per abilitare comunicazioni Web sicure utilizzando SSL e TLS.

Per maggiori informazioni sulle direttive SSL visitate il sito http://*vostro_dominio*/manual/mod/mod_ssl/. Alcune informazioni aggiuntive sulle direttive SSL sono disponibili all'indirizzo http://www.modssl.org/docs/2.7/ssl_reference.html/. Si tratta di un capitolo incluso nel documento Web sul modulo mod_ssl scritto da Ralf Engelschall. Lo stesso documento, lo *User's Manual* di mod_ssl, è disponibile all'indirizzo Web: http://www.modssl.org/docs/2.7/ ed è un ottimo riferimento per mod_ssl e per la cifratura in generale. Questo manuale fornisce informazioni generali sulla sicurezza del server Web al Capitolo 13, *Utilizzo di Apache come server Web sicuro*.

Nota Bene

Non modificate le vostre direttive SSL se non siete certi di quello che state facendo. Nella maggior parte dei casi è sufficiente utilizzare la configurazione di default.

14.3 Aggiungere moduli al server

Il supporto per i DSO è disponibile dalla versione 1.3 di Apache, quindi potete caricare o compilare i moduli di Apache per il vostro server Web. Il supporto DSO permette di caricare i moduli in modo dinamico durante l'esecuzione del programma. Dal momento che i moduli vengono caricati solo se necessario, non usano risorse di memoria.

Il team di sviluppo di Apache fornisce una documentazione completa all'indirizzo http://www.apache.org/docs/dso.html. Dopo aver installato il vostro server potete anche controllare http://*vostro_dominio*/manual/mod/ per la documentazione sui moduli di Apache in formato HTML. Una descrizione su come caricare i moduli viene fornita di seguito, ma se avete bisogno di un approfondimento, consultate le pagine Web agli indirizzi sopracitati.

Affinché Apache utilizzi dinamicamente il modulo condiviso, tale modulo deve comparire nelle direttive `LoadModule` e `AddModule` all'interno del file `httpd.conf`. Per default le due entry indicate

sopra sono già incluse in `httpd.conf`, ma alcuni dei moduli meno usati sono commentati e quindi non vengono caricati di default.

Se avete la necessità di utilizzare questi moduli non caricati, verificate nel file `httpd.conf` i moduli disponibili. Ogni modulo disponibile ha un riferimento `LoadModule`. Per mostrarvi un esempio ecco alcune entry della sezione `LoadModule`:

```
#LoadModule mmap_static_module modules/mod_mmap_static.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule env_module         modules/mod_env.so
LoadModule config_log_module  modules/mod_log_config.so
LoadModule agent_log_module   modules/mod_log_agent.so
LoadModule referer_log_module modules/mod_log_referer.so
#LoadModule mime_magic_module  modules/mod_mime_magic.so
```

Molte delle linee non sono commentate, il che significa che ogni modulo associato viene compilato e caricato per default. La prima linea è commentata, perciò il modulo corrispondente (`mmap_static_module`) viene compilato ma non caricato.

Per essere sicuri che Apache carichi un modulo, per prima cosa eliminate il commento alla linea corrispondente. Per esempio se volete che Apache attivi il modulo `mime_magic_module`, modificate la linea `LoadModule` in questo modo:

```
#LoadModule mime_magic_module modules/mod_mime_magic.so
```

È poi necessario eliminare il commento situato davanti alla direttiva `AddModule` in `httpd.conf`:

```
#AddModule mod_mime_magic.c
```

Dopo aver eliminato il commento dalle linee `LoadModule` e `AddModule` per il modulo che desiderate caricare, chiudete e riavviate Apache, come illustrato nella Sezione 14.1, *Avvio e chiusura di `httpd`*. Dopo l'avvio il modulo dovrebbe essere caricato in Apache.

Se avete un modulo personale, potete aggiungerlo al vostro file `httpd.conf` in modo che venga compilato e caricato come un DSO. Per farlo è necessario installare il pacchetto `apache-devel`, come illustrato nel Capitolo 13, *Utilizzo di Apache come server Web sicuro*, perché comprende i file include, i file header e il supporto per ampliare Apache (APXS). APXS utilizza i file include e i file header per compilare il vostro modulo in modo che funzioni con Apache.

AVVERTIMENTO

Se intendete utilizzare il Tool di configurazione di Apache, un'utility grafica fornita con Red Hat Linux, non è necessario compilare i propri moduli o modificare il file di configurazione di Apache `httpd.conf`. Viceversa, se desiderate aggiungere moduli ad Apache o modificare il file `httpd.conf` manualmente, non utilizzate il Tool di configurazione di Apache.

Per maggiori informazioni sul Tool di configurazione di Apache, consultate la *Official Red Hat Linux Customization Guide*.

Se avete scritto il modulo dovete usare APXS per compilare i file sorgenti esterni all'albero delle directory di Apache. Se avete bisogno di maggiori informazioni su APXS, consultate la documentazione di Apache all'indirizzo http://www.apache.org/docs/dso.html.

Dopo aver compilato il vostro modulo utilizzando APXS, inseritelo in `/usr/lib/apache`. Inserite ora sia una linea `LoadModule` che una linea `AddModule` nel file `httpd.conf`. Dopo `LoadModule` in `httpd.conf`, aggiungete una linea per l'oggetto condiviso simile alla seguente:

```
LoadModule foo_module  modules/mod_foo.so
```

È necessario cambiare il nome del modulo e il nome dell'oggetto condiviso.

Alla fine dell'elenco `AddModule` nel file `httpd.conf`, aggiungete la seguente linea (per il file con il codice sorgente):

```
AddModule mod_foo.c
```

È necessario modificare il nome del file con il codice sorgente.

Terminate le fasi precedenti, riavviate il vostro server Web come indicato nella Sezione 14.1, *Avvio e chiusura di `httpd`*. Se avete eseguito tutto correttamente, il server Web dovrebbe trovare il modulo e caricarlo.

14.3.1 Il modulo di sicurezza mod_ssl

La parte relativa alla sicurezza (mod_ssl) del vostro server Web Apache viene fornita come Dynamic Shared Object (DSO). Questo significa che il server Web può essere ricompilato dagli utenti e che ad Apache viene applicata la patch per l'estensione EAPI dal modulo mod_ssl. Seguite le istruzioni nella documentazione fornita con mod_ssl per inserire il mod_ssl in Apache, ma aggiungete il flag qui indicato:

```
--with-eapi-only
```

Il comando completo deve essere simile al seguente:

```
./configure [userflags] --with-eapi-only
```

Successivamente installate Apache.

Nota Bene

Red Hat non supporta le versioni ricompilate del server Web Apache. Dunque non ricompilate Apache se non conoscete esattamente i passi da seguire.

14.4 L'uso degli host virtuali

Se intendete usare il Tool di configurazione di Apache, un'utility grafica fornita con Red Hat Linux, non vi occorre modificare il file di configurazione di Apache `httpd.conf`. Viceversa, se desiderate modificare `httpd.conf` manualmente, non utilizzate il Tool di configurazione di Apache.

Per maggiori informazioni sul Tool di configurazione di Apache, consultate la *Official Red Hat Linux Customization Guide*.

Apache ha la possibilità di usare gli host virtuali, in modo che server diversi funzionino con indirizzi IP differenti sulla stessa macchina. Se siete interessati a utilizzare gli host virtuali, potete trovare la documentazione sulla vostra macchina oppure online all'indirizzo http://www.apache.org/docs/vhosts/.

Nota Bene

Non potete usare gli host virtuali con il vostro server sicuro perché la handshake SSL (il momento in cui il browser accetta il certificato di autenticazione del server Web) si attiva prima della richiesta HTTP che identifica l'host virtuale corretto. Se volete usare gli host virtuali basati sul nome, funzioneranno solo con il server Web non sicuro.

Gli host virtuali sono configurati nel file `httpd.conf` come descritto nella Sezione 14.2, *Direttive di configurazione in `httpd.conf`*. Prima di modificare la configurazione degli host virtuali, leggete la relativa documentazione.

14.4.1 Host virtuali del server Web sicuro

La configurazione di default del vostro server Web esegue un server sicuro e uno non sicuro. Entrambi i server utilizzano lo stesso indirizzo IP e il nome dell'host, ma attendono su porte differenti e il server sicuro è un host virtuale. Questa configurazione vi permette di abilitare documenti da un server sicuro e uno non sicuro nel modo più efficiente possibile. Come sapete le trasmissioni HTTP di tipo sicuro impiegano più tempo, perché il traffico è maggiore. Quindi non è una buona idea utilizzare il vostro server sicuro per un traffico Web non sicuro.

Le direttive di configurazione per il server sicuro sono contenute nei tag degli host virtuali nel file `httpd.conf`. Se dovete modificare la configurazione del server dovete cambiare il file `httpd.conf`. Se volete abilitare determinate caratteristiche per il vostro server, (per esempio gli include del server), vanno attivate nei tag degli host virtuali che definiscono il server sicuro.

Il server Web non sicuro viene configurato come host "non virtuale" nel file `httpd.conf`. In altre parole le opzioni di configurazione sono al di fuori della sezione sugli host virtuali nel file `httpd.conf`. Se volete modificare la configurazione del server Web non sicuro, dovete cambiare le direttive della configurazione nel file `httpd.conf` al di fuori dei tag relativi all'host virtuale

Di default i server Web sicuri e non sicuri condividono la stessa `DocumentRoot`, una direttiva di configurazione specificata nel file `httpd.conf`. In altre parole, i server Web sicuri e non sicuri cercano i file HTML nello stesso posto forniti in risposta alle richieste. Di default, `DocumentRoot` è `/var/www/html`.

Per cambiare la `DocumentRoot` in modo tale che non venga condivisa dai server sicuri e non sicuri, cambiate una delle direttive `DocumentRoot` nel file `httpd.conf`. La `DocumentRoot` al di fuori dei tag degli host virtuali definisce la `DocumentRoot` per il vostro server Web non sicuro.

Se per qualche ragione volete disabilitare il server Web non sicuro sulla vostra macchina, potete farlo. Il vostro server sicuro è in attesa sulla porta 443, la porta di default per le comunicazioni Web sicure, mentre il vostro server non sicuro rimane in attesa sulla porta 80, la porta di default per le comunicazioni Web non sicure. Affinché il server Web non sicuro non accetti le connessioni cercate nel file `httpd.conf` la seguente linea:

```
Port 80
```

Modificate la linea sopracitata in:

```
Port 443
```

Commentate quindi la linea `Listen 80`.

Una volta eseguite queste due operazioni, il vostro server Web accetterà connessioni sulla porta 443, la porta di default per le comunicazioni Web sicure. Quindi il vostro server non accetterà connessioni sulla porta 80. Il server Web non sicuro è infatti disabilitato.

14.4.2 Configurazione degli host virtuali

Probabilmente molte persone utilizzano il server Web con la configurazione di base. In questo modo usano la funzionalità integrata degli host virtuali, ma non sarà necessario effettuare modifiche nel file `httpd.conf`. Comunque, se per qualche ragione intendete utilizzare la funzionalità dei virtual host, potete farlo.

Per creare un host virtuale, dovete modificare le relative linee inserite per esempio nel file `httpd.conf`, o creare una sezione nuova. Ricordate che l'host virtuale basato sul nome non funziona con il vostro server sicuro — usate un host virtuale basato sull'indirizzo IP, se desiderate abilitare il supporto SSL. Invece, il server non sicuro supporta sia gli host virtuali basati sull'indirizzo IP che quelli basati sul nome.

Le righe d'esempio per l'host virtuale sono simili alle seguenti:

```
#<VirtualHost ip.address.of.host.some_domain.com>
#    ServerAdmin webmaster@host.some_domain.com
#    DocumentRoot /www/docs/host.some_domain.com
#    ServerName host.some_domain.com
#    ErrorLog logs/host.some_domain.com-error_log
#    CustomLog logs/host.some_domain.com-access_log common
#</VirtualHost>
```

Eliminate il commento dalle linee. Poi aggiungete le informazioni corrette per il vostro computer e/o per gli host virtuali in ogni linea.

Nella prima linea modificate `ip.address.of.host.some_domain.com` con i dati relativi al vostro indirizzo IP. Cambiate la direttiva `ServerName` con un nome del DNS *valido* da utilizzare come host virtuale. Se non sapete cosa inserire, contattate l'amministratore della rete.

È inoltre necessario eliminare il commento alle seguenti linee `NameVirtualHost` nel file `httpd.conf`:

```
#NameVirtualHost 12.34.56.78:80
#NameVirtualHost 12.34.56.78
```

Eliminate il commento da una delle seguenti linee e modificate l'indirizzo (e il numero di porta) per l'host virtuale.

Tra i tag degli host virtuali potete inserire molte altre direttive di configurazione, in base al tipo di configurazione.

Se state configurando un host virtuale e volete che rimanga in attesa su una porta che non sia quella di default (la 80 è la porta di default per le comunicazioni Web non sicure, mentre la 443 è la porta per le comunicazioni sicure) dovete configurare un host virtuale per quella porta e aggiungere una direttiva `Listen` corrispondente.

Per avere un host virtuale funzionante su una particolare porta, aggiungete il numero nella prima linea della configurazione dell'host virtuale. La prima linea è simile a:

```
<VirtualHost ip_address_of_your_server:12331>
```

Questa linea crea un host virtuale in attesa sulla porta 12331. Nell'esempio precedente, sostituite il numero di porta che volete utilizzare al posto di `12331`.

La linea `Listen` nel file `httpd.conf` configura il vostro server per rimanere in attesa sulla porta 12331:

```
Listen 12331
```

Effettuata la modifica, riavviate il file `httpd` per avviare un host virtuale nuovo. Per maggiori informazioni su come avviare e chiudere il file `httpd`, consultate la Sezione 14.1, *Avvio e chiusura di `httpd`*.

Informazioni più dettagliate sulla creazione e configurazione degli host virtuali basati sul nome e sull'indirizzo sono contenute all'indirizzo http://www.apache.org/docs/vhosts/index.html. Per maggiori informazioni, consultate la documentazione di Apache sull'uso degli host virtuali.

Parte IV Appendici

A Parametri generali dei moduli

Questa appendice illustra *alcuni* dei possibili parametri che potrebbero essere necessari per configurare dei driver[1]per particolari dispositivi hardware. In molti casi, questi parametri aggiuntivi non sono necessari, poiché il kernel potrebbe già essere in grado di usare il dispositivo senza tali parametri. I parametri contenuti in quest'appendice devono essere usati solo se Red Hat Linux ha problemi con un particolare dispositivo oppure se dovete sovrascrivere i parametri di default del sistema per il dispositivo.

Durante l'installazione di Red Hat Linux, dei limiti vengono posti su alcuni filesystem e su particolari driver di dispositivi supportati dal kernel. Tuttavia, dopo l'installazione è disponibile un supporto per tutti i filesystem sotto Linux. Al momento dell'installazione, il kernel modularizzato ha un supporto per i dispositivi (E)IDE (compresi i CD-ROM ATAPI), gli adattatori SCSI e le schede di rete.

Nota Bene

Dato che Red Hat Linux supporta l'installazione su diverse piattaforme hardware, alcuni driver (controller SCSI, schede di rete e alcuni CD-ROM) non sono compilati all'interno del kernel di Linux utilizzato durante la fase d'installazione, ma sono disponibili come moduli e vengono caricati all'occorrenza. Se necessario, avete la possibilità di specificare le opzioni per questi moduli in fase di caricamento.

Per specificare i parametri del modulo durante il caricamento di un driver, digitate **`linux expert`** al prompt `boot:` e inserite il dischetto dei driver quando richiesto dal programma di installazione. Una volta letto il dischetto dei driver, il programma vi chiede di selezionare il tipo di dispositivo che state configurando. In questa schermata potete specificare un parametro del modulo. Il programma di installazione visualizza in seguito una schermata dove potete digitare i parametri corrispondenti al tipo di dispositivo che state configurando.

Una volta completata l'installazione potete ricompilare il kernel per includervi il supporto per la vostra configurazione hardware specifica. È importante notare che in molti casi non è necessario ricompilare il kernel. Per maggiori informazioni sula ricompilazione del kernel, consultate la *Official Red Hat Linux Customization Guide*.

1 Un **driver** è un tipo di software che permette al sistema di usare un particolare dispositivo hardware. Senza il driver, il kernel può non sapere come usare correttamente il dispositivo.

A.1 Come specificare i parametri dei moduli

Se state fornendo i parametri sul caricamento di un modulo, potete specificarli usando uno o due metodi diversi:

- Specificando tutti i parametri di un insieme in un'unica frase. Per esempio il parametro `cdu31=0x340,0` può essere usato con una CDU Sony 31 o 33 sulla porta 340 senza IRQ.
- Specificando i parametri individualmente. Questo metodo viene usato quando alcuni parametri del primo insieme non sono necessari. Per esempio `cdu31_port=0x340 cdu31a_irq=0` può essere usato come parametro del CD-ROM usato sopra. Nelle tabelle CD-ROM, SCSI ed Ethernet di quest'appendice, un *OK* indica che il primo metodo termina e che inizia il secondo metodo.

Nota Bene

Quando caricate un modulo con parametri particolari, utilizzate un unico metodo anziché entrambi.

Se il parametro contiene delle virgole, assicuratevi che *non* ci siano spazi dopo la virgola.

A.2 Parametri per i CD-ROM

Nota Bene

Non tutte le unità CD-ROM elencate sono supportate. Consultate l'elenco delle compatibilità hardware disponibile nel sito Web di Red Hat all'indirizzo http://hardware.redhat.com e verificate che la vostra unità sia supportata.

Sebbene alcuni parametri vengano specificati dopo avere caricato il dischetto dei driver e indicato il dispositivo, uno dei parametri più comunemente usati (`hdX=cdrom`) *può* essere digitato al prompt di avvio (`boot:`). Quest'eccezione alla regola è permessa poiché serve per il supporto per i CD-ROM IDE/ATAPI, che fa già parte del kernel.

Nelle tabelle seguenti, molti moduli sono elencati senza parametri perché sono in grado di effettuare automaticamente un test oppure vi chiedono di modificare manualmente i paramentri nel codice sorgente del modulo e poi di effettuare la compilazione.

Tabella A–1 Parametri hardware

Hardware	Modulo	Parametri
Unità CD-ROM ATAPI/IDE		hd*X*=cdrom
Aztech CD268-01A, Orchid CD-3110, Okano/Wearnes CDD110, Conrad TXC, CyCDROM CR520, CyCDROM CR540 (non IDE)	`aztcd.o`	aztcd=*io_port*
CD-ROM Sony CDU 31A	`cdu31a.o`	cdu31a=*io_port,IRQ O* cdu31a_port=*base_addr* cdu31a_irq=*irq*
Lettore CDROM Philips/LMS 206 con scheda adattatore host cm260	`cm206.o`	cm206=*io_port,IRQ*
CD-ROM Goldstar R420	`gscd.o`	gscd=*io_port*
Interfaccia CD-ROM di scheda audio ISP16, MAD16 o Mozart (OPTi 82C928 e OPTi 82C929) con lettori Sanyo/Panasonic, Sony o Mitsumi	`isp16.o`	isp16=*io_port,IRQ,dma, drive_type* *OR* isp16_cdrom_base=*io_port* isp16_cdrom_irq=*IRQ* isp16_cdrom_dma=*dma* isp16_cdrom_type=*drive_type*
CD-ROM Mitsumi standard	`mcd.o`	mcd=*io_port,IRQ*
CD-ROM Mitsumi, sperimentale	`mcdx.o`	mcdx=*io_port_1,IRQ_1*, *io_port_n,IRQ_n*
Lettori CD-ROM di memorizzazione ottica "Dolphin" 8000 AT, Lasermate CR328A	`optcd.o`	
CD-ROM IDE porta parallela	`pcd.o`	

Hardware	Modulo	Parametri
Scheda audio compatibile Pro 16	`sbpcd.o`	sbpcd=*io_port*
CDR-H94A Sanyo	`sjcd.o`	sjcd=*io_port OR* sjcd_base=*io_port*
Sony CDU-535 & 531 (alcuni lettori Procomm)	`sonycd535.o`	sonycd535=*io_port*

Di seguito sono riportati alcuni esempi di moduli utilizzati:

Tabella A–2 Esempi di configurazione per i parametri hardware

Configurazione	Esempio
CD-ROM ATAPI, impostato tramite i jumper come master sul secondo canale IDE	hdc=cdrom
CD-ROM Mitsumi non IDE sulla porta 340, IRQ 11	mcd=0x340,11
Tre lettori CD-ROM Mitsumi non IDE che utilizzano il driver sperimentale, le porte io 300, 304 e 320 con gli IRQ 5, 10 e 11	mcdx=0x300,5,0x304,10,0x320,11
CDU Sony 31 o 33 sulla porta 340, senza IRQ	cdu31=0x340,0 *OR* cdu31_port=0x340 cdu31a_irq=0
CD-ROM Aztech sulla porta 220	aztcd=0x220
CD-ROM di tipo Panasonic su un'interfaccia SoundBlaster collegata alla porta 230	sbpcd=0x230,1
Phillips/LMS cm206 e cm260 su IO 340 e IRQ 11	cm206=0x340,11
Goldstar R420 su IO 300	gscd=0x300
Lettore Mitsumi su scheda MAD16 su IO Addr 330 e IRQ 1, test DMA	isp16=0x330,11,0,Mitsumi
Sony CDU 531 su indirizzo di IO 320	sonycd535=0x320

Nota Bene

Le schede Sound Blaster più recenti hanno un'interfaccia IDE. Per queste schede non è necessario utilizzare i parametri `sbpcd`, utilizzate solo i parametri `hd`*X*.

A.3 Parametri SCSI

Tabella A–3 Parametri SCSI

Hardware	Modulo	Parametri
Controller dei dischi 3ware	`3w-xxxx.o`	
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
Driver AM53/79C974 (PC-SCSI)	`AM53C974.o`	
Quasi tutte le schede Buslogic (adesso Mylex) con numero di parte "BT"	`BusLogic.o`	BusLogic_Options=*option,option,…*
Controller RAID Mylex DAC960	`DAC960.o`	
SCSI basato su MCR53c406a	`NCR53c406a.o`	
Initio INI-9100UW	`a100u2w.o`	a100u2w=*io,IRQ,scsi_id*
Adaptec AACRAID	`aacraid.o`	
Schede SCSI Advansys	`advansys.o`	
Adaptec AHA-152x	`aha152x.o`	aha152x=*io,IRQ,scsi_id*
Adaptec AHA 154x amd 631x-based	`aha1542.o`	
Adaptec AHA 1740	`aha1740.o`	

Hardware	Modulo	Parametri
Adaptec AHA-274x, AHA-284x, AHA-29xx, AHA-394x, AHA-398x, AHA-274x, AHA-274xT, AHA-2842, AHA-2910B, AHA-2920C, AHA-2930/U/U2, AHA-2940/W/U/UW/AU/, U2W/U2/U2B/, U2BOEM, AHA-2944D/WD/UD/UWD, AHA-2950U2/W/B, AHA-3940/U/W/UW/, AUW/U2W/U2B, AHA-3950U2D, AHA-3985/U/W/UW, AIC-777x, AIC-785x, AIC-786x, AIC-787x, AIC-788x, AIC-789x, AIC-3860	`aic7xxx.o`	aic7xxx=*string*
Controller SCSI PCI ACARD ATP870U	`atp870u.o`	
Controller Compaq Smart Array 5300	`cciss.o`	
Controller RAID Compaq Smart/2	`cpqarray.o`	
Controller FibreChannel Compaq	`cpqfc.o`	
Domex DMX3191D	`dmx3191d.o`	
Data Technology Corp DTC3180/3280	`dtc.o`	

Hardware	Modulo	Parametri
Adattatori host SCSI DTP (EATA/DMA) PM2011B/9X ISA, PM2021A/9X ISA, PM2012A, PM2012B, PM2022A/9X EISA, PM2122A/9X, PM2322A/9X, SmartRAID PM3021, PM3222, PM3224	`eata.o`	eata=*port0,port1,port2,…* *options OR* eata io_port=*port0,port1,port2,…* option=*value*
Adattatori SCSI DTP PM2011, PM2021, PM2041, PM3021, PM2012B, PM2022, PM2122, PM2322, PM2042, PM3122, PM3222, PM3332, PM2024, PM2124, PM2044, PM2144, PM3224, PM3334	`eata_dma.o`	
Schede DTP EATA-PIO	`eata_pio.o`	
Array di rete Sun Enterprise (FC-AL)	`fcal.o`	
Future Domain TMC-16*xx* SCSI	`fdomain.o`	
NCR5380 (generic driver)	`g_NCR5380.o`	
Controlloer RAID ICP	`gdth.o`	
Driver Block I2O	`i2o_block.o`	
Adattatore SCSI porta parallela IOMEGA MatchMaker	`imm.o`	
Scheda SCSI ISA Always IN2000	`in2000.o`	in2000=*setup_string*:*value O* in2000 *setup_string=value*
Adattatori host SCSI Initio INI-9X00U/UW	`initio.o`	
ServeRAID IBM	`ips.o`	
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	

Hardware	Modulo	Parametri
Controller SCSI NCR con chipset 810/810A/815/ 825/825A/860/875/876/895	`ncr53c8xx.o`	ncr53c8xx=*option1*:*value1*,*option2*:*value2*,… *OR* ncr53c8xx="*option1*:*value1 option2*:*value2*…"
Pro Audio Spectrum/Studio 16	`pas16.o`	
PCI-2000 IntelliCache	`pci2000.o`	
RAID EIDE PCI-2220I	`pci2220i.o`	
Array SparcSTORAGE	`pluto.o`	
Adattatore host SCSI porta parallela IOMEGA PPA3	`ppa.o`	
Perceptive Solutions PSI-240I EIDE	`psi240i.o`	
Qlogic 1280	`qla1280.o`	
Qlogic 2*x*00	`qla2x00.o`	
QLogic Fast SCSI FASXXX ISA/VLB/PCMCIA	`qlogicfas.o`	
QLogic ISP2100 SCSI-FCP	`qlogicfc.o`	
Schede SCSI QLogic ISP1020 Intelligent IQ-PCI, IQ-PCI-10, IQ-PCI-D	`qlogicisp.o`	
SCSI SBUS Qlogic ISP1020	`qlogicpti.o`	
Seagate ST-01/02, Future Domain TMC-8*xx*	`seagate.o`	
Future Domain TMC-885, TMC-950	`seagate.o`	controller_type=2 base_address=*base_addr* irq=*IRQ*
Schede con chipset sym53c416	`sym53c416.o`	sym53c416=*PORTBASE*,*[IRQ]* *O* sym53c416 io=*PORTBASE* irq=*IRQ*

Hardware	Modulo	Parametri
Adattatore host SCSI Trantor T128/T128F/T228	`t128.o`	
Tekram DC-390(T) PCI	`tmscsim.o`	
UltraStor 14F/34F (non 24F)	`u14-34f.o`	
UltraStor 14F, 24F e 34F	`ultrastor.o`	
WD7000 Series	`wd7000.o`	

Di seguito sono riportati alcuni esempi di moduli utilizzati:

Tabella A–4 Esempi di configurazione dei parametri SCSI

Configurazione	Esempio
Adaptec AHA1522 sulla porta 330, IRQ 11, SCSI ID 7	aha152x=0x330,11,7
Adaptec AHA1542 sulla porta 330	bases=0x330
Future Domain TMC-800 su CA000, IRQ 10	controller_type=2 base_address=0xca000 irq=10

A.4 Parametri Ethernet

Tabella A–5 Parametri del modulo Ethernet

Hardware	Modulo	Parametri
3Com 3c501	`3c501.o`	3c501=*io_port,IRQ*
3Com 3c503 e 3c503/16	`3c503.o`	3c503=*io_port,IRQ O* 3c503 io=*io_port_1,io_port_n* irq=*IRQ_1,IRQ_n*
3Com EtherLink Plus (3c505)	`3c505.o`	3c505=*io_port,IRQ O* 3c505 io=*io_port_1,io_port_n* irq=*IRQ_1,IRQ_2*
3Com EtherLink 16	`3c507.o`	3c507=*io_port,IRQ O* 3c507 io=*io_port* irq=*IRQ*
3Com EtherLink III	`3c509.o`	3c509=*IRQ*

Hardware	Modulo	Parametri
3Com ISA EtherLink XL "Corkscrew"	`3c515.o`	
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	
RTL8139, SMC EZ Card Fast Ethernet	`8139too.o`	
Apricot 82596	`82596.o`	
Ansel Communications Model 3200	`ac3200.o`	ac3200=*io_port,IRQ O* ac3200 io=*io_port_1*,*io_port_n* irq=*IRQ_1*,*IRQ_n*
Alteon AceNIC Gigabit	`acenic.o`	
Aironet Arlan 655	`arlan.o`	
Aironet 4500 PCI-ASI-i365 wireless	`aironet4500_card.o`	
Allied Telesis AT1700	`at1700.o`	at1700=*io_port,IRQ O* at1700 io=*io_port* irq=*IRQ*
Tangent ATB-II, Novel NL-10000, Daystar Digital LT-200, Dayna DL2000, DaynaTalk PC (HL), COPS LT-95, Farallon PhoneNET PC II, III	`cops.o`	cops=*io_port,IRQ O* cops io=*io_port* irq=*IRQ*
Driver modulare per la scheda seriale sincrona COSA o SRP	`cosa.o`	cosa=*io_port,IRQ,dma*
Crystal Semiconduc-torCS89[02]0	`cs89x0.o`	

Hardware	Modulo	Parametri
Schede EtherWORKS DE425 TP/COAX EISA, DE434 TP PCI, DE435/450 TP/COAX/AUI PCI DE500 10/100 PCI Kingston, LinkSys, SMC8432, SMC9332, Znyx31[45] e Znyx346 10/100 con chipset DC21040 (non SROM), DC21041[A], DC21140[A], DC21142, DC21143	`de4x5.o`	de4x5=*io_port OR* de4x5 io=*io_port* de4x5 args='eth*X[fdx]* autosense=*MEDIA_STRING*'
Adapter Pocket Ethernet D-Link DE-600	`de600.o`	
Adapter Pocket EthernetD-Link DE-620	`de620.o`	
DIGITAL DEPCA & EtherWORKS DEPCA, DE100, DE101, DE200 Turbo, DE201Turbo DE202 Turbo TP/BNC, DE210, DE422 EISA	`depca.o`	depca=*io_port,IRQ O* depca io=*io_port* irq=*IRQ*
Digi Intl. RightSwitch SE-X EISA e PCI	`dgrs.o`	
Davicom DM9102(A)/DM9132/ DM9801 Fast Ethernet	`dmfe.o`	
EtherExpress/1000 Gigabit Intel	`e1000.o`	
Cabletron E2100	`e2100.o`	e2100=*io_port,IRQ,mem OR* e2100 io=*io_port* irq=*IRQ* mem=*mem*

Hardware	Modulo	Parametri
EtherExpress Pro10 Intel	`eepro.o`	eepro=*io_port,IRQ O* eepro io=*io_port* irq=*IRQ*
Driver Intel i82557/i82558 PCI EtherExpressPro	`eepro100.o`	
Intel EtherExpress 16 (i82586)	`eexpress.o`	eexpress=*io_port,IRQ O* eexpress io=*io_port* irq=*IRQ*
SMC EtherPower II 9432 PCI (serie EPIC 83c170/175)	`epic100.o`	
Racal-Interlan ES3210 EISA	`es3210.o`	
ICL EtherTeam 16i/32 EISA	`eth16i.o`	eth16i=*io_port,IRQ O* eth16i ioaddr=*io_port* IRQ=*IRQ*
EtherWORKS 3 (DE203, DE204 e DE205)	`ewrk3.o`	ewrk=*io_port,IRQ O* ewrk io=*io_port* irq=*IRQ*
Fujitsu FMV-181/182/183/184	`fmv18x.o`	fmv18x=*io_port,IRQ O* fmv18x io=*io_port* irq=*IRQ*
GNIC-II Gigabit Packet Engines	`hamachi.o`	
Driver modulare per il Comtrol Hostess SV11	`hostess_sv11.o`	hostess_sv11=*io_port,IRQ, DMABIT OR* hostess_sv11 io=*io_port* irq=*IRQ* dma=*DMABIT*
HP PCLAN /plus	`hp-plus.o`	hp-plus=*io_port,IRQ O* hp-plus io=*io_port* irq=*IRQ*
HP Ethernet LAN	`hp.o`	hp=*io_port,IRQ O* hp io=*io_port* irq=*IRQ*

Hardware	Modulo	Parametri
Adattatori di rete 100VG-AnyLan HP J2585B, J2585A, J2970, J2973, J2573 Compex ReadyLink ENET100-VG4, FreedomLine 100/VG	`hp100.o`	hp100=*io_port,name O* hp100 hp100_port=*io_port* hp100_name=*name*
IBM Token Ring 16/4	`ibmtr.o`	ibmtr=*io_port,IRQ,mem O* ibmtr io=*io_port* irq=*IRQ* mem=*mem*
AT1500, HP J2405A, la maggior parte dei cloni NE2100	`lance.o`	
Mylex LNE390 EISA	`lne390.o`	
	`ltpc.o`	ltpc=*io_port,IRQ O* ltpc io=*io_port* irq=*IRQ*
SBUS MyriCOM MyriNET	`myri_sbus.o`	
Fast Ethernet NatSemi DP83815	`natsemi.o`	
NE1000 / NE2000 (non pci)	`ne.o`	ne=*io_port,IRQ O* ne io=*io_port* irq=*IRQ*
Schede PCI NE2000 RealTEk RTL-8029, Winbond 89C940, Compex RL2000, KTI ET32P2, NetVin, NV5000SC, Via 82C926, SureCom NE34	`ne2k-pci.o`	
Novell NE3210 EISA	`ne3210.o`	
MiCom-Interlan NI5010	`ni5010.o`	
Scheda NI5210(chip Ethernet i82586)	`ni52.o`	ni52=*io_port,IRQ O* ni52 io=*io_port* irq=*IRQ*
NI6510 Ethernet	`ni65.o`	

Hardware	Modulo	Parametri
Versioni precedenti il DEC 21040, quasi tutti i modelli 21*40 Ethernet	`old_tulip.o`	old_tulip=*io_port O* old_tulip io=*io_port*
AMD PCnet32 e PCnetPCI	`pcnet32.o`	
PCI RedCreek Communications	`rcpci.o`	
Schede RealTek che usano i chipset RTL8129 o RTL8139 Fast Ethernet	`rtl8139.o`	
S502/S508 multi-protocollo FR Sangoma	`sdla.o`	
Sangoma S502A, ES502A, S502E, S503, S507, S508, S509	`sdladrv.o`	
SK-98 SysKonnect*XX* Gigabit	`sk98lin.o`	
Adattatore ISA/PCI SysKonnect Token Ring, TR4/16(+) ISA o PCI, TR4/16 PCI e precedenti alle schede ISA SK NET TR4/16	`sktr.o`	sktr=*io_port*,*IRQ*,*mem O* sktr io=*io_port* irq=*IRQ* mem=*mem*
Scheda di rete ISA SMC Ultra e SMC EtherEZ (8K, 83c790)	`smc-ultra.o`	smc-ultra=*io_port*,*IRQ O* smc-ultra io=*io_port* irq=*IRQ*
Scheda Ethernet SMC Ultra32 EISA (32K)	`smc-ultra32.o`	
Schede Ethernet serie SMC 9000	`smc9194.o`	smc9194=*io_port*,*IRQ O* smc9194 io=*io_port* irq=*IRQ* ifport=*[0,1,2]*
Ethernet Sun BigMac	`sunbmac.o`	
ST201 Alta Sundance	`sundance.o`	

Hardware	Modulo	Parametri
Ethernet Sun Happy Meal	`sunhme.o`	
Ethernet Sun Quad	`sunqe.o`	
ThunderLAN	`tlan.o`	
Schede Digital 21x4x Tulip PCI Ethernet SMC EtherPower 10 PCI(8432T/8432BT) SMC EtherPower 10/100 PCI(9332DST) DEC EtherWorks 100/10 PCI(DE500-XA) DEC EtherWorks 10 PCI(DE450) DEC QSILVER's, Znyx 312 etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	
Schede Ethernet Fast VIA Rhine PCI con PCI VIA VT86c100A Rhine-II o 3043 Rhine-I D-Link DFE-930-TX 10/100	`via-rhine.o`	
Scheda ISA AT&T GIS (nee NCR) WaveLan	`wavelan.o`	wavelan=*[IRQ,0],io_port,NWID*
Schede Ethernet compatibili WD8003 e WD8013	`wd.o`	wd=*io_port,IRQ,mem, mem_end O* wd io=*io_port* irq=*IRQ* mem=*mem* mem_end=*end*
Compex RL100ATX-PCI	`winbond.o`	
Packet Engines Yellowfin	`yellowfin.o`	
Schede HDLC basate su Z8530 per AX.25	`z85230.o`	

Di seguito sono riportati alcuni esempi di moduli utilizzati:

Tabella A–6 Esempi di configurazione dei parametri Ethernet

Configurazione	Esempio
Scheda ISA NE2000 sull'indirizzo di IO 300 e IRQ 11	ne=0x300,11 ether=0x300,11,eth0
Scheda Wavelan su IO 390, autotest per IRQ e utilizzo di NWID fino a 0x4321	wavelan=0,0x390,0x4321 ether=0,0x390,0x4321,eth0

A.4.1 Utilizzo di schede Ethernet multiple

Potrete usare più schede Ethernet su una macchina. Se ciascuna scheda utilizza un driver diverso (per esempio, un 3c509 e un DE425), dovrete semplicemente aggiungere degli `alias` (e possibilmente delle `opzioni`) per ciascuna scheda a `/etc/conf.modules`. Per maggiori informazioni, consultare la *Official Red Hat Linux Customization Guide*.

Se due schede Ethernet utilizzano lo stesso driver (per esempio, due 3c509 o una 3c595 e una 3c905), nel caso di schede ISA avrete bisogno di specificare gli indirizzi di entrambe le schede nella linea delle opzioni del driver o, nel caso di schede PCI dovrete aggiungere una linea di `alias` per ciascuna scheda PCI.

Per maggiori informazioni sull'uso di più schede Ethernet, consultate il *Linux Ethernet-HOWTO* all'indirizzo http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

B Introduzione al partizionamento del disco

Le partizioni di disco costituiscono da molto tempo un aspetto corrente dell'informatica "personale". Tuttavia, poiché la maggior parte delle persone acquistano computer dotati di sistema operativo preinstallato, pochi ne capiscono il funzionamento. Questo capitolo tenta di spiegare l'utilità e il funzionamento delle partizioni di disco affinché l'installazione di Red Hat Linux sia il più semplice possibile.

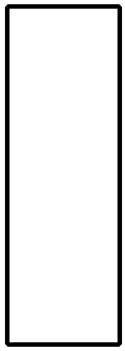
Se conoscete il funzionamento delle partizioni del disco, andate avanti alla Sezione B.1.4, *Creazione di spazio per l'installazione di Red Hat Linux* per ricevere maggiori informazioni sul processo da effettuare per liberare spazio su disco e preparare l'installazione di Red Hat Linux. Questa sezione espone inoltre lo schema utilizzato in Linux per i nomi delle partizioni, per condividere lo spazio su disco con altri sistemi operativi e altri argomenti correlati.

B.1 Concetti di base riguardanti i dischi fissi

I dischi fissi svolgono una funzione molto semplice: possono contenere e cancellare dati.

Per la discussione di questioni come il partizionamento del disco, è importante avere qualche nozione sull'hardware, purtroppo è semplice perdersi fra i dettagli. Per semplificare la spiegazione di ciò che realmente avviene durante il partizionamento, abbiamo deciso di utilizzare un diagramma semplificato di un disco fisso. La Figura B–1, *Un'unità disco non utilizzata prima* riporta un disco fisso nuovo, mai utilizzato prima.

Figura B–1 Un’unità disco non utilizzata prima

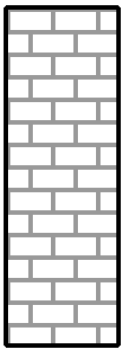


Non c’è molto da vedere, vero? Ma se parliamo di dischi fissi a livello base, la questione cambia. Supponiamo di voler salvare alcuni dati su un disco. In questo momento non è possibile. Dobbiamo prima fare qualcosa.…

B.1.1 Non conta ciò che scrivete, ma come lo scrivete

Coloro che hanno utilizzato Red Hat Linux in precedenza forse hanno già eseguito queste operazioni. Si tratta di **formattare** l’unità. Con la formattazione (in genere in gergo viene intesa come "creare un **filesystem**") vengono scritte delle informazioni sul disco. In questo modo viene creata una struttura nel disco non formattato.

Figura B–2 Unità disco con filesystem



Come mostra la Figura B–2, *Unità disco con filesystem*, l'ordine imposto da un filesystem comporta alcuni compromessi:

- Una piccola percentuale dello spazio disponibile su disco viene utilizzata per salvare i dati relativi al filesystem e può essere considerata come se si trovasse all'inizio.
- Un filesystem divide lo spazio rimanente in piccoli segmenti di dimensioni consistenti. Nel mondo Linux, questi segmenti sono conosciuti come **blocchi**. [1]

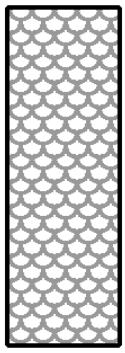
Dato che i filesystem rendono possibile operazioni come la creazione di file e directory, questi compromessi vengono generalmente visti come piccoli prezzi da pagare.

È anche vero che non esiste un filesystem singolo e universale; come mostra la Figura B–3, *Unità disco con filesystem differenti*, un disco può avere uno o più filesystem differenti. Come potrete immaginare, filesystem differenti tendono a essere incompatibili; questo vuol dire che un sistema operativo che supporta un tipo di filesystem (o un numero utile di tipi di filesystem) non è detto che ne possa supportare un altro differente. Non si tratta comunque di una regola sempre valida. Per esempio, Red

[1] I blocchi *sono* realmente di dimensioni consistenti, a differenza delle illustrazioni. Tenete inoltre presente che un disco rigido medio contiene migliaia di blocchi. Ma per lo scopo di questa spiegazione, ignorate queste piccole discrepanze.

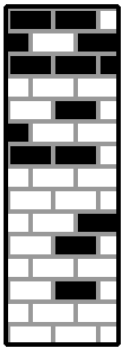
Hat Linux supporta un'ampia varietà di filesystem (inclusi quelli comunemente utilizzati da altri sistemi operativi), rendendo semplice lo scambio di dati.

Figura B–3 Unità disco con filesystem differenti



Naturalmente, l'inserimento di un filesystem su disco costituisce solo l'inizio. L'obiettivo di questo processo è quello di *conservare* e *cancellare* dati. Proviamo a controllare il nostro disco dopo la scrittura di alcuni file.

Figura B–4 Unità disco contenente dati



Come mostra la Figura B–4, *Unità disco contenente dati*, 14 dei blocchi in precedenza vuoti ora contengono dati. Non possiamo determinare quanti file risiedono su questo disco; potrebbe essere 1 così come 14, poichè tutti i file utilizzano solo un blocco. Un altro punto importante da notare è che i blocchi utilizzati non devono formare una regione contigua; blocchi utilizzati e non, possono essere separati. Questo processo è noto come **frammentazione**. La frammentazione può giocare un ruolo importante quando si tenta di ridimensionare una partizione esistente.

Con lo sviluppo delle tecnologie informatiche, le unità disco hanno continuato a mutare nel tempo. In particolare, sono diventate più grandi, non dal punto di vista delle dimensioni ma delle capacità. Ed è stato questo aumento di capacità a portare un cambiamento nell'utilizzo dei dischi.

B.1.2 Partizionamento di un disco

Con l'aumento delle capacità delle unità disco, alcune persone cominciarono a chiedersi se era una buona idea avere tutto quello spazio disponibile su un unico disco. Questa linea di pensiero fu guidata da vari argomenti, alcuni filosofici, altri tecnici. Da un punto di vista filosofico, oltre una certa dimensione, sembrava che lo spazio aggiuntivo fornito da un disco più grande creasse più confusione. Da un punto di vista tecnico, alcuni filesystem non erano mai stati disegnati per supportare dischi più

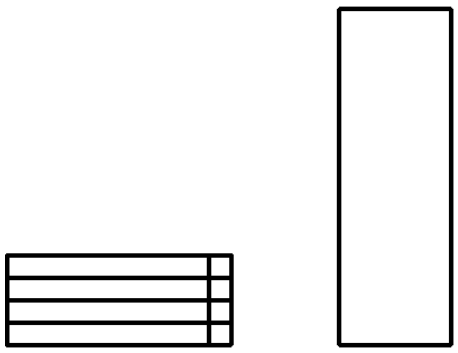
grandi. Oppure i filesystem *potevano* supportare dischi più grandi, ma la loro occupazione era diventata eccessiva.

La soluzione a questo problema fu quella di dividere i dischi in **partizioni**. Si può accedere a ogni partizione come se fosse un disco separato. Questo viene fatto attraverso l'aggiunta di una **tabella delle partizioni**.

Nota Bene

Mentre i diagrammi in questo capitolo mostrano la tavola delle partizioni separata dal resto del disco, in realtà questa è salvata all'inizio del disco, prima di ogni filesystem o dato. Ma per maggior chiarezza verrà visualizzata come un diagramma separato.

Figura B–5 Disco fisso e tabella delle partizioni



Come viene mostrato nella Figura B–9, *Unità disco con partizione inutilizzata* , la tavola delle partizioni è divisa in quattro sezioni. Ogni sezione può contenere le informazioni necessarie a definire una singola partizione: questo significa che la tavola delle partizioni può definire non più di quattro partizioni.

Ogni voce della tavola delle partizioni contiene molte caratteristiche importanti riguardanti la partizione:

- le parti del disco in cui la partizione inizia e finisce;
- informazioni relative all'attivazione della partizione;
- il tipo di partizione.

Le parti del disco in cui la partizione inizia e finisce in verità definiscono la misura delle partizioni e la posizione sul disco. L'informazione relativa all'attivazione viene utilizzata dai loader di avvio di alcuni sistemi operativi: il sistema operativo della partizione "attiva" viene avviato.

Il tipo di partizione può confondere. È infatti un numero che identifica l'utilizzo anticipato della partizione. Quest'informazione può sembrarvi un pò vaga, perché il significato stesso del tipo di partizione è vago. Alcuni sistemi operativi utilizzano il tipo di partizione per denotare un tipo specifico di filesystem, per identificare la partizione come associata a un particolare tipo di filesystem, per indicare che la partizione contiene un sistema operativo avviabile o una combinazione di queste tre possibilità.

La Tabella B–1, *Tipi di partizione* contiene una lista di alcuni tipi di partizioni diffusi (e oscuri) e il loro valore numerico.

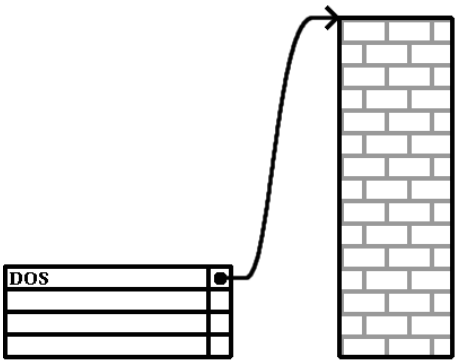
Tabella B–1 Tipi di partizione

Tipi di partizione	Valore	Tipi di partizione	Valore
Empty	00	Novell Netware 386	65
DOS 12-bit FAT	01	PIC/IX	75
XENIX root	02	Old MINIX	80
XENIX usr	03	Linux/MINUX	81
DOS 16-bit <=32M	04	Linux swap	82
Extended	05	Linux native	83
DOS 16-bit >=32	06	Linux extended	85
OS/2 HPFS	07	Amoeba	93
AIX	08	Amoeba BBT	94
AIX bootable	09	BSD/386	a5
OS/2 Boot Manager	0a	OpenBSD	a6
Win95 FAT32	0b	NEXTSTEP	a7

Tipi di partizione	Valore	Tipi di partizione	Valore
Win95 FAT32 (LBA)	0c	BSDI fs	b7
Win95 FAT16 (LBA)	0e	BSDI swap	b8
Win95 Extended (LBA)	0f	Syrinx	c7
Venix 80286	40	CP/M	db
Novell	51	DOS access	e1
Microport	52	DOS R/O	e3
GNU HURD	63	DOS secondary	f2
Novell Netware 286	64	BBT	ff

Ora vi chiederete come venga normalmente utilizzata questa parte aggiuntiva. Consultate la Figura B–6, *Disco fisso con partizione singola* per avere un esempio.

Figura B–6 Disco fisso con partizione singola



In molti casi un'unica partizione occupa tutto il disco. In questo caso, dalla tavola delle partizioni viene utilizzata solo una voce, che punta all'inizio della partizione.

Abbiamo etichettato questa partizione come se fosse di tipo "DOS", anche se come potete vedere dalla Tabella B–1, *Tipi di partizione*, questo è un pò semplicistico, ma adeguato allo scopo di questa discussione. Si tratta di una tipica configurazione di partizioni della maggior parte dei computer acquistati con una versione di Windows pre-installata.

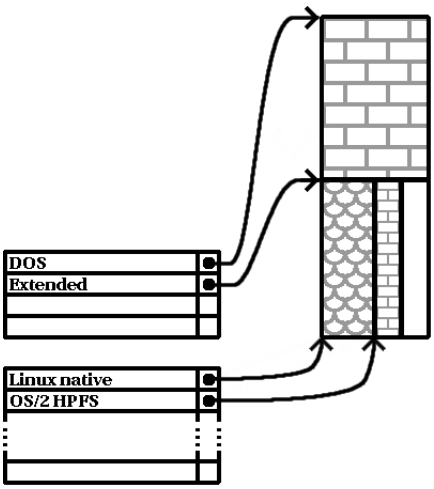
B.1.3 Partizioni all'interno di partizioni – Panoramica sulle partizioni estese

Col passare del tempo quattro partizioni non bastavano più. Con la crescita delle dimensioni dei dischi fissi, è diventata sempre più diffusa l'abitudine di creare più partizioni di dimensioni ragionevoli, riuscendo contemporaneamente ad avere ancora spazio sul disco.

Inserite la partizione estesa. Come avrete notato nella Tabella B–1, *Tipi di partizione*, esiste un tipo di partizione esteso. È proprio questo tipo di partizione che si trova al centro delle partizioni estese.

Quando una partizione viene creata e selezionata come "Extended", viene creata una tavola delle partizioni estese. In sostanza, la partizione estesa è come un'unità disco con tutte le sue caratteristiche. Ha una tavola delle partizioni che punta a una o più partizioni (ora chiamate **partizioni logiche**, invece delle quattro **partizioni primarie**) contenute interamente nella stessa partizione estesa. La Figura B–7, *Unità disco con partizione estesa* mostra una unità disco con una partizione primaria che contiene due partizioni logiche (insieme con altro spazio libero non partizionato).

Figura B–7 Unità disco con partizione estesa



Come si può notare da questa figura, esiste una differenza tra partizioni logiche e partizioni primarie -- si possono creare solo quattro partizioni primarie, ma non c'è un limite per il numero di partizioni logiche. (Tuttavia, non è una buona idea tentare di definire più di 12 partizioni su una singola unità).

Ora che abbiamo trattato in modo generale l'argomento delle partizioni, possiamo applicare queste conoscenze per installare Red Hat Linux.

B.1.4 Creazione di spazio per l'installazione di Red Hat Linux

Durante la ripartizione del disco si possono incontrare tre possibili scenari:

- spazio libero non partizionato
- partizione inutilizzata
- spazio libero in una partizione utilizzata

Analizziamo nell'ordine ogni scenario.

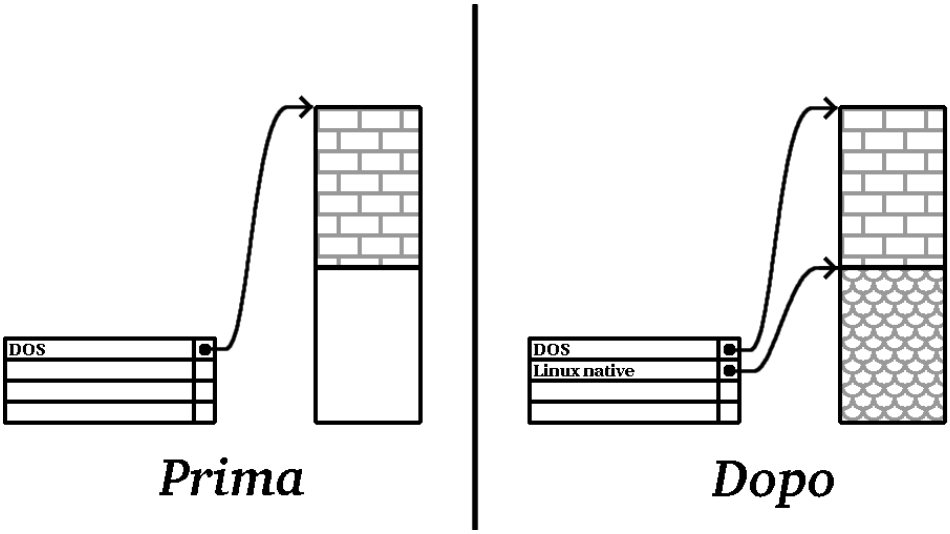
Nota Bene

Dovete tener presente che le seguenti illustrazioni sono state semplificate per maggior chiarezza, e non riflettono la struttura generale delle partizioni che incontrerete durante l'installazione di Red Hat Linux.

Utilizzo dello spazio libero non partizionato

In questo caso, le partizioni già definite non occupano l'intero disco, lasciando spazio non appartenente ad alcuna partizione definita. La Figura B–8, *Unità disco con spazio libero non partizionato* vi fornisce un esempio.

Figura B–8 Unità disco con spazio libero non partizionato



In fondo, anche un disco non utilizzato rientra in questa categoria, la sola differenza è che *tutto* lo spazio è libero e non fa parte di alcuna partizione definita.

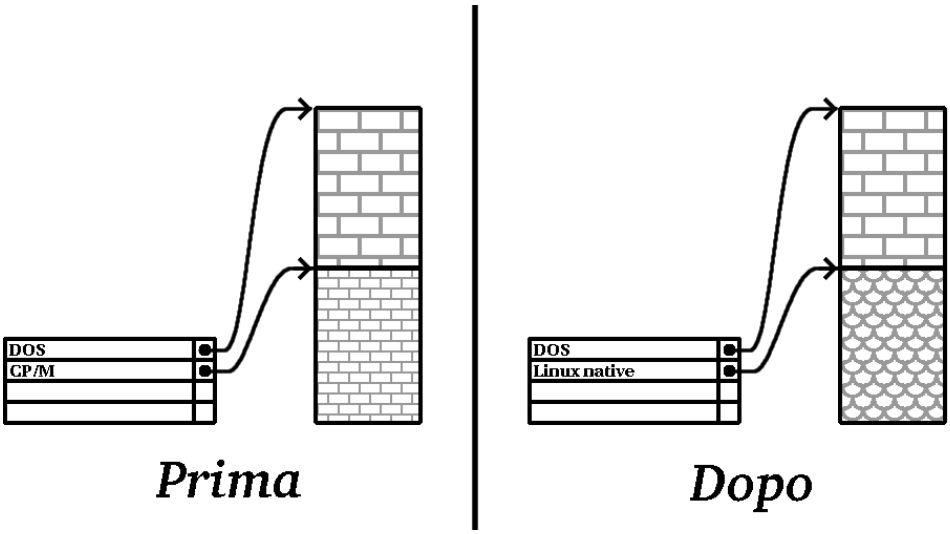
In ogni caso, potete semplicemente creare le partizioni necessarie dallo spazio non utilizzato. Sfortunatamente, questa situazione, anche se molto semplice, non è molto comune (a meno che non abbiate appena acquistato un nuovo disco solo per Red Hat Linux). La maggior parte dei sistemi operativi pre-installati sono configurati in modo da prendere tutto lo spazio disponibile su un'unità (vedere l'*Utilizzo dello spazio libero di una partizione attiva* nella sezione B.1.4).

Vediamo ora una situazione più comune.

Utilizzo dello spazio di una partizione non utilizzata

Forse avete una o più partizioni che non utilizzate più. Forse usavate un altro sistema operativo e le sue partizioni (o la partizione) non vi servono più. La Figura B–9, *Unità disco con partizione inutilizzata* illustra una situazione del genere.

Figura B–9 Unità disco con partizione inutilizzata



In questo caso, potete utilizzare lo spazio allocato per la partizione inutilizzata. Dovete prima di tutto cancellare la partizione e quindi creare le partizioni appropriate per Linux. Potete cancellare la partizione utilizzando il comando `fdisk` di DOS, oppure avete l'opportunità di farlo durante l'installazione della classe Personalizzata.

Utilizzo dello spazio libero di una partizione attiva

Questa è la situazione più comune. È anche, sfortunatamente, la più difficile da risolvere. Il problema principale infatti è che, anche se avete abbastanza spazio libero, esso è comunque allocato su una partizione già in uso. Se avete acquistato un computer con un software preinstallato, il disco rigido ha probabilmente una partizione ampia contenente il sistema operativo e i dati.

Oltre ad aggiungere un nuovo disco rigido al vostro sistema, avete due possibilità:

Ripartizionamento distruttivo

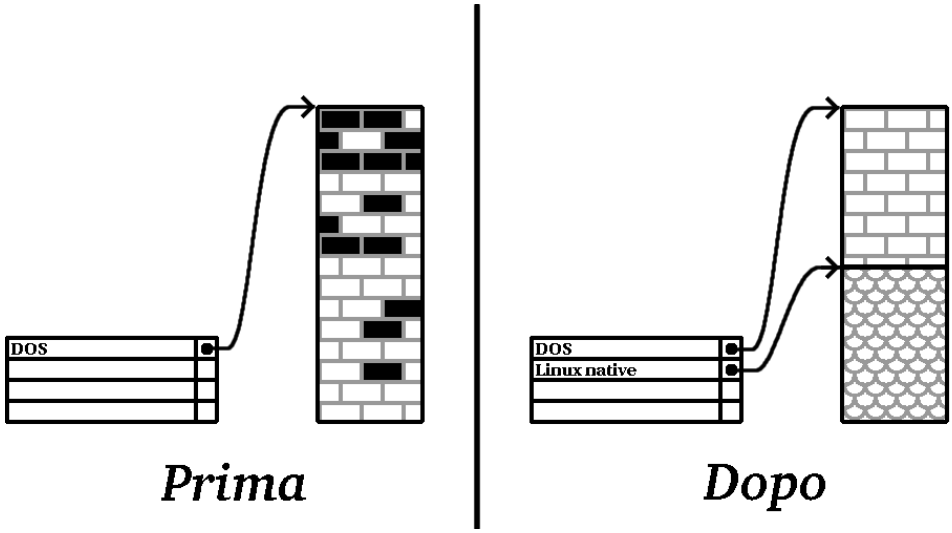
In poche parole, dovete cancellare la partizione singola, e crearne alcune più piccole. Come potrete immaginare, tutti i dati inseriti nella partizione originale verranno distrutti. Questo significa che è necessario fare prima un backup. Per sicurezza fate due backup, utilizzate la verifica (se possibile nel vostro software di backup) e provate a leggere i dati dal backup *prima* di cancellare la partizione.

ATTENZIONE

Notate inoltre che se esiste un sistema operativo installato sulla partizione, dovete reinstallarlo. Alcuni computer dotati di sistema operativo pre-installato possono non fornire il supporto CD-ROM per la reinstallazione del sistema operativo originale. Verificatelo *prima* di distruggere la partizione originale e l'installazione del sistema operativo.

Dopo aver creato una partizione più piccola per il vostro software, potete reinstallare qualunque software, ripristinare i dati e continuare con l'installazione di Red Hat Linux. La Figura B–10, *Unità disco partizionata in modo distruttivo* mostra questa operazione.

Figura B–10 Unità disco partizionata in modo distruttivo



Come mostra la Figura B–10, *Unità disco partizionata in modo distruttivo* tutti i dati presenti sulla partizione originale verranno persi senza possibilità di recupero!

Ripartizionamento non-distruttivo

Qui potete avviare un programma capace di creare una partizione più piccola senza perdere nessuno dei file contenuti nella partizione principale. Molti hanno trovato questo metodo affidabile e privo di particolari problemi. Quale software dovete utilizzare per compiere questa operazione? Ci sono parecchi software di gestione del disco sul mercato. Dovete cercare quello che più si addice alla vostra situazione.

Mentre il processo di ripartizionamento distruttivo è abbastanza intuitivo, qui ci sono alcuni passi da seguire:

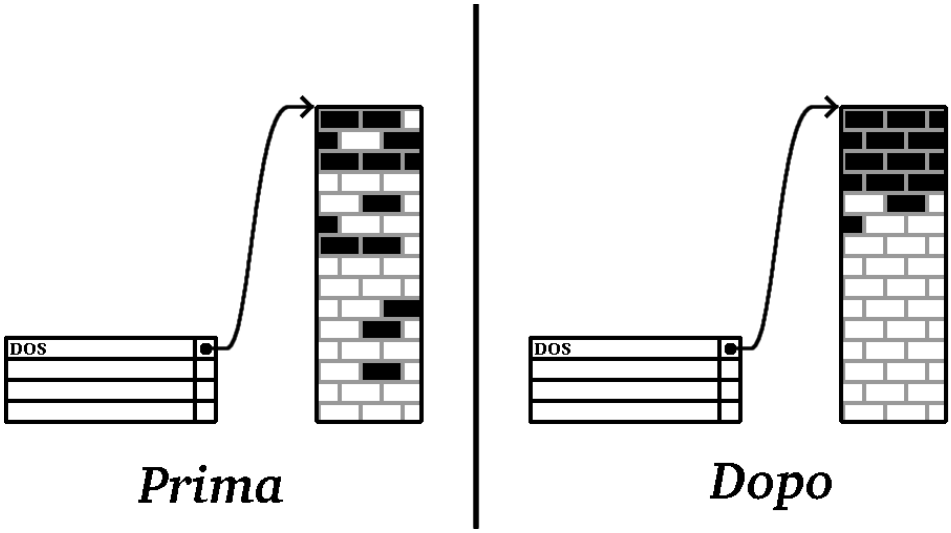
- Compressione dei dati esistenti
- Ridimensionamento della partizione
- Creazione di nuove partizioni

Osserviamo ogni passo in modo dettagliato.

Compressione dei dati esistenti

Come mostra la Figura B–11, *Unità disco durante la compressione*, il primo passo è quello di comprimere i dati della vostra partizione esistente. Il motivo di questa operazione è di riorganizzare i dati in modo da massimizzare lo spazio libero disponibile alla fine della partizione.

Figura B–11 Unità disco durante la compressione

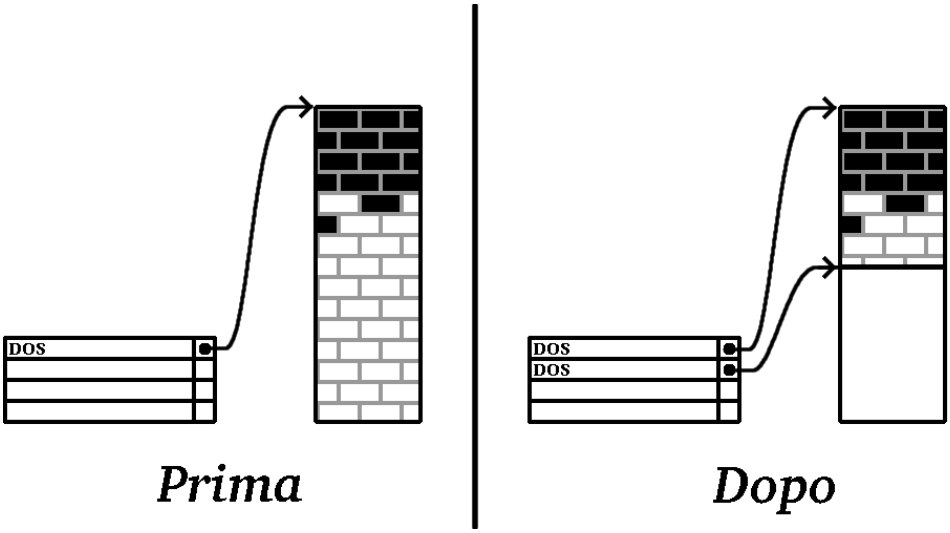


Questo passo è cruciale. Senza di esso, la locazione dei vostri dati può impedire che la partizione venga ridimensionata nella misura desiderata. Notate anche che alcuni dati non possono venire spostati. Se questo succede (e restringe la misura della/e nuova/e partizione/i), rischiate di forzare il ripartizionamento distruttivo del vostro disco.

Ridimensionamento della partizione

La Figura B–12, *Unità disco con partizione ridimensionata* mostra il processo di ridimensionamento. Mentre il risultato finale dell'operazione di ridimensionamento può variare in funzione del software utilizzato, in molti casi lo spazio appena liberato viene utilizzato per creare una partizione non formattata dello stesso tipo della partizione originale.

Figura B–12 Unità disco con partizione ridimensionata

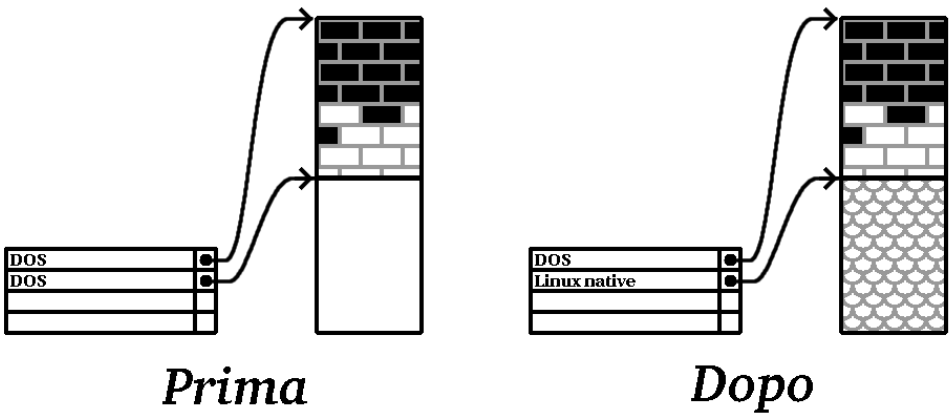


È importante capire come il software di ridimensionamento lavora con lo spazio libero creato, in modo da poter eseguire i passi appropriati. Nell'esempio fornito, sarebbe più appropriato cancellare la nuova partizione DOS e creare le partizioni appropriate per Linux.

Creazione di nuove partizioni

Può essere necessario creare nuove partizioni. Tuttavia, a meno che il vostro software di ridimensionamento consideri l'esistenza di Linux, è probabile che dobbiate cancellare la partizione creata durante il processo sopra descritto. La Figura B–13, *Unità disco con configurazione di partizione finale* mostra questa operazione.

Figura B–13 Unità disco con configurazione di partizione finale



Nota Bene

Le informazioni seguenti riguardano i computer basati su Intel.

Per una questione di convenienza, vi forniamo l'utility `fips`. Si tratta di un programma distribuito liberamente che può ridimensionare partizioni FAT (File Allocation Table). Esso è incluso nella directory `dosutils` del CD-ROM di Red Hat Linux/x86.

AVVERTIMENTO

Molte persone hanno utilizzato con successo `fips` per ripartizionare i dischi fissi. Tuttavia, a causa della natura delle operazioni che `fips` deve compiere e della varietà di configurazioni hardware e software esistenti, Red Hat non può garantire che `fips` funzioni correttamente sul vostro sistema. Per questo motivo, non viene fornito il supporto per l'installazione di `fips` e il suo utilizzo è a vostro rischio e pericolo.

Di conseguenza, se decidete di ripartizionare il vostro disco con `fips`, è *importante* che facciate due cose:

- *Eseguire un backup* — Fate due copie di tutti i dati importanti presenti sul vostro computer: queste copie dovrebbero essere fatte su dispositivi rimovibili (come nastri o dischetti). Prima di procedere dopo aver fatto il backup assicuratevi che i dati siano leggibili.
- *Leggere la documentazione* — Leggete tutta la documentazione di `fips` contenuta nella sottodirectory `/dosutils/fipsdocs` del primo CD di Red Hat Linux/x86.

Se decidete di utilizzare `fips`, verificate che dopo il suo avvio ci siano *due* partizioni: quella ridimensionata e quella che `fips` ha creato dallo spazio libero della prima partizione. Se il vostro obiettivo è quello di utilizzare questo spazio per installare Red Hat Linux, cancellate la partizione appena creata utilizzando il comando `fdisk` sotto il sistema operativo corrente, oppure configurate le partizioni durante l'installazione di classe Personalizzata.

B.1.5 Schema dei nomi per le partizioni

Linux fa riferimento alle partizioni del disco utilizzando una combinazione di lettere e numeri che può confondere, soprattutto se siete abituati al metodo di riferimento come "drive C" per i dischi e le partizioni. Nel mondo DOS/Windows:

- Ogni tipo di partizione viene controllato per determinare se può essere letto da DOS/Windows.
- Se la partizione è compatibile, le viene assegnata una "lettera del disco". Le lettere dei dischi iniziano dalla lettera "C" e proseguono in funzione del numero di partizioni da etichettare.
- La lettera del disco può quindi essere utilizzata per fare riferimento a questa partizione così come al filesystem contenuto in questa partizione.

Red Hat Linux utilizza per i nomi uno schema più flessibile e ricco di informazioni rispetto all'approccio utilizzato da altri sistemi operativi. Lo schema dei nomi è basato sui file, con nomi del tipo:

`/dev/`*`xxyN`*

Ecco come decifrare lo schema del nome della partizione:

`/dev/`

Questa stringa è il nome di una directory nella quale risiedono tutti i file device. Visto che le partizioni risiedono su disco e i dischi rigidi sono dispositivi, i file che rappresentano tutte le possibili partizioni sono contenuti in `/dev/`.

`xx`

Le prime due lettere del nome della partizione indicano il tipo di periferica su cui risiede la partizione stessa. In genere trovate `hd` (per i dischi IDE) oppure `sd` (per i dischi SCSI).

y

Questa lettera indica su quale dispositivo si trova la partizione. Per esempio, `/dev/hda` (il primo disco IDE) oppure `/dev/sdb` (il secondo disco SCSI).

N

Il numero finale indica la partizione. Le prime quattro partizioni (primarie o estese) vengono numerate da `1` a `4`. Le partizioni logiche iniziano da `5`. Per esempio, `/dev/hda3` è la terza partizione primaria o estesa sul primo disco IDE; `/dev/sdb6` è la seconda partizione logica sul secondo disco SCSI.

Nota Bene

Non esiste ancora nessuna convenzione su questa metodologia di partizionamento. A differenza di DOS/Windows, *tutte* le partizioni possono essere identificate sotto Red Hat Linux. Naturalmente, questo non significa che Red Hat Linux può accedere ai dati su qualunque tipo di partizione, ma in molti casi è possibile accedere ai dati di partizioni dedicate ad altri sistemi operativi.

Queste informazioni vi faciliteranno le cose quando configurerete le partizioni richieste da Red Hat Linux.

B.1.6 Partizioni e altri sistemi operativi

Se le partizioni di Red Hat Linux devono dividere lo spazio sul disco con partizioni utilizzate da altri sistemi operativi, non dovreste avere problemi. Tuttavia, alcune combinazioni di Linux e altri sistemi operativi richiedono maggiori precauzioni. Informazioni sulla creazione di partizioni su disco compatibili con altri sistemi operativi sono disponibili in molti HOWTO e Mini-HOWTO contenuti nelle directory `doc/HOWTO` e `doc/HOWTO/mini` del CD di Red Hat Linux. In particolare, sono molto utili i Mini-HOWTO i cui nomi iniziano con `Linux+`.

Nota Bene

Perché Red Hat Linux/x86 possa coesistere sulla vostra macchina con altri sistemi operativi , dovrete creare le partizioni con il software per la gestione delle partizioni di OS/2 —— altrimenti OS/2 potrebbe non riconoscere le partizioni sul disco. Durante l'installazione non create alcuna nuova partizione, ma create le giuste partizioni per Linux utilizzando il comando `fdisk` di Linux.

B.1.7 Partizioni su disco e Mount Point

Una situazione in cui molti nuovi utenti di Linux si trovano in difficoltà è capire come vengono utilizzate le partizioni e come si accede ad esse sotto il sistema operativo Linux. In DOS/Windows la questione è relativamente semplice: se esistono più partizioni, ogni partizione utilizza una "lettera per disco". Quindi potete utilizzare la lettera per fare riferimento a tale partizione.

Il metodo con cui Red Hat Linux gestisce le partizioni e, quindi, le unità disco in generale, è completamente differente. La differenza risiede nel fatto che ogni partizione viene utilizzata come parte dell'albero del filesystem di Linux. Questo viene fatto associando una partizione a una directory attraverso un processo chiamato **mounting** (lett. montaggio). Montare una partizione vuol dire rendere disponibile il contenuto di questa a partire dalla directory specificata (alla quale si fa riferimento con il nome di **mount point**).

Per esempio, se la partizione `/dev/hda5` viene montata sotto `/usr`, significha che tutti i file e le directory sotto `/usr` risiedono fisicamente su `/dev/hda5`. Così il file `/usr/doc/FAQ/txt/Linux-FAQ` è contenuto in `/dev/hda5`, ma non il file `/etc/X11/gdm/Sessions/Gnome`.

Continuando con questo esempio, è anche possibile che una o più directory sotto `/usr` siano mount point per altre partizioni. Per esempio, una partizione (come `/dev/hda7`) può essere montata sotto `/usr/local`, il che significa che `/usr/local/man/whatis` risiede su `/dev/hda7` anziché su `/dev/hda5`.

B.1.8 Quante partizioni?

A questo punto del processo di preparazione per l'installazione di Red Hat Linux, dovete tenere in considerazione il numero e le dimensioni delle partizioni che vengono utilizzate con il nuovo sistema operativo. La domanda "quante partizioni" continua a scatenare discussioni nella comunità Linux. Probabilmente ci sono tante possibilità di creare partizioni quante sono le persone che ne discutono.

Tenendo presente questo, vi raccomandiamo di creare le partizioni seguenti:

- *Partizione swap* — Le partizioni swap vengono utilizzate per supportare la memoria virtuale. In altre parole, i dati vengono scritti sulla partizione swap quando la memoria disponibile non è in grado di contenere i dati che il vostro sistema sta elaborando. La partizione swap è *indispensabile* affiché Red Hat Linux funzioni correttamente. La dimensione minima della partizione swap dovrebbe corrispondere al doppio della RAM del computer oppure a 32 MB (tra le due la dimensione maggiore).
- *Partizione `/boot`* — La partizione montata sotto `/boot` contiene il kernel del sistema operativo (che permette l'avvio di Red Hat Linux), nonché alcuni file utilizzati durante il processo di avvio.

Assicuratevi di leggere la Sezione B.1.9, *Ultimo consiglio: utilizzare LILO* — le informazioni riportate in questa sezione riguardano la partizione `/boot`!

A causa delle limitazioni della maggior parte dei BIOS dei PC, creare una piccola partizione contenente questi file può essere una buona idea. Le dimensioni di questa partizione non devono superare i 32 MB.

- *Partizione di root (/)* — In essa risiede `/` (la directory di root). In questa configurazione di partizioni, tutti i file (eccetto quelli che risiedono in `/boot`) risiedono sulla partizione di root. Per questo sarebbe una buona scelta massimizzare la misura della vostra partizione di root. Una partizione di root di 1.2 GB permette di effettuare un'installazione di classe Workstation (con *pochissimo* spazio libero), mentre una partizione di root di 2.4 GB permette di installare qualsiasi pacchetto. Ovviamente, vi raccomandiamo di assegnare alla partizione di root il maggior spazio possibile

L'*Official Red Hat Linux x86 Installation Guide* contiene raccomandazioni riguardanti le dimensioni delle varie partizioni Red Hat Linux.

B.1.9 Ultimo consiglio: utilizzare LILO

LILO (il LInux LOader) è il metodo più comune per avviare Red Hat Linux su sistemi Intel. Come loader per il sistema operativo, LILO opera "esternamente" a qualsiasi sistema operativo, utilizzando solo il Basic I/O System (o BIOS) incluso nell'hardware del sistema stesso. Questa sezione descrive l'interazione di LILO con i BIOS dei PC ed è specifica per i computer compatibili con Intel.

Limitazioni riguardanti il BIOS con LILO

LILO è soggetto ad alcune limitazioni imposte dal BIOS in molti computer Intel. In modo specifico, la maggior parte dei BIOS non possono accedere a più di due dischi fissi e non possono accedere ai dati inclusi oltre il cilindro 1023 di qualunque unità. I BIOS più recenti non hanno queste limitazioni, ma questo non significa che il problema non sia diffuso.

Tutti i dati di cui LILO ha bisogno al momento dell'avvio della macchina (incluso il kernel di Linux) sono contenuti nella directory `/boot`. Se seguite la configurazione per le partizioni di cui sopra, oppure state eseguendo un'installazione di classe Workstation o Server, la directory `/boot` verrà creata in una partizione piccola e separata. Altrimenti, risiederà nella partizione di root. Affinché LILO funzioni bene sul vostro sistema Red Hat Linux, la partizione sulla quale risiede `/boot` deve essere conforme alle seguenti regole:

Sui primi due dischi IDE

Se avete 2 dischi IDE (o EIDE), `/boot` deve risiedere su uno di essi. Notate che questo limite dei due dischi include anche qualunque unità CD-ROM IDE sul controller primario IDE. Se avete un disco IDE e un CD-ROM IDE sul controller primario, `/boot` deve essere contenuta *solo* sul primo disco, anche se avete altri dischi rigidi sul controller secondario IDE.

Sul primo disco IDE o SCSI

Se avete una unità IDE (o EIDE) e una o più unità SCSI, `/boot` deve trovarsi o sul disco IDE o su quello SCSI sull'ID 0. Altri ID SCSI non funzioneranno.

Sui primi due dischi SCSI

Se avete solo dischi SCSI, `/boot` deve trovarsi su un disco sull'ID 0 o ID 1. Altri ID SCSI non funzioneranno.

Partizione *completamente* sotto il cilindro 1023

Non importa quale delle configurazioni descritte utilizziate, la partizione che conterrà `/boot` deve essere creata entro il cilindro 1023. Se la partizione che contiene `/boot` supera il cilindro 1023, potreste ritrovarvi in situazioni dove il LILO funziona inizialmente (perché tutte le informazioni necessarie sono sotto il cilindro 1023), ma non funziona se deve essere caricato un nuovo kernel, e questo si trova oltre tale cilindro.

Come si è detto prima, è possibile che alcuni dei BIOS più recenti permettano a LILO di funzionare con configurazioni che non corrispondono alle configurazioni descritte. Allo stesso modo possono essere utilizzate alcune caratteristiche del LILO più nascoste per far avviare il sistema, anche con configurazioni apparentemente diverse da quelle descritte. Tuttavia, a causa del numero di possibili configurazioni esistenti, Red Hat Linux non può supportare ulteriori metodi straordinari riguardo a questo argomento

---

Nota Bene

Disk Druid e le installazioni delle classi server e workstation tengono conto di queste limitazioni dovute al BIOS.

C Dischetto dei driver

C.1 Perché ho bisogno di un disco contenente dei driver?

Durante il caricamento del programma di installazione Red Hat Linux, potrebbe apparire una schermata che vi chiede di inserire un dischetto contenente dei driver. Il dischetto dei driver viene richiesto nei tre casi seguenti:

- se state eseguendo un'installazione in `modalità expert`,
- se eseguite il programma di installazione digitando `linux dd` al prompt `boot:`,
- se eseguite il programma di installazione su un computer senza dispositivi PCI.

C.1.1 Cos'è un dischetto dei driver?

Un dischetto dei driver aggiunge il supporto per la gestione di particolari periferiche hardware che altrimenti non sarebbero supportate dal programma di installazione. Può essere prodotto da Red Hat, potete crearlo voi a partire da driver trovati in Internet o può essere fornito con l'hardware dal rivenditore.

Non ci dovrebbe essere bisogno di un dischetto dei driver a meno che non abbiate bisogno del supporto di un particolare dispositivo per installare Red Hat Linux. Il dischetto dei driver viene utilizzato di solito per unità CD-ROM non standard o molto recenti, particolari controller SCSI o schede di rete. Questi sono gli unici dispositivi usati durante l'installazione che potrebbero richiedere driver non inclusi nel nel CD-ROM di Red Hat Linux (o nel dischetto floppy, se avete creato un dischetto di avvio per lanciare il processo di installazione).

Nota bene

Se un dispositivo non è richiesto per l'installazione di Red Hat Linux, continuate con l'installazione standard e aggiungete la gestione del nuovo hardware al riavvio di Red Hat Linux.

C.1.2 Come ottenere il dischetto dei driver?

Il CD-ROM 1 di Red Hat Linux include un'immagine di un dischetto dei driver (`images/drivers.img`) contenente numerosi driver poco usati. Se pensate che il vostro sistema necessiti di uno di questi driver, vi consigliamo di creare il dischetto dei driver prima di iniziare l'installazione di Red Hat Linux.

Informazioni specifiche sui driver sono contenute anche nel sito Web di Red Hat all'indirizzo http://www.redhat.com/support/errata nella sezione chiamata **Bug Fixes**. Può capitare che alcune macchine molto famose siano messe in commercio dopo la versione di Red Hat Linux. Per questo motivo, tali macchine non possono funzionare con i driver già presenti nel programma di installazione o inclusi nell'immagine del dischetto dei driver del CD-ROM 1 di Red Hat Linux. Per l'installazione di Red Hat Linux su queste macchine vi consigliamo di usare l'immagine del dischetto dei driver presente nel sito Web di Red Hat.

Creazione di un dischetto dei driver a partire da un file di immagine

Se dovete trasferire un'immagine del dischetto dei driver su un dischetto floppy, potete farlo usando DOS o Red Hat Linux.

Per creare un dischetto dei driver a partire da un'immagine del dischetto dei driver usando Red Hat Linux:

1. Inserite un dischetto vuoto e formattato nell'unità floppy A:.
2. Nella stessa directory contenente l'immagine del dischetto dei driver *dd.img*, digitate `cat`*`dd.img`* `> /dev/fd0` come root.

Per creare un dischetto dei driver a partire da un'immagine di dischetto dei driver usando DOS:

1. Inserite un dischetto vuoto e formattato nell'unità floppy.
2. Nella stessa directory contenente l'immagine del dischetto dei driver *dd.img*, digitate `rawrite` *`dd.img`* `A:` alla linea di comando.

C.1.3 Utilizzo di un dischetto dei driver durante l'installazione

Il fatto di disporre di un dischetto dei driver non basta. È necessario infatti dire al programma di installazione di Red Hat Linux di caricare il dischetto e di utilizzarlo durante il processo di installazione.

Nota Bene

Un dischetto dei driver è diverso da un dischetto di avvio. Se necessitate di un dischetto floppy per iniziare l'installazione di Red Hat Linux, prima di poter usare il dischetto dei driver dovrete creare un dischetto di avvio e avviare il sistema da tale.

Se non avete ancora un dischetto per l'installazione e il vostro sistema non supporta l'avvio da CD-ROM, create un dischetto di installazione usando il file *`nomefile`*`.img` corretto (per esempio `boot.img`) della directory `images` del CD-ROM 1. Per informazioni sulla creazione di un dischetto di avvio, consultate la sezione *Creazione dei dischetti di installazione* della *Official Red Hat Linux x86 Installation Guide*.

Una volta creato il dischetto dei driver, lanciate il processo di installazione con il dischetto di avvio o il CD-ROM 1 (oppure il dischetto di avvio dell'installazione creato, se per qualche ragione non riuscite ad avviare l'installazione dal CD-ROM). Quindi, al prompt `boot:`, digitate **`linux expert`** o **`linux dd`**.

Il programma di installazione di Red Hat Linux vi chiederà di inserire il dischetto dei driver. Una volta che il dischetto viene letto dal programma di installazione, può gestire i driver rilevati durante il processo di installazione.

D RAID (Redundant Array of Independent Disks)

D.1 Cos’è il RAID?

L’idea di base dietro al RAID è di combinare più dischi di modeste dimensioni e di costo ridotto in un array che superi le prestazioni di un disco unico, grande e costoso. Questo array di dischi viene visto dal computer come un unico dispositivo.

La tecnologia RAID offre un metodo per suddividere le informazioni su vari dischi, usando tecniche come il **disk striping** (RAID livello di 0), il **disk mirroring** (RAID di livello 1) e il **disk striping with parity** (RAID di livello 5) per aggiungere ridondanza ai dati, ottenere una latenza inferiore e/o una larghezza banda superiore per leggere o scrivere dati su dischi e massimizzare la capacità di recupero dopo un crash del disco.

Il concetto di base della tecnologia RAID è che i dati possono essere distribuiti tra i dischi dell’array in maniera consistente. Per fare questo, i dati devono prima venir spezzati in "chunk" (spesso di 32k o 64k di grandezza, anche se vengono a volte usate altre dimensioni). Ogni chunk viene così scritto sui dischi a turno. Quando i dati vengono letti, il processo avviene al contrario, dando l’illusione che più dischi siano combinati in una unica unità.

D.1.1 Chi dovrebbe usare i RAID?

Coloro che devono gestire grandi quantità di dati e necessitano di un sistema che resista ai guasti hardware. I principali vantaggi apportati dalla la tecnologia RAID sono:

- maggiore velocità
- aumento della capacita di archiviazione usando un unico disco virtuale
- grande efficienza nel recupero in seguito a un crash del sistema

D.1.2 RAID: hardware e software

Esistono due possibili approcci al RAID: il RAID hardware e il RAID software.

RAID hardware

Le soluzioni hardware gestiscono il sottosistema RAID indipendentemente dall’host e presentano all’host un singolo disco per array.

Un esempio di RAID hardware potrebbe essere quello collegato a un controller SCSI che presenta al sistema un unico disco SCSI. Un sistema RAID esterno sposta tutta "l’intelligenza" gestita dal RAID

in un controller situato nel sottosistema del disco esterno. Tutto il sottosistema è collegato a un calcolatore tramite un normale controller SCSI e compare come un singolo disco.

Esistono anche controller RAID nella forma di schede che *agiscono* come un controller e gestiscono tutte le comunicazioni reali tra i dischi in modo autonomo. In questi casi, basta collegare i dischi a un controller RAID così come fareste con un controller SCSI, ma dovete aggiungerli alla configurazione del controller RAID perché il sistema operativo non veda la differenza.

RAID software

Il Software RAID implementa i vari livelli di RAID nel codice del kernel riguardante la gestione del disco (block device). Offre inoltre la soluzione in assoluto meno costosa: non sono richiesti costosi controller dedicati o chassis hot-swap, [1]e il RAID software funziona sia con dischi IDE meno costosi sia con dischi SCSI. Con le CPU dell'ultima generazione, le prestazioni di un RAID software possono eccellere quelle di un RAID hardware.

Il driver MD nel kernel di Linux è un esempio di una soluzione RAID completamente indipendente dall'hardware. Le prestazioni di un array basato su software dipende dalle prestazioni e dal carico della CPU.

Per informazioni sulla configurazione del RAID software nel programma di installazione di Red Hat Linux, consultate la *Official Red Hat Linux Customization Guide*.

Per coloro che desiderano ricevere maggiori informazioni sul RAID software, ecco un breve elenco delle sue caratteristiche più importanti:

- Processo di ricostruzione basato su thread
- Configurazione completamente basata sul kernel
- Portabilità di array tra macchine Linux senza ricostruire l'array RAID
- Ricostruzione dell'array in background utilizzando risorse inutilizzate di sistema
- Supporto per drive sostituibili a caldo
- Riconoscimento automatico della CPU per sfruttare alcune ottimizzazioni della CPU

D.1.3 Livelli e supporto lineare

Il RAID offre il supporto per i livelli 0, 1, 4, 5, e lineare. Questi tipi di RAID si comportano nel modo seguente:

- *Livello 0* — Il RAID di livello 0, spesso chiamato "striping," è una tecnica orientata alle prestazioni di mappatura dati "striped". Questo vuol dire che i dati scritti sull'array vengono divisi in strisce e scritti sui dischi membri dell'array. Questo permette alte prestazioni di I/O a un basso costo, ma

[1] Uno chassis hot-swap vi permette di rimuovere un disco rigido senza dover spegnere il computer.

non fornisce ridondanza. La capacità di memorizzazione dell'array è uguale alla capacità totale dei dischi membri in un RAID hardware o alla capacità totale delle partizioni membri in un RAID software.

- *Livello 1* — Il RAID di livello 1 o "mirroring," è stato utilizzato più a lungo rispetto ad altre forme di RAID. Il livello 1 fornisce ridondanza scrivendo dati identici su ogni disco membro dell'array, lasciando una copia "identica" su ciascun disco. Il mirroring rimane popolare grazie alla sua semplicità e all'alto livello di disponibilità di dati. Il livello 1 opera con due o più dischi che possono utilizzare una modalità di accesso parallelo per trasferimenti veloci di dati in lettura, ma più comunemente opera in modo indipendente per fornire alti valori di transazioni di I/O. Il livello 1 assicura un'alta affidabilità e migliora le prestazioni per applicazioni intensive nella lettura dati ma a un costo relativamente alto[2]. La capacità di memorizzazione dell'array di livello 1 è uguale alla capacità di uno dei dischi fissi copiati in un RAID hardware o di una della partizioni copiate in un RAID software.

- *Livello 4* — Il RAID di livello 4 utilizza la parità[3]concentrandola su un singolo disco per la protezione dei dati. È più adeguato alle transazioni di I/O piuttosto che ai pesanti trasferimenti di dati. Poiché il disco dedicato alla parità rappresenta un collo di bottiglia non indifferente, il livello 4 è utilizzato di rado senza tecnologie aggiuntive come il write-back caching. Anche se il RAID di livello 4 è un'opzione in alcuni schemi di ripartizionamento RAID, non è un opzione permessa nell'installazione RAID di Red Hat Linux [4]. La capacità del RAID hardware di livello 4 è uguale alla capacità dei dischi membri meno la capacità di un disco. La capacità del software RAID di livello 4 è uguale alla capacità delle partizioni membri meno le dimensioni di una partizione se hanno le stesse dimensioni.

- *Livello 5* — È il tipo più comune di RAID. Distribuendo la parità tra alcuni o tutti i dischi membri, il RAID di livello 5 elimina il collo di bottiglia inerente al livello 4. L'unico collo di bottiglia è il processo di calcolo della parità. Con le moderne CPU e il RAID software, ciò non rappresenta un grosso problema. Come con il livello 4, i risultati sono prestazioni molto elevate, con letture sostanzialmente migliori delle scritture. Il livello 5 è spesso utilizzato con il write-back caching per ridurre l'asimmetria. La capacità del RAID hardware di livello 5 è uguale alla capacità dei

[2] Il RAID livello 1 ha un alto costo poiché si scrivono le stesse informazioni su tutti i dischi dell'array, sprecando un notevole spazio di memorizzazione. Per esempio: avete configurato il RAID di livello 1 in modo che la vostra partizione root (`/`) sia su dischi da 40 GB. Avete una capacità totale di 80 GB ma potete memorizzarne solo 40 GB. Gli altri 40 GB si comportano come una copia di riserva dei primi 40 GB.

[3] Le informazioni sulla parità vengono calcolate in base al contenuto degli altri dischi membri dell'array. Queste informazioni possono essere quindi utilizzate per la ricostruzione dei dati quando uno dei dischi dell'array viene danneggiato. I dati ricostruiti possono quindi essere utilizzati per soddisfare le richieste di I/O per il disco danneggiato prima che venga sostituito e per ricostituirne il contenuto dopo la sua sostituzione.

[4] Il RAID di livello 4 richiede fino allo stesso spazio richiesto dal livello 5, ma il livello 5 ha molti più vantaggi rispetto al livello 4. Per questo motivo il livello 4 non viene supportato.

dischi membri meno la capacità di un disco. La capacità del RAID software di livello 5 è uguale alla capacità delle partizioni membri meno le dimensioni di una partizione se hanno le stesse dimensioni.

- *RAID lineare* — Il RAID lineare è un semplice raggruppamento di dischi in modo da creare un disco virtuale più grande. Nel RAID lineare, i chunk sono disposti sequenzialmente da un disco membro fino al disco successivo solo quando il primo è pieno. Questo raggruppamento non porta vantaggi a livello delle prestazioni, così come è poco probabile che un'operazione di I/O venga divisa tra i dischi membri. Il RAID lineare non offre ridondanza e infatti l'affidabilità diminuisce: se uno dei drive viene meno, l'intero array non può essere utilizzato. La capacità è quella totale di tutti i dischi membri.

E PowerTools

E.1 Cosa sono i PowerTools?

Red Hat PowerTool è una raccolta di pacchetti software creati per il sistema operativo Red Hat Linux 7.1. PowerTools include le ultime versioni (alla data di rilascio del prodotto) di centinaia di programmi. Perciò risulterà semplice trovare qualunque tipo di applicazione.

Questa raccolta di software contiene applicazioni audio, chat client, tool per lo sviluppo, editor di testi, file manager, emulatori, giochi, programmi per la grafica, pacchetti matematici/statistici, amministrazione di sistema e tool per la gestione della rete, window manager ecc.

Siete un amministratore di sistema? PowerTools offre un insieme di strumenti che possono semplificarvi la vita e sostituire varie utility costose di diagnosi con un'unica applicazione. Date un'occhiata ad applicazioni quali Ethereal per l'analisi dei protocolli di rete, PortSentry per impedire la lettura delle porte sulla rete e Postfix come alternativa a Sendmail.

Vi piace giocare? PowerTools contiene numerosi giochi semplici e divertenti quali SpeedX, XFrisk e Amphetamine.

E visto che, grazie alle applicazioni RPM e Gnome-RPM, installare e disinstallare pacchetti software su Red Hat Linux è molto semplice, potete provare varie applicazioni uguali prima di scegliere quella che più vi convince.

E.2 Pacchetti PowerTools

Se sapete già quali pacchetti PowerTools installare, consultate la Sezione E.3, *Installazione dei pacchetti PowerTools* per informazioni sull'installazione.

Tuttavia, a causa dell'elevato numero di pacchetti PowerTools disponibili, è utile scorrere le descrizioni per capire quali rispondono alle proprie necessità.

E.2.1 Lettura del contenuto del CD-ROM

Potete accedere al contenuto del CD-ROM PowerTools dal prompt di una shell (sia in una finestra terminale che dalla console di testo). Innanzitutto dovete montare l'unità CD-ROM.

Montaggio del CD-ROM di PowerTools

Se il vostro sistema non è configurato in modo da montare automaticamente l'unità CD-ROM quando è inserito un CD, inserite il CD di PoweTools nell'unità e digitate come root:

```
mount -t iso9660 /dev/cdrom /mnt/cdrom
```

Nota Bene

L'amministratore del sistema potrebbe permettere agli altri utenti di effettuare l'operazione di mount di CD. Gli utenti possono beneficiare di questo privilegio solo se l'opzione `user` è inclusa nella linea `/dev/cdrom` del file `/etc/fstab`. Comunque solo l'utente root può installare i pacchetti RPM PowerTools.

Lettura del file `CONTENTS`

Una volta montata l'unità, cambiate directory digitando il comando seguente:

```
cd /mnt/cdrom
```

Infine, digitate `less CONTENTS` per visualizzare le applicazioni disponibili. Il file `CONTENTS` contiene tutti i programmi del CD-ROM di PowerTools elencati in ordine alfabetico.

Leggere il file `CONTENTS` del CD-ROM di PowerTools può essere un compito faticoso considerato il numero di applicazioni disponibili. Ecco alcuni consigli per trovare un tipo particolare di programma senza dovere leggere tutte le descrizioni:

- *Usate i nomi di gruppo* — Ogni applicazione è assegnata a un gruppo particolare. Per esempio FaxMail, utility per l'invio di fax, si trova nel gruppo Applicazioni/Comunicazioni e Icecast, sistema di diffusione su Internet di MP3, si trova nel gruppo Applicazioni/Multimedia. Effettuando una selezione dei nomi di gruppo, potete evitare di dovere leggere la descrizione di ogni pacchetto.
- *Effettuate una ricerca con parole chiave* — Il comando `ls` permette di effettuare una ricerca semplificata. Se state cercando un client IRC, digitate `less CONTENTS` per visualizzare `CONTENTS`, poi digitate **`/IRC`** e premete [Invio]. Comparirà il primo client IRC dell'elenco. Se non vi interessa, premete il tasto [n] ripetutamente finché non trovate il pacchetto che vi interessa.

Se avete problemi con il comando `less` command, digitate `man less` al prompt per visualizzare l'help.

Smontaggio del CD-ROM di PowerTools

Una volta che avete finito di usare il CD-ROM di PowerTools per installare i pacchetti, rimuovetelo dall'unità. Se il CD-ROM è montato nella directory `/mnt/cdrom` fate quanto segue:

1. Cambiate directory usando il comando `cd /mnt` fino a trovarvi un livello sopra la directory `/mnt/cdrom`.
2. Smontate il CD-ROM digitando il comando `umount /mnt/cdrom`.
3. Digitate `eject /dev/cdrom` per aprire l'unità e rimuovere il CD.

E.3 Installazione dei pacchetti PowerTools

E.3.1 Installazione di PowerTools in ambiente grafico

Se state utilizzando l'interfaccia grafica GNOME o KDE, inserite il CD nel vostro lettore CD-ROM. Vi viene richiesta la password di root per poter installare i nuovi pacchetti. Dopo aver digitato la password di root, viene eseguito automaticamente il programma Gnome-RPM o Kpackage, in base all'ambiente grafico che utilizzate.

Per maggiori informazioni sull'utilizzo di Gnome-RPM, consultate la *Official Red Hat Linux Getting Started Guide*. Per maggiori informazioni sull'utilizzo di Kpackage, collegatevi all'indirizzo http://www.general.uwa.edu.au/u/toivo/kpackage.

Se non utilizzate né GNOME né KDE, Powertools deve essere installato dal prompt della shell.

E.3.2 Installazione di PowerTools dal prompt della shell

Per prima cosa montate il CD di PowerTools nell'apposita unità e digitate il comando `ls` per visualizzarne il contenuto. Se non sapete come montare un CD-ROM, consultate il *Montaggio del CD-ROM di PowerTools* nella sezione E.2.1.

Compariranno le seguenti directory: `SRPMS` e `RedHat`. La directory `SRPMS` contiene gli RPM sorgenti di PowerTools. La directory - `RedHat/RPMS` contiene gli RPM per le tre architetture di sistema specificate.

La directory `RedHat/RPMS` viene utilizzata come esempio generale. Potete sostituire la directory corretta in funzione dell'architettura e del pacchetto che state installando.

Con il comando `cd` andate alla directory `RedHat/RPMS`:

```
cd RedHat/RPMS
```

Per visualizzare i file RPM presenti nella directory compatibili con i sistemi Intel, digitate il comando `ls`.

Probabilmente vi servono maggiori informazioni su un pacchetto prima di decidere se lo volete installare. Le opzioni di interrogazione di RPM vi permettono di ricevere maggiori dettagli sui pacchetti, come le loro funzioni e origini. Consultate la *Official Red Hat Linux Customization Guide* per ottenere maggiori istruzioni su come interrogare i pacchetti usando l'applicazione RPM.

Altrimenti, potete trovare i pacchetti che vi interessano facendo scorrere il file `CONTENTS`. Consultate la *Lettura del file `CONTENTS`* nella sezione E.2.1 per maggiori informazioni sulla procedura da seguire.

I pacchetti selezionati con RPM possono essere installati. Il programma RPM è un potente gestore di pacchetti utilizzabile direttamente dalla linea di comando della shell. Consultate la *Official Red Hat Linux Customization Guide* per ottenere maggiori informazioni su come usare RPM e per installare e gestire i pacchetti PowerTools.

Terminata l'installazione dei pacchetti, dovete smontare il CD-ROM. Se non sapete come fare, consultate *Smontaggio del CD-ROM di PowerTools* nella sezione E.2.1.

E.4 Rimozione dell'installazione di PowerTools

Per rimuovere l'installazione dei pacchetti di PowerTools dal vostro sistema, seguite la procedura per la rimozione dei pacchetti RPM.

Innanzitutto, dovete conoscere il nome del pacchetto che volete rimuovere. Per esempio se volte eliminare `thrust-0.83c-11` dal vostro sistema, digitate come root:

```
rpm -e thrust
```

In generale, il comando `rpm -e <nomepacchetto>` rimuove il pacchetto e i relativi file dal sistema. Il CD-ROM di PowerTools non è richiesto per quest'operazione.

Per maggiori informazioni sull'utilizzo di RPM, consultate la *Official Red Hat Linux Customization Guide*.

Indice analitico

A

`AccessConfig`
direttiva di configurazione di Apache .. 180
`AccessFileName`
direttiva di configurazione di Apache .. 187
accessi
controllo 149
accesso alla console
attivazione 153
configurazione..... 150, 152
disattivazione..... 151
disattivazione totale..... 152
`Action`
direttiva di configurazione di Apache .. 194
`AddDescription`
direttiva di configurazione di Apache .. 192
`AddEncoding`
direttiva di configurazione di Apache .. 193
`AddHandler`
direttiva di configurazione di Apache .. 194
`AddIcon`
direttiva di configurazione di Apache .. 192
`AddIconByEncoding`
direttiva di configurazione di Apache .. 192
`AddIconByType`
direttiva di configurazione di Apache .. 192
`AddLanguage`
direttiva di configurazione di Apache .. 193
`AddModule`
direttiva di configurazione di Apache .. 182
`AddType`
direttiva di configurazione di Apache .. 193
aggiornamento
Apache..... 164
vecchi file di configurazione 165
del server sicuro 1.0 o 2.0 167
per installare il server sicuro 162
server sicuro
nuova `DocumentRoot`..... 164
`Alias`
direttiva di configurazione di Apache .. 190
`Allow`
direttiva di configurazione di Apache .. 186
`AllowOverride`
direttiva di configurazione di Apache .. 186
Apache
aggiornamento da una versione precedente..... 164
avvio 177
chiusura..... 177
configurazione..... 178
lavorare in modalità non sicura 202
report sullo stato del server..... 196
riavvio..... 177
ricompilazione..... 201
sicurezza 165
APXS 158
APXS, utility di Apache..... 200
autenticazione
Kerberos 113
avvio
Apache..... 177
modalità a utente singolo..... 43
server sicuro 177

B

`BindAddress`
direttiva di configurazione di Apache .. 182
BIOS, argomenti riguardanti LILO..... 245
`/boot` partizione
(Vedi partizione, `/boot`)
`BrowserMatch`
direttiva di configurazione di Apache .. 195

C

CA
(Vedi autorità di certificazione)

CacheNegotiatedDocs
direttiva di configurazione di Apache .. 187
CCVS
assistenza 84
avvio 83
avvio del demone ccvsd 83
caratteristiche 72
configurazione 77
conto commerciante 74
conto commerciante multiplo 82
cvupload 83
elaborazione batch 83
installazione 76
linee guida 75
linguaggi di programmazione 84
modem 73
panoramica 71
prima della configurazione 76
requisiti 73
risorse addizionali
siti Web utili 85
risorse aggiuntive 84
documentazione installata 85
uso internazionale 71
utilizzi 71
ccvsd 83
CD-ROM
montaggio 255
parametri 210
smontaggio 256
certificato
autorità
scelta 168
installazione 173
pre-esistente 166
richiesta 170
formulazione 170
self-signed 172
spostarlo dopo un aggiornamento 167
test, signed e self-signed 167
verifica 173
chiusura 57
Apache 177
server sicuro 177
chkconfig 57
ClearModuleList
direttiva di configurazione di Apache .. 182
configurazione
accesso alla console 150
Apache 178
host virtuali 202
server sicuro 177
SSL 199
console
rendere i file accessibili dalla 152
[Ctrl]-[Alt]-[Canc]
shutdown, disattivazione 151
CustomLog
direttiva di configurazione di Apache .. 189

D

DefaultIcon
direttiva di configurazione di Apache .. 192
DefaultType
direttiva di configurazione di Apache .. 188
Deny
direttiva di configurazione di Apache .. 186
/dev directory 22
devel package 158
directory
/dev 22
/etc 22
/lib 22
/mnt 23
/opt 23
/proc 26
/sbin 23
/usr 24
/usr/local 24, 26
/var 25
Directory

direttiva di configurazione di Apache .. 184
directory /etc 22
directory public_html 186
directory /lib 22
directory /mnt 23
directory /opt 23
directory /proc 26
directory /sbin 23
directory /usr 24
directory /usr/local 24, 26
directory /var 25
DirectoryIndex
direttiva di configurazione di Apache .. 187
direttive della cache per Apache 197
direttive di configurazione, Apache 179
AccessConfig 180
AccessFileName 187
Action 194
AddDescription 192
AddEncoding 193
AddHandler 194
AddIcon 192
AddIconByEncoding 192
AddIconByType 192
AddLanguage 193
AddModule 182
AddType 193
Alias 190
Allow 186
AllowOverride 186
BindAddress 182
BrowserMatch 195
CacheNegotiatedDocs 187
ClearModuleList 182
CustomLog 189
DefaultIcon 192
DefaultType 188
Deny 186
Directory 184
DirectoryIndex 187
DocumentRoot 184
ErrorDocument 195
ErrorLog 189
ExtendedStatus 183
Group 183
HeaderName 193
HostnameLookups 188
IfDefine 182
IfModule 188
IndexIgnore 193
IndexOptions 191
KeepAlive 180
KeepAliveTimeout 181
LanguagePriority 193
Listen 181
LoadModule 182
Location 195
LockFile 179
LogFormat 189
LogLevel 189
MaxClients 181
MaxKeepAliveRequests 180
MaxRequestsPerChild 181
MaxSpareServers 181
MetaDir 194
MetaSuffix 194
MinSpareServers 181
NameVirtualHost 198
Options 185
Order 186
per la funzionalità della cache 197
per la funzionalità SSL 199
PidFile 179
Port 183
ProxyRequests 197
ProxyVia 197
ReadmeName 193
Redirect 191
ResourceConfig 180
ScoreBoardFile 180
ScriptAlias 191
ServerAdmin 184

ServerName 184
ServerRoot 179
ServerSignature 190
ServerType 179
SetEnvIf 199
StartServers 181
Timeout 180
TypesConfig 187
UseCanonicalName 187
User 183
UserDir 186
VirtualHost 198
direttive SSL 199
dischetto
driver 247
dischetto dei driver 247
creazione da un'immagine 248
prodotto da altre società 247
prodotto da Red Hat 247
utilizzo 248
disco fisso
concetti di base 225
introduzione alle partizioni 229
partizionamento 225
partizioni estese 233
tipi di filesystem 226
tipi di partizione 231
DocumentRoot 164
direttiva di configurazione di Apache .. 184
modifica 202
modifica della condivisione 203
DSO
caricamento 158, 199

E

ErrorDocument
direttiva di configurazione di Apache .. 195
ErrorLog
direttiva di configurazione di Apache .. 189
/etc/lilo.conf, impostazioni 36
/etc/pam.conf 105
/etc/pam.d 105
/etc/sysconfig
amd 44
apmd 44
authconfig 44
cipe 45
clock 45
desktop 46
firewall 46
harddisks 46
hwconf 47
init 47
irda 48
keyboard 49
kudzu 49
mouse 49
network 50
pcmcia 51
rawdevices 51
sendmail 51
soundcard 52
ups 52
vncservers 53
/etc/sysconfig, file in 43
Ethernet
parametri 217
supporto di schede multiple 224
ExtendedStatus
direttiva di configurazione di Apache .. 183

F

FHS 21–22
file di log 179
agent 190
combinati 190
formato comune del file di log 189
referer 190
filesystem
formati, panoramica sui 226

gerarchia 21
organizzazione 22
standard 22
struttura
libri 21
formato comune del file di log 189
FrontPage 177

G

gerarchia, filesystem 21
`Group`
direttiva di configurazione di Apache .. 183
gruppi 29
privati utente 31
logica 33
privati utenti 29
standard 30
gruppi privati utente 31
logica 33
gruppi utenti privati 29
gruppo
floppy, utilizzo 154
gruppo floppy, utilizzo 154

H

halt 57
`HeaderName`
direttiva di configurazione di Apache .. 193
host virtuali
basati sul nome 202
configurazione 202
include del server 185, 193
`Listen` command 205
`Options` 185
`HostnameLookups`
direttiva di configurazione di Apache .. 188
HTTP PUT 195
`httpd.conf`
(Vedi direttive di configurazione, Apache)

I

`IfDefine`
direttiva di configurazione di Apache .. 182
`IfModule`
direttiva di configurazione di Apache .. 188
include del server 185, 193
host virtuali 185
`IndexIgnore`
direttiva di configurazione di Apache .. 193
`IndexOptions`
direttiva di configurazione di Apache .. 191
init 38
init, SysV 42
installazione
server sicuro 157
dopo l'installazione di Red Hat Linux 163
durante un aggiornamento di Red Hat Linux 162
server Web sicuro
durante l'installazione di Red Hat Linux 161

K

`KeepAlive`
direttiva di configurazione di Apache .. 180
`KeepAliveTimeout`
direttiva di configurazione di Apache .. 181
Kerberos 113
come funziona 115
configurazione del server 116
configurazione di un client 119
e PAM 120
perché non usarlo 113
perché usarlo 113
risorse aggiuntive 120
documentazione installata 120
siti Web utili 120
terminologia 114
kernel 209

driver 209

L

LanguagePriority
direttiva di configurazione di Apache .. 193
LDAP
aggiornamento 62
antaggi e svantaggi 59
applicazioni 60
demoni e utility 64
file 62
directory schema 63
slapd.conf 62
Moduli per aggiungere funzioni 65
risorse aggiuntive 69
documentazione installata 69
libri correlati 70
siti Web utili 69
spiegazione 59
terminologia 61
uso di 60
utilizzo con PAM 60
utilizzo dell'autenticazione 66
LILO
argomenti relativi al partizionamento .. 245
argomenti riguardanti il BIOS 245
Listen
direttiva di configurazione di Apache .. 181
LoadModule
direttiva di configurazione di Apache .. 182
Location
direttiva di configurazione di Apache .. 195
LockFile
direttiva di configurazione Apache 179
LogFormat
direttiva di configurazione di Apache .. 189
LogLevel
direttiva di configurazione di Apache .. 189

M

MaxClients
direttiva di configurazione di Apache .. 181
MaxKeepAliveRequests
direttiva di configurazione di Apache .. 180
MaxRequestsPerChild
direttiva di configurazione di Apache .. 181
MaxSpareServers
direttiva di configurazione di Apache .. 181
MetaDir
direttiva di configurazione di Apache .. 194
MetaSuffix
direttiva di configurazione di Apache .. 194
MinSpareServers
direttiva di configurazione di Apache .. 181
mod_ssl
fornito come DSO 201
moduli
Apache
caricamento 199
personali 200
Moduli di autenticazione
(Vedi PAM)
montaggio
CD-ROM drive 255
mount point
partizioni e 244
mtools e il gruppo floppy 154

N

NameVirtualHost
direttiva di configurazione di Apache .. 198
Netscape Navigator
caratteristica di pubblicazione 195
ntsysv 57
numero di porte 174

O

oggetti, dinamicamente condivisi

(Vedi DSO)
OpenLDAP 59
OpenSSH 139
file di configurazione 144
`Options`
direttiva di configurazione di Apache .. 185
`Order`
direttiva di configurazione di Apache .. 186
OS/2 243

P

pacchetti
server sicuro
scelta per l'installazione 158
PAM 105
accesso via `rexec` 111
accesso via `rlogin` 111
accesso via `rsh` 111
argomenti 108
e Kerberos 120
esempi 109
file di configurazione 105
moduli 106
nomi di servizio 106
opzioni 107
percorsi dei moduli 108
risorse aggiuntive 112
documentazione installata 112
siti Web utili 112
vantaggi 105
parametri
moduli 209
moduli CD-ROM 210
moduli Ethernet 217
parametri dei moduli 209
specificare 210
partizionamento
altri sistemi operativi 243
argomenti LILO relativi al 245
attribuzione di un nome alle partizioni . 242
concetti di base 225
creazione di spazio per le partizioni 234
distruttivo 236
introduzione al 229
mount point e 244
non-distruttivo 238
numerazione delle partizioni 242
partizioni estese 233
quante partizioni 244
tipi di partizione 231
utilizzo dello spazio libero 235
utilizzo di una partizione in uso 236
utilizzo di una partizione non utilizzata 236
partizione
`/boot` 244
estesa 233
root 245
swap 244
partizione di root
(Vedi partizione, root)
partizione swap
(Vedi partizione, swap)
partizioni estese 233
password
shadow 111
`PidFile`
direttiva di configurazione di Apache .. 179
`Port`
direttiva di configurazione di Apache .. 183
posizioni dei file di Red Hat Linux 27
PowerTools 255
installazione
GNOME o KDE 257
in un ambiente grafico 257
prompt della shell 257
leggere il file `CONTENTS` 255
pacchetti 255
rimozione dell'installazione 258
privilegi
controllo 149

processo di avvio..... 35
init..... 38
x86 35
programmi
esecuzione all'avvio 57
ProxyRequests
direttiva di configurazione di Apache .. 197
ProxyVia
direttiva di configurazione di Apache .. 197

R

RAID..... 251
livelli 252
livello 0 252
livello 1 252
livello 4 252
livello 5 252
RAID hardware 251
RAID software 251
spiegazione 251
vantaggi..... 251
RAID hardware
(Vedi RAID)
RAID software
(Vedi RAID)
rc.local
modica 57
ReadmeName
direttiva di configurazione di Apache .. 193
Redirect
direttiva di configurazione di Apache .. 191
ResourceConfig
direttiva di configurazione di Apache .. 180
rexec
con PAM..... 111
rimozione dell'installazione
PowerTools 258
risoluzione di problemi
dopo la modifica di httpd.conf..... 179
rlogin
con PAM..... 111
rsh
con PAM..... 111
runlevel 56

S

scelta di una CA..... 168
ScoreBoardFile
direttive di configurazione Apache 180
script CGI
esecuzione di programmi esterni a cgi-bin..... 185
fuori dalla direttiva ScriptAlias ... 194
ScriptAlias
direttiva di configurazione di Apache .. 191
SCSI 209
security 97
Sendmail..... 87
alias 89
con IMAP..... 89
con UUCP 89
e LDAP 91
installazione predefinita 88
introduzione 87
mascheramento..... 90
modifiche della configurazione 89
risorse aggiuntive 92
documentazione installata 92
libri correlati..... 93
siti Web utili 93
spam..... 90
server proxy 197
server sicuro
accesso..... 174
avvio 177
chiave
creazione..... 168
chiusura..... 177
configurazione..... 177

connessione....174
documentazione
installata....175
installazione....157
con RPM....164
libri....176
ottenimento di un certificato....165
problemi durante l'installazione....175
riavvio....177
siti Web....175
spiegazione sulla sicurezza....165
trovare aiuto....175
URL....174
server Web non sicuro
disabilitare....203
`ServerAdmin`
direttiva di configurazione di Apache..184
`ServerName`
direttiva di configurazione di Apache..184
`ServerRoot`
direttiva di configurazione di Apache..179
`ServerSignature`
direttiva di configurazione di Apache..190
`ServerType`
direttiva di configurazione di Apache..179
servizi
sistema
avvio con `chkconfig`.... 57
avvio con `ntsysv`.... 57
`SetEnvIf`
direttiva di configurazione di Apache..199
sever sicuro
ringraziamenti....158
shadow
password....111
utility....149
shutdown
disattivazione[Ctrl]-[Alt]-[Canc] 151
sicurezza
approcci.... 98
configurare....199
dilemma.... 97
eseguire Apache senza....202
Kerberos....113
password....101
politiche....100
rete....102
risorse aggiuntive....103
libri correlati....104
siti Web utili....104
spiegazione....165
ulteriori azioni....101
sistema
chiusura.... 57
smontaggio
unità CD-ROM....256
SSH....139
connessioni remote....147
file di configurazione....144
introduzione.... 139–140
livelli....142
perché usarlo....140
protocollo.... 139, 142
autenticazione....143
connessione....143
livello di trasporto....142
sessioni X11....145
TCP/IP forwarding.... 145–146
X11 forwarding....145
standard
gruppi.... 30
utenti.... 29
`StartServers`
direttiva di configurazione di Apache..181
striping
Fondamenti del RAID....251
struttura
comune.... 21
struttura, filesystem.... 21
SysV init.... 42
directory utilizzate da.... 42
runlevel utilizzati da.... 56

T

Timeout
  direttiva di configurazione di Apache .. 180
Tripwire 123
  chiavi
    scelta 129
  componenti 128
  configurazione di 126
  controllo dell'integrità
    eseguire 130
  database
    aggiornamento 133
    inizializzazione 130
  file di configurazione
    firma 135
  file di policy
    aggiornamento 134
    modifica 129
  funzioni di e-mail 135
    prova 136
  installazione di 125
  installazione di RPM 126
  posizione dei file 128
  risorse aggiuntive 136
    documentazione installata 136
    siti Web utili 137
  twprint e il database 132
  uso di 123
  visualizzazione dei report 131
troubleshooting
  log degli errori 189
TypesConfig
  direttiva di configurazione di Apache .. 187

U

URL
  per il server sicuro 174
UseCanonicalName
  direttiva di configurazione di Apache .. 187
User
  direttiva di configurazione di Apache .. 183
UserDir
  direttiva di configurazione di Apache .. 186
utenti 29
  directory HTML personali 186
  standard 29
utility
  shadow 149
utility di initscript 57
utility di partizionamento fips 241

V

verifica dei certificati 173
VeriSign
  utilizzo di un certificato esistente 166
VirtualHost
  Direttiva di configurazione di Apache .. 198

W

webmaster
  indirizzo e-mail per 184