

Linux Administration Made Easy

di Steve Frampton, <frampton@LinuxNinja.com>

Linux Administration Made Easy

di Steve Frampton, <frampton@LinuxNinja.com>

Pubblicato 21 Ottobre 1999

La guida “Linux Administration Made Easy” (LAME) ha come scopo quello di descrivere le operazioni quotidiane di amministrazione e manutenzione comunemente affrontate dagli amministratori di sistema Linux. È parte integrante del Linux Documentation Project. Traduzione a cura di Emiliano Cocco, <emcocco@sunstone.it> e revisione a cura di Marcello Seri.

Sommario

1. Prefazione	1
1.1. Riconoscimenti	1
1.2. Informazioni sul Copyright e note legali.....	1
1.3. Richiesta d'aiuto.....	1
2. Introduzione	2
2.1. Scopi.....	2
2.2. Scegliere una distribuzione Linux	2
3. In generale su Linux	5
3.1. Che cos'è Linux?.....	5
3.2. Sfatiamo i miti	5
3.3. Prospettive per un uso mono-utente	6
4. Installazione e configurazione hardware	8
4.1. Creare un dischetto d'installazione	8
4.2. Avviare il programma di installazione di Linux.....	8
4.3. Partizionamento dei dischi fissi	10
4.4. Impostare lo spazio di Swap.....	14
4.5. Scegliere le partizioni da formattare	14
4.6. Scegliere i pacchetti da installare	14
4.7. Installazione e configurazione Hardware	15
4.8. Boot con LILO	15
4.9. Scaricare e installare gli aggiornamenti di Red Hat.....	16
5. Configurare il sistema X Window.....	18
5.1. Far funzionare X Window con X-Configurator.....	18
5.2. Usare l'X Desktop Manager.....	19
5.3. Migliorare l'aspetto dei font sotto X	20
5.4. Scegliere un Window Manager per X	20
5.5. Installazione e configurazione di GNOME	21
5.6. Installazione e configurazione di KDE.....	21
6. Operazioni generali per l'amministrazione di sistema.....	23
6.1. Account di Root	23
6.2. Creare gli Account degli utenti	23
6.3. Cambiare le password degli utenti	25
6.4. Disabilitare gli account degli utenti.....	25
6.5. Rimuovere gli account degli utenti.....	25
6.6. Le password di Linux e il formato shadow	26
6.7. Spegnimento e riavvio del sistema.....	27
7. Questioni di amministrazione e configurazioni personalizzata	29
7.1. Amministrazioni di un web server e di un HTTP caching proxy.....	29
7.2. Configurazione e amministrazione di un Domain Name Server (DNS)	30
7.3. Autenticazione degli utenti internet con TACACS.....	34
7.4. Servizi file e stampa in stile Windows con Samba.....	35
7.5. Servizi file e di stampa in stile Macintosh con Netatalk	39
7.6. Servizi Network File System (NFS).....	41

7.7. Configurazione dalla A alla Z con Linuxconf	41
8. Procedure di backup e restore	43
8.1. Procedure per il backup dei server	43
8.2. Procedure per il restore dei dati del server	47
8.3. Backup della configurazione di un router Cisco	49
9. Compiti di amministrazione vari ed eventuali	51
9.1. Controllare lo spazio destinato alla memorizzazione dei dati	51
9.2. Gestire i processi	52
9.3. Avviare e fermare i processi	53
9.4. Automatizzare i compiti con cron e i file crontab	54
10. Aggiornare Linux e altre applicazioni	56
10.1. Usare il Red Hat Package Manager (RPM).....	56
10.2. Installare o aggiornare senza RPM.....	57
10.3. Strategie per mantenere un sistema aggiornato.....	58
10.4. Aggiornamenti del kernel Linux	59
10.5. Aggiornare il kernel fornito da Red Hat.....	59
10.6. Costruire un kernel personalizzato	60
10.7. Passare ai kernel Linux 2.2.x.....	63
10.8. Configurare il web server Apache	65
10.9. Configurare il demone Squid HTTP caching proxy.....	66
10.10. Configurare il demone per le e-mail Sendmail.....	66
11. Linux in azienda.....	69
11.1. Messa a punto delle prestazioni	69
11.2. Alta disponibilità con RAID	69
11.3. Migrazione di Server e questioni di scalabilità	70
12. Strategie per mantenere un server sicuro.....	73
13. Aiuto! Il paradiso mi annoia!.....	76
13.1. Installare Linux su hardware non supportato	76
13.2. File System corrotto dopo un crash di sistema o un'interruzione di corrente elettrica.....	76
13.3. A chi rivolgersi per chiedere aiuto	76
13.4. Riferimenti ad altra documentazione	79

Capitolo 1. Prefazione

1.1. Riconoscimenti

Vorrei ringraziare tutta la comunità Linux e, in particolare, coloro che hanno fornito preziosi consigli attraverso newsgroup e mailing-list. Questa documentazione è stata scritta in formato DocBook SGML e poi convertita in vari formati, come l'HTML, postscript, RTF e PDF. Per maggiori informazioni sugli SGMLTools consultate il sito <http://www.sgmltools.org/>.

1.2. Informazioni sul Copyright e note legali

Copyright © 1997-1999 by Steve Frampton. This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, v0.4 or later (the latest version is presently available at <http://www.opencontent.org/openpub/>).

Copyright © 1997-1999 by Steve Frampton. Questo materiale può essere distribuito soltanto nel rispetto dei termini e delle condizioni previsti nella Open Publication License, versione 0.4 e successive (l'ultima versione è disponibile su <http://www.opencontent.org/openpub/>).

Ho scritto questo testo e ho provveduto a fornirlo alla comunità Linux in maniera del tutto gratuita. Ho cercato di fare in modo che le informazioni contenute potessero essere il più possibile precise ed accurate, ma non mi riterrò responsabile in alcun modo di eventuali danni, diretti o indiretti, derivanti dalle informazioni qui descritte.

Accetterò volentieri qualunque comunicazione di eventuali errori e suggerimenti per sviluppi futuri. Controllate, comunque, sempre il numero di versione del testo, per assicurarvi di avere quello più recente. Controllate sul sito <http://metalab.unc.edu/LDP/> se è previsto il rilascio di nuove versioni.

Questo documento è da considerarsi come versione beta. Ho iniziato a scriverlo nel 1997 e continuo ad aggiornarlo nei ritagli di tempo, anche se è davvero una sfida perché lo sviluppo dell'Open Source procede sempre più velocemente. Quindi, nonostante i miei sforzi, questo libro potrebbe contenere informazioni obsolete.

In breve, non garantisco che le informazioni qui riportate siano corrette. Spero comunque che vi sia d'aiuto!

1.3. Richiesta d'aiuto

Se trovate che questa guida vi sia d'aiuto e volete esprimere il vostro apprezzamento per essa, vi prego di considerare la possibilità di fare una donazione alla banca del cibo.

Capitolo 2. Introduzione

Linux 2.2.0, released 25-Jan-99: Onwards to World Domination...

Forse vi state avvicinando per la prima volta a Linux e sperate di trovare un riassunto di tutti i compiti di configurazione e amministrazione che potrebbero esservi richiesti. Se tutto ciò è vero, allora questa guida potrebbe essere quello che state cercando

2.1. Scopi

Questa documentazione tenterà di riassumere le procedure d'installazione e di configurazione, nonché quelle di amministrazione e manutenzione, che dovrebbero essere eseguite per mantenere un server o un pc Linux completamente funzionanti. È rivolto sia agli utenti casalinghi e sia a quelli che ci lavorano. Tratterà solo gli argomenti generali, dato che ci sono molti testi, disponibili anche on-line, a cui fare riferimento nel caso si dovesse aver bisogno di informazioni più dettagliate.

Diciamo che, in generale, il vostro sistema Linux può funzionare tranquillamente anche con un minimo di manutenzione. I compiti di routine, come l'avvicendamento e l'eliminazione dei log di sistema, vengono svolti in automatico. Quindi, anche con interventi minimi da parte dell'utente, Linux continuerà a svolgere il suo lavoro. Questo documento potrebbe risultare utile, invece, nel caso di modifiche personali o di collasso del sistema.

Attualmente uso Linux sia a casa e sia sul lavoro. Mi è sempre stato utile e lavora egregiamente per i servizi Internet, e di condivisione di file e stampante, dei miei impiegati da ormai quattro anni.

2.2. Scegliere una distribuzione Linux

Esiste una grande varietà di distribuzioni Linux tra cui è possibile scegliere. Ogni distribuzione fornisce il kernel Linux e alcuni strumenti di sistema, ma differisce dalle altre per le modalità d'installazione e per le applicazioni incluse. Ogni distribuzione presenta i propri vantaggi e svantaggi. Vi illustrerò, quindi, brevemente le caratteristiche di ognuna di esse per aiutarvi nella scelta.

Di seguito vi propongo una lista di siti web che potete visitare, ognuno dei quali descrive una diversa distribuzione Linux, comprensivo d'informazioni sul download e sulla modalità d'acquisto.

<http://www.redhat.com/>

La distribuzione Red-Hat, della Red Hat Software, Inc. è una delle più popolari. È possibile installare facilmente Linux sia attraverso una interfaccia grafica, sia attraverso un'interfaccia testuale. Permette la gestione dei pacchetti con l'utilità "RPM", e include sia *GNOME* sia *KDE* come interfaccia grafica per il sistema X Window. La distribuzione è disponibile per piattaforme Intel, Alpha e Sparc.

<http://www.debian.org/>

La distribuzione Debian, di una organizzazione non-profit conosciuta come "Il progetto Debian", è quella prediletta dalla comunità Open Source. Fornisce l'utilità "dpkg" per gestire pacchetti e per effettuare aggiornamenti. È disponibile per piattaforme Intel, Alpha, Sparc e Motorola (Macintosh, Amiga, Atari).

<http://www.suse.com/>

La distribuzione S.u.S.E., venduta da S.u.S.E., è anch'essa popolare ed è la più utilizzata in Europa. Comprende *KDE* e l'utilità "YAST2" per una facile gestione dei pacchetti e degli aggiornamenti. È disponibile per piattaforme Intel e Alpha.

<http://www.linux-mandrake.com/>

La distribuzione Mandrake, venduta dalla MandrakeSoft S.A., integra le distribuzioni Red Hat o Debian (a voi la scelta) con pacchetti software non inclusi nelle distribuzioni originali. Comprende l'utilità "DrakConf" e una serie di strumenti che permettono una facile gestione e configurazione del sistema, tra cui la pratica estensione del programma rpm "urpm*". È considerata una delle più semplici distribuzioni del momento, adatta anche a sistemi Desktop.

<http://www.slackware.com/>

La distribuzione Slackware, di Patrick Volkerding della Walnut Creek Software, è l'antenato delle moderne distribuzioni Linux. Offre una procedura d'installazione abbastanza semplice, ma povera dal punto di vista della gestione dei pacchetti e degli aggiornamenti. Raccomandata agli utenti più preparati dal punto di vista tecnico e che hanno già familiarizzato con Linux. È disponibile solo per piattaforma Intel.

Fornire una lista di tutte le distribuzioni disponibile va oltre gli scopi di questo documento, quindi ho incluso solo quelle più popolari. Tuttavia, ulteriori informazioni sulle distribuzioni disponibili possono essere reperite nella guida "*English-language GNU/Linux distributions on CD-ROM*", disponibile su http://www.startex.co.uk/msw/CD_Distributions_EN/index.html. [NdT: disponibile in italiano su <http://it.tldp.org/HOWTO/CD-Distributions-EN-HOWTO/index.html>]

Suggerimento: Suggerimento: Se decidete di acquistare la vostra distribuzione su CD-ROM, potreste trovare prezzi migliori da altri rivenditori (per esempio, sono rimasto abbastanza soddisfatto dal rivenditore di software <http://www.cheapbytes.com/>). Dall'altro lato, potreste volere pagare un prezzo più alto ai venditori delle distribuzioni per assicurarvi che la loro offerta continui a migliorare.

Personalmente ho scelto la distribuzione Red Hat (che sembra essere, indiscutibilmente, quella più popolare tra gli utenti Linux). Per quasi tre anni, sono stato un grande fanatico di Slackware (prima di essa, mi sono incasinato un po' con una piccola distribuzione tsx-11 nei giorni del kernel 0.90a), e sebbene avessi provato Red Hat in passato, non riuscivo a trovare niente di buono nella loro distribuzione. Poi, ho provato la Red Hat 5.1, e mi sono convertito immediatamente. Secondo me, con la 5.1, Red Hat ha finalmente "capito cosa fare".

Alcune delle ragioni che mi hanno spinto verso la distribuzione di Red Hat sono da ricercare nella facilità d'installazione, supporto multi-piattaforma (fino a poco tempo fa, Red Hat era l'unica a fornire la propria distribuzione per piattaforma Intel, Alpha e Solaris.), e, soprattutto, l'utilità di gestione dei pacchetti RPM. In più, mettono gli aggiornamenti in RPM sul loro sito FTP (su <ftp://ftp.redhat.com/redhat/updates/>) appena sono disponibili, il che rappresenta un buon modo di mantenere il proprio sistema funzionante e senza i bug, o problemi di sicurezza, che vengono scoperti di tanto in tanto.

Dal primo caricamento di Red Hat 5.1 su computer non utilizzati sul lavoro (per effettuare dei test), ho sostituito Slackware con Red Hat su due dei nostri server Internet/File & Print principali, e non mi sono mai pentito. L'ho caricato anche sul mio sistema a casa, e l'ho installato pure su altri tre sistemi come light server. In più, ho avuto la possibilità non solo di usare la versione Intel ma anche quelle per Alpha e Sparc. Ultimamente ho messo Red Hat 6.1 su tutti i sistemi di cui sono responsabile.

Quindi, questo documento si riferisce principalmente a Red Hat e, soprattutto, alla versione 6.1 per Intel. Comunque, credo che la maggior parte delle informazioni contenute possano essere utilizzate anche su altre distribuzioni.

Capitolo 3. In generale su Linux

Benvenuti su Linux!

3.1. Che cos'è Linux?

Linux è un sistema operativo a 32 bit che funziona su diverse piattaforme, incluse Intel, Sparc, Alpha e Power Pc (su alcune di queste piattaforme, Linux è a 64-bit). Esistono versioni anche per altre piattaforme, ma non le conosco nello specifico.

Linux fu sviluppato per la prima volta agli inizi degli anni '90 da Linus Torvalds, un giovane studente universitario. Linus aveva a casa un 386 e decise di scrivere un sistema alternativo al Minix basato su 286 (una piccola implementazione simile a unix), per sfruttare il nuovo set d'istruzioni del nuovo chip. Iniziò così a scrivere un piccolo kernel.

Comunicò il suo progetto sul gruppo di discussione comp.os.minix (news:comp.os.minix), chiedendo se qualcuno fosse interessato a partecipare. Il risultato fu fenomenale!

La cosa interessante è che Linux è completamente gratuito. Linus decise di adottare la licenza GNU della Free Software Foundation, che significa che il codice è protetto da un copyright cioè quello di essere sempre disponibile per tutti.

free significa che puoi: averlo liberamente, usarlo liberamente, e sei addirittura libero di venderlo per ricavare un profitto (non è poi così strano come potrebbe sembrare; alcune organizzazioni, inclusa la Red Hat, hanno realizzato pacchetti contenenti, oltre al kernel Linux e una collezione di utilità GNU, anche applicazioni "personalizzate", vendendoli poi come distribuzioni. Le distribuzioni più comuni sono Slackware, Red Hat, Suse e Debian). La grande cosa è che puoi accedere al codice sorgente, con la possibilità, quindi, di personalizzare il sistema operativo secondo le *tue* esigenze. Al contrario di "altri" sistemi operativi commerciali.

Linux può essere considerato a tutti gli effetti un'implementazione di Unix, soltanto che non può essere chiamato in questo modo; non per questioni di incompatibilità, ma solo per il fatto che la parola "Unix" è un marchio di fabbrica della AT&T, ed è consentito l'uso di tale termine solo con il rilascio della licenza.

Linux è affidabile così come qualunque altro sistema operativo (secondo me un po' più degli altri). Comunque, forse per le sue origini, oppure per tutta la filosofia che c'è dietro, si sono creati diversi miti su di esso.

3.2. Sfatiamo i miti

Uso Linux da un po' di anni e mi piace pensare che un po' lo conosco e che, quindi, so cosa può e cosa non può fare. Dato che mi piace molto leggere USENET, seguo gli ultimi sviluppi e naturalmente tutte le "guerre" che si scatenano inevitabilmente. Ho constatato che esistono diversi miti in cui credono molte persone; permettetemi di presentarvene qualcuno.

- Linux è gratis, perciò è un giocattolo.

Alcuni sembrano credere che, soltanto perché un software è stato scritto da volontari senza scopo di lucro, allora il prodotto che ne risulta deve per forza essere inferiore a quelli commerciali.

Forse poteva essere vero in passato (mi riferisco all'enorme quantità di software spazzatura per DOS e Windows), ma non certamente di questi tempi.

Internet dà la possibilità di unire tutti le migliori menti del pianeta, permettendo loro di collaborare a quei progetti che ritengono interessanti. Le persone che hanno contribuito allo sviluppo di Linux e delle centinaia di utilità e applicazioni GNU, hanno tutte un diverso background e hanno contribuito alla loro realizzazioni spinti dalle ragioni più diverse.

Qualcuno si è impegnato nello sviluppo solo per amore della programmazione, altri l'hanno fatto per particolari esigenze (come quello di poter monitorare il traffico di una Lan). Altri sono scienziati che stanno usando Linux per le loro ricerche.

Diversamente dalle offerte commerciali, dove i pacchetti vengono sviluppati e venduti, senza codice sorgente, agli utilizzatori finali, Linux può essere analizzato, migliorato, studiato da chiunque abbia un po' d'interesse o di abilità. Questa è sicuramente una delle ragioni per cui Linux offre un alto grado di affidabilità e di prestazioni.

Non dimenticate: Internet è stata costruita e funziona quasi esclusivamente in base a progetti open source. Le e-mail che vi scambiate in tutto il mondo, hanno l'80% di probabilità di essere gestite da Sendmail, e le pagine web su cui "navigate" nel 50% dei casi vi vengono inviate da Apache. Che ne dite, è abbastanza affidabile ?

- Non c'è supporto per Linux.

Sentire dire una cosa del genere certe volte mi dà la nausea. Ma perché, gli "altri" distributori *offrono* supporto? L'ho sperimentato personalmente con uno dei sistemi operativi più popolari, dove il "supporto" era praticamente nullo.

Innanzitutto, il supporto per Linux *esiste* e mi riferisco al supporto commerciale. Ci sono alcune compagnie che, più avete voglia di spendere e più loro vi sostengono, offrendovi assistenza telefonica, via e-mail, oppure direttamente a casa vostra.

Comunque sappiate che il 99% dei problemi in cui vi imbratterete utilizzando Linux, possono essere risolti semplicemente con risposte ad una o due domande. E per questo c'è USENET e le mailing-list.

Non ho mai avuto un problema senza poi trovare la soluzione in uno dei tanti newsgroup. E, inoltre, ricevo una risposta alle mie domande in un tempo che varia normalmente dalle tre alle dodici ore dopo.

Un altro aspetto interessante di Linux è che, dato che il codice di tutto il kernel e delle altre parti del sistema operativo è disponibile gratuitamente, i problemi di sicurezza o con alcune CPU, vengono scoperti e risolti *molto* rapidamente, molto ma molto più rapidamente di problemi simili che si verificano con altri prodotti commerciali. Allora, dov'è il supporto commerciale!?

Ce ne sarebbero anche altri di miti, ma trattarli approfonditamente va oltre lo scopo di questa guida. Comunque, se siete interessati date un'occhiata al "Linux Myth Dispeller" su <http://www.KenAndTed.com/KensBookmark/linux/index.html> e anche al "The Linux FUDfactor FAQ" su <http://www.geocities.com/SiliconValley/Hills/9267/fud2.html>

3.3. Prospettive per un uso mono-utente

Personalmente uso Linux sia a casa sia sul lavoro.

Sul posto di lavoro, utilizziamo Linux per offrire servizi Internet a centinaia di utenti. Questi servizi comprendono l'autenticazione TACACS, hosting di pagine web e servizio di proxy caching, oltre a quelli SMTP e POP. Oltre a ciò, usiamo Linux per offrire servizi NFS e il pacchetto Samba per il protocollo SMB (WfW/Win95/WinNT) file & print e servizi FAX.

A casa, uso Linux per le mie esigenze, per Internet, per lo sviluppo di software e, naturalmente, per giocare (Quake II gira su Linux che è una bellezza). Una delle cose di Linux che più amo è che per quante cose possa fare, *non* va mai in crash. Inoltre, è un ottimo metodo per imparare, sviluppare e mantenere le mie conoscenze Unix.

Uso la distribuzione Red Hat 6.1 che include tutto il software necessario: le shell, compilatori e interpreti, supporto per il networking, il sistema X Window e tutti i servizi per Internet (per la posta, i newsgroup, telnet, web server, ecc.). La distribuzione comprende il kernel 2.2.12

Sul posto di lavoro, il sistema Linux che usiamo come Internet server primario ha questa configurazione:

- Kernel: 2.2.12
- Pentium II @ 300 MHz (bogo-mips 299.83) con PCI-bus, 256 Mb RAM
- Hard-disk da 3 Gb Fujitsu IDE (/dev/hda)
- Quattro hard-disk 4.4 Gb Quantum Fireball SCSI (da /dev/sd0 a /dev/sd3),
- CD-ROM 24x SCSI (/dev/scd0),
- Controller Adaptec AHA-131 SCSI
- Unità a nastri HP SCSI DAT (/dev/st0 e /dev/nst0),
- Scheda Ethernet Intel EtherExpress Pro 10/100

Sul secondo sistema gira una Red Hat 5.2, posizionato in un altro ufficio. Offre alcuni servizi con Samba, Squid e DNS secondari. Sfortunatamente dista più di 50 km da dove lavoro di solito, ed è un po' abbandonato a se stesso, ma è comunque il mio orgoglio e la mia gioia. È così composto:

- Kernel: 2.2.12
- Pentium II @ 350 MHz (bogo-mips 349.80) con PCI-bus, 256 Mb RAM
- Hard-disk da 4.1 Gb Quantum Fireball SCSI (/dev/sda)
- Quattro hard-disk 9.4 Gb Quantum Fireball SCSI (/dev/rd/c0d0, /dev/rd/c0d1) come hardware RAID level 5,
- CD-ROM 36x SCSI (/dev/scd0),
- Controller BusLogic BT-948 SCSI
- Controller RAID Mylex AcceleRAID 250 (DAC960),
- Unità a nastro HP SCSI DAT (/dev/st0 and /dev/nst0),
- Scheda Ethernet Intel EtherExpress Pro 10/100

Abbiamo, modestamente, un'incredibile disponibilità di 24+ Gb di spazio, con immagazzinamento ridondante configurato come apparato hardware RAID5. Il controller Mylex RAID funziona alla grande e consiglio di utilizzarlo a tutti coloro che vogliono utilizzare un hardware RAID. Se siete interessati a configurare il vostro sistema Linux con un apparato RAID, andate alla Sezione 11.2 per maggiori dettagli.

Abbiamo altre quattro macchine Linux, un Alpha, uno Sparc e due Intel; due dei quali sono usati in produzione, e poi c'è il mio sistema personale a casa ma non vi annoierò oltre con i dettagli.

Cercherò di rimanere in generale, senza riferirmi a nessun hardware particolare, ma ho pensato potesse essere utile per voi sapere che tipo di hardware possiedo.

Capitolo 4. Installazione e configurazione hardware

Questo capitolo mostrerà le procedure per installare Red Hat 6.1 su un sistema Intel; le procedure d'installazione sono simili sia usando l'interfaccia grafica sia usando la modalità solo testo. Dato che molte di queste informazioni sono ben spiegate nella Guida all'Utente di Red Hat (fornita in formato cartaceo con la distribuzione "ufficiale", inclusa nella directory `/doc` del cd, oppure disponibile online su <ftp://ftp.redhat.com/pub/redhat/redhat-6.1/i386/doc/rhinst/index.htm>, ho eliminato molti dettagli. Comunque, ci sono un po' di cose che credo manchino nella guida Red Hat, e quindi ho cercato di colmare queste lacune.

4.1. Creare un dischetto d'installazione

Il primo passo da fare per avere una distribuzione Red Hat di Linux sul vostro sistema è trovare il modo di far partire il programma d'installazione. Per fare ciò, di solito, bisogna creare un dischetto d'installazione, oppure, se volete installare da CD-ROM e il vostro bios lo permette, potete far partire l'installazione direttamente da CD.

Altrimenti, per creare un dischetto d'installazione, dovrete copiare il `boot.img` (che è semplicemente l'immagine di un dischetto d'avvio di Linux, formattato in ext2, con in più un programma d'installazione) su un floppy. Il file `boot.img` può essere reperito nella directory `/images` del CD-ROM della Red Hat, oppure potete scaricarlo via FTP da <ftp://ftp.redhat.com> (nella directory `/pub/redhat/redhat-6.1/i386/images`) (nel caso stiate installando linux su una box Intel).

Potete creare il dischetto di boot sia da un sistema DOS o Windows, sia da un sistema Linux o Unix. Potete usare un dischetto non formattato o uno pre-formattato (per DOS), non fa differenza.

Sotto DOS, supponendo che D: sia la vostra unità CD-ROM, potete scrivere:

```
d:
cd \images
..\dosutils\rawrite
```

Per il "file sorgente" (source file), inserite `boot.img`. Per il "file di destinazione" (destination file), inserite `a:` (se il drive A: corrisponde al vostro lettore floppy). Il programma `rawrite` copierà il file `boot.img` sul dischetto.

Sotto Linux/Unix, supponendo che il file `boot.img` si trovi nella directory corrente (potrete aver bisogno di montare il CD-ROM sotto `/mnt/cdrom` e trovare il file in `/mnt/cdrom/images`), potete scrivere;

```
dd if=boot.img of=/dev/fd0
```

L'utilità `dd` copierà il suo input file ("if"), il file `boot.img`, sull'output file ("of") `/dev/fd0` (ipotizzando che il vostro lettore floppy sia accessibile da `/dev/fd0`).

Se il vostro sistema Linux o Unix richiede i permessi di scrittura su floppy, dovrete dare questo comando come superutente. Se conoscete la password di root, scrivete `su` per diventare superuser, eseguite `dd` e poi digitate `exit` per tornare al normale stato d'uso.

Con entrambi questi metodi sarete in grado di creare un dischetto per l'avvio dell'installazione del vostro nuovo sistema Linux Red Hat!

4.2. Avviare il programma di installazione di Linux

Per impostare il vostro nuovo sistema Red Hat, inserite il CD d'installazione oppure il dischetto d'installazione nel lettore floppy A: e riavviate il sistema. Dopo qualche istante, dovrebbe apparire il programma di installazione di Red Hat.

In molti casi, basta premere <Enter> per iniziare l'installazione, ma se avete già una buona esperienza e conoscete esattamente il vostro hardware, potete digitare "expert" per le informazioni aggiuntive e le richieste previste da questa opzione. (Se non fate nulla, il processo d'installazione predefinita partirà dopo 10-15 secondi dopo l'apparizione della prima schermata).

Vi verrà poi chiesto di scegliere la vostra lingua, il tipo di tastiera e da dove state installarlo (per esempio da CD-ROM o dalla rete). Red Hat è molto flessibile su questo punto.

Probabilmente sceglierete "Local CDROM" per installare dal vostro CD-ROM Red Hat (che dovrebbe essere inserito nel lettore CD). Qualora il vostro sistema fosse sprovvisto di una unità CD-ROM, potrete scegliere altri tipi d'installazione.

Se avete un altro sistema Linux (oppure qualsiasi altro sistema operativo che supporta NFS), potete usare anche "NFS" per fare l'installazione. Per far ciò, dovete montare il vostro CD-ROM nell'altro sistema (oppure avere l'albero della distribuzione Red Hat da qualche parte sull'altro sistema -- è possibile scaricare qualunque cosa via FTP e poi installarla dall'hard-disk dell'altro vostro sistema), assicurarvi di avere nel file /etc/exports una riga che permetta l'accesso, per il nuovo sistema, alla giusta directory (andate alla Sezione 7.6 per informazioni su come impostare e usare NFS), e poi inserire le informazioni appropriate. Ecco un esempio:

- Inserite il CD di Red Hat CD nell'altro sistema (es. un sistema chiamato "spock").
- Per montare il CD, digitate:

```
mount /dev/cdrom /mnt/cdrom -t iso9660
```

- Modificate, come super-utente, il file "/etc/exports" ed inserite qualcosa come:

```
/mnt/cdrom newsys.mydomain.name(ro)
```

(Ciò indica che il nuovo sistema su newsys.mydomain.name può accedere, solo in lettura, alla directory "/mnt/cdrom/" e a qualunque altra subdirectory sotto di essa).

Se il vostro nuovo sistema non ha ancora un nome di dominio, potete utilizzare il suo indirizzo IP:

```
/mnt/cdrom 10.23.14.8(ro)
```

(Posto che il vostro nuovo sistema abbia l'indirizzo IP 10.23.14.8).

- Di nuovo, come super-utente, digitate:

```
killall -HUP rpc.nfsd ; killall -HUP rpc.mountd
```

Ciò riavvierà i demoni NFS e mountd, operazioni necessaria prima che NFS funzioni.

- Adesso, dal nuovo sistema, potete scegliere "NFS" come sorgente d'installazione. Vi verrà chiesto di fornire informazioni sulla vostra scheda di rete e sulle vostre impostazioni IP. Probabilmente userete impostazioni per IP statici se il vostro sistema fa parte di un LAN locale, oppure impostazioni DHCP se, per esempio, il vostro sistema è connesso a un cable modem. Inserite le giuste informazioni.

- Vi verrà poi chiesto il nome del server NFS e la directory di Red Hat. Per il nostro esempio dovremmo inserire "spock" come nome del server NFS, e "/mnt/cdrom/" per la directory di Red Hat.

Esistono anche altri modi per installare Red Hat, come l'utilizzo di Samba (networking in stile Windows), da un partizione sul vostro hard-disk (come la vostra partizione DOS o Windows 95), oppure via FTP. Consultate la guida all'utente di Red Hat per avere maggiori informazioni su questi altri metodi, oppure provateli direttamente (non sono molto difficili!).

Una volta scelto il metodo d'installazioni, Red Hat vi chiederà se volete "Install" (installare) oppure "Upgrade" (aggiornare) il vostro sistema. Voi scegliere ovviamente la prima opzione ("Install"). (personalmente non faccio *mai* aggiornamenti di nuove versioni della distribuzione su quelle vecchie -- credo di aver sofferto abbastanza con i prodotti Microsoft e quindi non mi fido più. Preferisco fare l'installazioni dall'inizio e poi recuperare i dati, miei e degli utenti, da copie di backup).

Il programma d'installazione vi chiederà poi se una scheda SCSI. Se rispondete di si, vi verrà chiesto di scegliere il driver adatto. In alcuni casi, comunque, Red Hat riconoscerà la vostra scheda automaticamente.

Vi verrà poi chiesto di impostare i vostri file system (cioè di partizionare uno o più dischi per Linux). Ci sono due strumenti disponibili per impostare le partizioni, quello incluso con Red Hat cioè "Disk Druid", e quello standard di Linux "/fdisk".

Sono molto simili tra loro e vi permettono di specificare i tipi di partizione e le dimensioni. Comunque, Disk Druid sembra essere più "user friendly" e un po' più completo di fdisk. Infatti, se scegliete di usare fdisk, vi troverete *comunque* di fronte ad una schermata di Disk Druid nella quale potrete specificare i vostri mount point. C'è da dire che, essendo stato un utente Slackware, uso sempre fdisk -- forza dell'abitudine, credo! :-)

La sezione successiva contiene informazione sul come e sul perché impostare le partizioni.

4.3. Partizionamento dei dischi fissi

Perché mai effettuare un partizionamento? Sebbene sia possibile avere un sistema Linux perfettamente funzionante su un'unica partizione, ed è anche leggermente più facile da fare, si possono ottenere molti vantaggi dividendo uno o più dispositivi di immagazzinamento dati in partizioni multiple.

Anche se è vero che Linux funzionerà egregiamente su un disco con un'unica grande partizione, può essere conveniente, sotto diversi aspetti, suddividere il vostro disco almeno per i quattro file system principali (root, usr, home e swap). Questi aspetti includono:

Primo, è possibile ridurre il tempo necessario ad effettuare i controlli dei file system (sia al momento del boot e sia eseguendo manualmente un fsck), perché tali controlli possono essere fatti in parallelo (A proposito, *MAI* eseguire un fsck su un file system montato!! Quasi certamente ve ne pentireste. L'eccezione a questa regola è che il file system sia montato read-only, allora tale azione risulterebbe innocua). Inoltre, i controlli sui file system sono più facili da realizzare su un sistema con partizioni multiple. Per esempio, se sapessi che la mia partizione /home presenta dei problemi, potrei semplicemente smontarla, effettuare un controllo del file system, e poi rimontare il file system riparato (invece di fare il boot del mio sistema, con un dischetto di soccorso, in modalità mono-utente e effettuare le riparazioni).

Secondo, con partizioni multiple, potete, se volete, montare una o più partizioni come read-only. Per esempio, se decidete che tutto quello che c'è in /usr non possa essere toccato nemmeno dal root, potete montare la partizione /usr come read-only.

In ultimo, il beneficio maggiore che si può trarre del partizionamento è la protezione dei vostri file system. Se dovesse succedere qualcosa ad un file system (a causa di un errore di un utente o di un malfunzionamento del sistema), su un sistema partizionato voi, probabilmente, perdereste file solo su un singolo file system. Mentre su un sistema non partizionato, probabilmente li perdereste su tutti i file system.

Ciò può esservi ulteriormente d'aiuto. Per esempio, se la vostra partizione root è talmente corrotta da non permettervi di effettuare il boot, potete usare il dischetto di soccorso, montare la vostra partizione root, e copiare quello che potete (o recuperare da un backup; si veda il Capitolo 8 per informazioni su come effettuare il backup e il restore dei file), su un'altra partizione come home, e poi riavviare ancora con il dischetto di emergenza, digitare "mount root=/dev/hda3" (posto che la partizione che contiene il vostro temporaneo file system root sia sulla terza partizione di hda) e avviare Linux completamente funzionante. Potete poi avviare un fsck sulla vostra smontata partizione root corrotta.

Ho *avuto*, personalmente, esperienza con catastrofi nei file system, e sono stato molto contento di aver potuto limitare i danni grazie all'uso di partizioni multiple.

Infine, visto che Linux vi permette di impostare altri sistemi operativi (come Windows 95/98/NT, BeOS, o quello che avete), e di avviare quello che vi pare, potreste trarre vantaggio dall'aver partizioni in più. Tipicamente, vorrete impostare almeno una partizione per ogni sistema operativo. Linux include un discreto boot loader (chiamato LILO sui sistemi basati su Intel, oppure MILO su Alpha e SILO su Sparc) che vi permette di specificare quale sistema operativo volete avviare al momento dell'accensione, con un periodo di tempo trascorso il quale verrà avviato il vostro sistema operativo preferito (probabilmente Linux, giusto?)

Dovete partizionare un disco (o più dischi) a seconda delle vostre esigenze. Nella mia esperienza con piattaforme Intel, Alpha e Sparc, per un sistema caricato completamente e che svolge una notevole quantità di compiti (come un sistema desktop a casa, o come un Internet server sul lavoro), ho scoperto che la seguente approssimazione di spazio funziona piuttosto bene per determinare la dimensione di una partizione.

Dato:

Dato un disco di X Mb/Gb (es. 2 Gb)
(O più di un disco con complessivi X Mb/Gb)

Calcolare:

```
(swap) circa il doppio della memoria RAM (es. 64 Mb allora 128 Mb swap)
/ (root) circa il 10% di quanto disponibile (es. 200 Mb)
/home circa il 20% di quanto disponibile (es. 400 Mb)
/usr tutto lo spazio rimanente (es. 1272 Mb)

/var (opzionale -- vedi sotto)
/boot (opzionale -- vedi sotto)
/archive (opzionale -- vedi sotto)
```

Sicuramente, quanto sopra rappresenta solo una linea guida. Ovviamente manipolerete queste percentuali a seconda di come volete utilizzare il vostro sistema Linux. Se volete aggiungere molte applicazioni voluminose come WordPerfect oppure Netscape, o forse volete aggiungere il supporto per i caratteri giapponesi, allora probabilmente vorrete un po' più di spazio per /usr.

Mi sembra *sempre* di avere troppo spazio disponibile in /home, quindi se i vostri utenti non fanno molto (oppure avete imposto loro dei limiti), oppure non offrite account di shell, pagine web personali, ecc. allora potrete diminuire lo spazio per /home e aumentare quello per /usr.

Qui di seguito c'è una descrizione dei vari mount point e informazioni sui file system, che potrebbero chiarirvi le idee su come definire al meglio le dimensioni delle vostre partizioni:

- */ (root)* - viene usato per memorizzare cose come file temporanei, il kernel di Linux e l'immagine di boot, importanti file binari (cose di cui c'è bisogno prima che Linux possa montare la partizione */usr*), i più importanti file di log, aree di spool per compiti di stampa, e-mail in uscita, ed e-mail in entrata degli utenti. Viene anche usato come spazio temporaneo quando si compiono certe operazioni come la creazione di pacchetti RPM dai file RPM sorgenti. Quindi, se avete molti utenti con tante e-mail, o pensate di aver bisogno di tanto spazio temporaneo, allora avrete bisogno di più spazio a disposizione. Il tipo di partizione dovrebbe essere lasciato, come predefinito, a 83 (Linux native). In più probabilmente attiverete il bootable flag su questa partizione per fare in modo che le informazioni del boot vengano memorizzate qui.
- */usr/* - dovrebbe essere la partizione più grande, perché la maggior parte dei file binari richiesti da Linux, così come ogni software installato localmente, le pagine web, il proxy cache di Squid, i servizi di condivisione di Samba, i file di log di alcuni software installati localmente, ecc, sono memorizzati qui. Il tipo di partizione dovrebbe essere lasciato, come predefinito, a 83 (Linux native).
- */home/* - se non fornite account di shell ai vostri utenti, non avete bisogno di una partizione molto grande. L'eccezione è che se fornite pagine web agli utenti (come quelle per una scuola) allora sarebbe meglio avere una partizione più grande. Il tipo di partizione dovrebbe essere lasciato, come predefinito, a 83 (Linux native).
- (*swap*) - Linux offre qualcosa chiamata "memoria virtuale" per rendere disponibile una quantità maggiore di memoria rispetto alla RAM fisica del vostro sistema. La partizione di swap è usata insieme alla memoria RAM. Come regola generale, la vostra partizione di swap dovrebbe essere almeno di doppio della memoria RAM installata sul vostro sistema.

Se avete più di un disco fisso sul vostro sistema, potete creare partizioni multiple di swap. Ciò può aumentare le performance di swapping sfruttando l'accesso a dischi paralleli. Per esempio, su un sistema con 256 Mb e quattro dischi, io creerei quattro partizioni di swap da 128 Mb, per un totale di 256 Mb di RAM e 512 Mb di swap. (Per un totale di 768 Mb disponibili come memoria virtuale). Il tipo di partizione deve essere cambiato a 82 (Linux swap).

Nota: Si è spesso detto che per Linux la dimensione di swap può essere di massimo 128 Mb. Ciò era vero in passato, ma nelle moderne distribuzioni la dimensione dipende dalla vostra architettura (per esempio, sistemi Intel possono aver dimensioni di swap anche di 2 Gb). Digitate "man mkswap" per maggiori informazioni.

- */var/* (opzionale) - Potreste considerare l'idea di suddividere ulteriormente la vostra partizione */root*. La directory */var* è usata molto quando la macchina è in funzione, contiene molti dati, compresi gli spool di posta (sia in uscita che in entrata), code di stampa, processi di lock, ecc. Essendo questa directory montata sotto */(root)* può essere un po' pericolosa perché un gran numero di e-mail in arrivo (per esempio) potrebbe riempirla velocemente. Poiché possono succedere cose spiacevoli (crash di sistema, ad esempio) quando la partizioni */(root)* si riempie, avere */var* su una propria partizione può evitare tali problemi. Ho trovato utile prendere tutto lo spazio che avevo dato a */(root)*, forse raddoppiandolo, e poi creare partizioni separate per */(root)* e per */var*. Il tipo di partizione dovrebbe essere lasciato, come predefinito, a 83 (Linux native).
- */boot/* (opzionale) - In alcuni casi (come un sistema impostato con configurazione RAID) può essere necessario avere una partizione separata dalla quale effettuare il boot del sistema Linux. Questa partizione permetterebbe di fare il boot e poi caricare qualunque driver necessario per leggere gli altri file system. La dimensione di questa partizione può essere anche di un paio di Mb; Io raccomando di usare circa 10 Mb (che dovrebbero darvi spazio

sufficiente per il kernel, l'immagine ram disk iniziale e anche per uno o due backup del kernel). Il tipo di partizione dovrebbe essere lasciato, come predefinito, a 83 (Linux native).

- */archive/* (opzionale) - Se avete dello spazio extra potreste trovare utile avere una partizione per una directory chiamata, per esempio, */archive*. Potete usare questa directory per memorizzare copie di backup, file grandi con pochi accessi, i servizi file di samba, o qualunque altra cosa vogliate. Il tipo di partizione dovrebbe essere lasciato, come predefinito, a 83 (Linux native), o se se volete accedervi da Linux e da qualche altro sistema operativo, allora dovrete cambiarlo, come ad esempio 6 (DOS 16-bit >=32M).

In caso di aggiunta di altri dischi, potete aggiungere ulteriori partizioni, montate con diversi mount point -- ciò significa che un sistema Linux non si preoccuperà mai della mancanza di spazio. Per esempio, se in futuro sda6 dovesse iniziare a riempirsi, potremmo aggiungere un altro drive, impostare una partizione ben dimensionata con un mount-point in */usr/local* -- e poi trasferire tutte le informazioni da */usr/local* sul nuovo drive. Ma nessun sistema o applicazioni si “bloccherebbe”, perché Linux vedrebbe */usr/local* senza preoccuparsi di dove si trova.

Per darvi un esempio di come potrebbero essere impostate le partizioni, ho usato il seguente schema su un sistema Intel (doppio boot, Windows95 e Linux):

Device	Boot	Begin	Start	End	Blocks	Id	System
/dev/hda1	*	1	1	254	1024096+	6	DOS 16-bit >=32M
/dev/hda2		255	255	782	2128896	5	Extended
/dev/hda5		255	255	331	310432+	83	Linux native
/dev/hda6		332	332	636	1229728+	83	Linux native
/dev/hda7		637	637	749	455584+	83	Linux native
/dev/hda8		750	750	782	133024+	82	Linux swap

La prima partizione, */dev/hda1*, è un file system DOS per il sistema operativo alternativo (Windows 95). Ciò mi dà per esso 1 Gb di spazio.

La seconda partizione, */dev/hda2*, è una partizione fisica (chiamata “estesa”) che comprende lo spazio rimanente sul drive. È usata solo per incapsulare le rimanenti partizioni logiche (ci possono essere solo 4 partizioni fisiche su un disco; nel mio caso avevo bisogno di più di 4 partizioni, quindi ho dovuto usare uno schema di partizionamento logico per le altre).

Le partizioni da tre a cinque, */dev/hda5*, */dev/hda6* e */dev/hda7*, sono tutti file system e2fs usati rispettivamente per le partizioni */*(root), */usr* e */home*.

Infine, la sesta partizione, */dev/hda8*, è usata come partizione di swap.

Come ulteriore esempio, questa volta su un box Alpha con 2 hard-disk (unico boot, solo Linux), ho scelto il seguente schema di partizionamento:

Device	Boot	Begin	Start	End	Blocks	Id	System
/dev/sda1		1	1	1	2046	4	DOS 16-bit <32M
/dev/sda2		2	2	168	346859	83	Linux native
/dev/sda3		169	169	231	130851	82	Linux swap
/dev/sda4		232	232	1009	1615906	5	Extended
/dev/sda5		232	232	398	346828	83	Linux native
/dev/sda6		399	399	1009	1269016	83	Linux native
/dev/sdb1		1	1	509	2114355	83	Linux native
/dev/sdb2		510	510	1019	2118540	83	Linux native

La prima partizione, */dev/sda1*, è un file system DOS per il boot loader MILO. La piattaforma Alpha ha un metodo per il boot leggermente diverso rispetto ai sistemi Intel, quindi Linux memorizza le informazioni di boot in una partizione FAT. Questa partizione deve essere grande come il minimo possibile consentito; in questo caso, 2 Mb.

La seconda partizione, `/dev/sda2`, è un file system `e2fs` per la partizione `/`(root).

La terza partizione, `/dev/sda3`, viene usata come partizione di swap.

La quarta partizione, `/dev/sda4`, è una partizione “estesa” (date un’occhiata all’esempio precedente per maggiori dettagli).

La quinta e sesta partizione, `/dev/sda5` e `/dev/sda6`, sono file system `e2fs` usati per `/home` e `/usr`.

La settima partizione, `/dev/sdb1`, è un file system `e2fs` per la partizione `/archive`.

L’ottava e ultima partizione, `/dev/sdb2`, è un file system `e2fs` usato per la partizione `/archive2`.

Dopo avere impostato le informazioni per la partizione, dovete scrivere la nuova partizione sul disco. Fatto ciò, il programma di installazione di Red Hat ricaricherà in memoria la tabella di partizione, in modo che possiate continuare col processo d’installazione.

4.4. Impostare lo spazio di Swap

Una volta che avete impostato le partizioni e avete assegnato i mount point (per esempio `/usr` è il “mount point” per il file system `/usr`), il programma d’installazione vi chiederà quale partizione deve essere usata per lo spazio di swap. Dato che la partizione di swap dovrebbe essere già identificata come tale (ID #82) premete `<Enter>` per iniziare a formattarla. Vi consiglio di attivare l’opzione “`Check for bad blocks during format`” per fare in modo di eliminare eventuali danneggiamenti. Ciò rallenterà il processo di formattazione ma credo rappresenti un buon compromesso.

4.5. Scegliere le partizioni da formattare

Adesso il programma d’installazione vi mostrerà una lista di partizioni che avete assegnato a Linux, e vi chiederà di selezionare quali, se ve ne sono, di queste volete formattare come nuovi file-system. Probabilmente, vorrete formattarle tutte, tranne se volete aggiornare il vostro file-system o se avete informazioni (ad esempio in `/home`) che non volete perdere.

Ancora una volta vi ricordo di attivare l’opzione “`Check for bad blocks during format`”.

4.6. Scegliere i pacchetti da installare

Dopo questo, vi verrà mostrata una lista di componenti di sistema e vi verrà chiesto di specificare quali devono essere installati. Se siete un utente Linux con un po’ di esperienza, potete scegliere solo quelli di cui avete bisogno. Se, invece, siete nuovi di Linux, probabilmente sceglierete l’opzione più in basso, “Everything”.

Io, di solito, scelgo i componenti di cui ho bisogno e poi attivo l’opzione “`Select individual packages`”, che mi consente di controllare meglio il processo d’installazione.

Una volta che avete fatto le vostre scelte, selezionate “`ok`” per iniziare l’installazione. Se avete attivato l’opzione “`Select individual packages`”, vi verrà chiesto di specificare i singoli pacchetti da installare. Ciò è molto semplice, e se volete assicurarvi di cosa faccia un pacchetto, premete `<F1>` per averne una breve descrizione.

Non preoccupatevi se scegliete per errore (o non scegliete affatto) uno o due pacchetti. Dopo tutto, i pacchetti sono sul CD-ROM (o su altro supporto), e potete usare l’utilità Red Hat RPM per fare aggiustamenti dopo che il vostro sistema è in funzione (si veda la Sezione 10.1 per maggiori informazioni).

Dopo che avete scelto i pacchetti, il programma d'installazione formatterà le partizioni che avete definito. Ci vorrà qualche minuto, specialmente per partizioni molto grandi e se avete attivato l'opzione di controllo dei blocchi danneggiati, quindi non pensate che il vostro sistema si sia bloccato durante questa operazione.

Dopo che il processo di formattazione è terminato, Red Hat Linux comincerà a installare i pacchetti. Dovrebbero volerci dai cinque ai quindici minuti per completare l'operazione, ma ciò dipende dalla velocità del vostro sistema.

4.7. Installazione e configurazione Hardware

Dopo l'installazione dei pacchetti, Red Hat provvederà alla configurazione dei componenti del vostro sistema. Nella maggior parte dei casi, tranne che per componenti molto recenti che potrebbero non essere supportati da Linux, il programma di installazione farà tutto da sé, automaticamente.

Vedrete nell'ordine:

- Riconoscimento del vostro mouse (con la scelta tra i modelli a due o tre tasti. Se avete un mouse a 2 tasti, probabilmente attiverete l'emulazione a 3 tasti).
- Riconoscimento della scheda video
- Scelta del monitor
- Esecuzione di "XConfigurator" per configurare il sistema X Window (vorrete "testare" la vostra scheda. Se incappate in un errore, non preoccupatevi, potrete mettere a posto la configurazione di X più tardi, quando il vostro sistema sarà in funzione; andate al Capitolo 5 per maggiori dettagli.)
- Selezionare la modalità video (potete scegliere quella predefinita, o selezionare quella che vorrete usare in X Window)
- Configurazione della LAN
- Configurazione dell'orologio
- I servizi di start up (la selezione predefinita è probabilmente la migliore, ma potete premere <F1> per avere una descrizione dei compiti svolti da ogni servizio.)
- Configurazione della stampante
- Assegnazione della password di root (sceglietela con cura!)
- Creazione di un boot disk [non siate pigri, fatene uno! :-)]

4.8. Boot con LILO

Fatto ciò, il programma di installazione scriverà un boot-loader sul vostro hard-disk. Il boot-loader (*LILLO* sui sistemi Intel) vi permetterà di caricare Linux oppure ogni altro sistema operativo presente, nel caso abbiate impostato il vostro sistema per un multi-boot (si veda la Sezione 4.8.1 per maggiori dettagli).

La finestra di dialogo del "Lilo Installation" vi chiederà di scegliere dove scrivere il boot-loader.

Probabilmente sceglierete di installarlo nel master boot record del vostro primo disco (di solito dev/hda per IDE, /dev/sda per SCSI).

Fatto questo, apparirà una seconda finestra di dialogo, che vi permetterà di inserire parametri extra di configurazione. Di solito qui non viene inserito nulla ma, se avete più di 64 Mb di memoria RAM, avrete bisogno di inserire uno speciale parametro per permettere a Linux di gestire la memoria extra (altrimenti userete solo i primi 64 Mb). Se, ad esempio, avete 128 Mb di RAM dovete inserire:

```
append="mem=128M"
```

Se il vostro sistema ha dischi SCSI o volete installare LILO su una partizione con più di 1023 cilindri, potrebbe essere necessario attivare l'opzione "Use linear mode". Se non è così, anche attivando tale opzione non succederà nulla. Quindi vi consiglio di farlo.

4.8.1. Multi-boot con altri Sistemi Operativi

Se avete impostato il vostro sistema per un multi-boot di Linux con altri sistemi operativi, vi troverete di fronte ad una terza finestra di dialogo contenente una lista delle partizioni disponibili. Qui, potrete assegnare dei nomi agli altri sistemi operativi (quello che inserite apparirà, poi, al prompt di "LILO", al momento della scelta di quale sistema operativo avviare). Il programma d'installazione assegna comunque dei nomi predefiniti ad ogni partizione bootabile.

Il sistema operativo che sarà avviato in modo predefinito, sarà ovviamente Linux. Se volete, comunque, potrete cambiare anche questo parametro.

Dopo aver installato il boot-loader sul vostro hard-disk, il programma di configurazione vi farà le sue "Congratulations", indicandovi che Linux è stato installato correttamente. Togliete il dischetto d'installazione (se c'è) e premete <Enter> per fare il reboot del vostro sistema... in Linux!

Linux verrà caricato e, se tutto è andato per il meglio, dovrete trovarvi di fronte la scritta "login". A questo punto, dovrete essere in grado di entrare come "root" usando la password che avete scelto durante il processo d'installazione.

4.9. Scaricare e installare gli aggiornamenti di Red Hat

Red Hat ha prodotto alcune buone versioni della sua distribuzione, ma sembra che esse siano state rilasciate anche se non ancora completamente pronte all'uso. Quindi, per ottenere il meglio dal vostro sistema Linux, è necessario scaricare e implementare alcuni pacchetti d'aggiornamento. Questi pacchetti, meglio noti come "file rpm" possono essere implementati ricorrendo alla utilità RPM (per maggiori dettagli si veda la Sezione 10.1).

Questo è uno dei compiti che richiede più tempo al fine di avere il vostro sistema Linux pronto all'uso (a meno che non abbiate una connessione a Internet davvero veloce). Comunque, mettete in conto un po' di tempo per far ciò. Vi risparmierete senz'altro *parecchie* noie!

Innanzitutto, scaricate tutti i file da:

`ftp://ftp.redhat.com/redhat/updates/6.1/i386/`

(Ammesso che stiate usando Linux su un box Intel).

Scaricherete, con ogni probabilità, tutto in una sola directory, e dovrete quindi digitare "rpm -Uvh *" che aggiornerà tutti i pacchetti. Se avete scaricato qualche file rpm per il kernel, dovrete probabilmente spostarli, per il momento, in un'altra directory. Aggiornare e personalizzare il kernel è un po' complicato e dev'essere fatto con molta attenzione (maggiori informazioni nella Sezione 10.4). Quindi, prima di procedere agli aggiornamenti, spostate tutti i file rpm per il kernel in un'altra directory.

Per implementare gli aggiornamenti, potete semplicemente applicare tutti i pacchetti in una volta sola ("rpm -Uvh *"), o se preferite, potete aggiornarli uno alla volta ("rpm -Uvh file_da_aggiornare.rpm"). Il secondo metodo permette di assicurarci che ogni aggiornamento sia stato applicato senza errori. :-)

Con l'utilità RPM potete anche vedere se, prima di aggiornarlo, un determinato pacchetto è già installato oppure verificarne la versione; Maggiori dettagli nella Sezione 10.1.

Capitolo 5. Configurare il sistema X Window

Il sistema X Window, anche noto come "X" (comunemente conosciuto da molti come "X-Windows") è una GUI su Linux. Al contrario di Microsoft Windows, X Window può apparire e funzionare in molti modi. Può lavorare in maniera primitiva o molto avanzata. Può apparire bello o brutto. Funzionare velocemente o molto lentamente (tutti aspetti che hanno portato ad un lungo dibattito tra gli utilizzatori, come già è accaduto per la discussione "Linux vs. Microsoft NT").

Far funzionare X in maniera corretta può essere facile o anche molto complicato! È la lamentela più comune per quelli che si avvicinano per la prima volta a Linux. E, dato che anch'io ho lottato parecchie volte con i parametri di configurazione, mi sento molto coinvolto. Fortunatamente, alcune configurazioni sono diventate molto più facile e spesso svolte in automatico dalle nuove distribuzioni di Linux. Se utilizzate Red Hat 6.1 probabilmente non vi dovrete preoccupare di questo problema.

Sebbene nella maggior parte dei casi X può essere configurato automaticamente, ci sono alcune eccezioni; Vi raccomando di scoprire di quale scheda video siete dotati e la sua quantità di memoria RAM, oltre al tipo di monitor e i valori di sincronizzazione verticale e orizzontale (queste informazioni sono di solito disponibili nel manuale del monitor, oppure possono essere reperite su Internet).

5.1. Far funzionare X Window con X-Configurator

Ci sono due metodi per far funzionare X sotto una distribuzione Linux di Red Hat. Il primo e il più facile, è quello di usare l'utilità "xconfigurator" che Red Hat ci mette a disposizione. Questa utilità cerca di individuare il vostro hardware e installa il software più appropriato con le impostazioni di configurazione più idonei.

Se, dopo aver provato diverse configurazioni con Xconfigurator, non avete avuto successo, forse potreste essere più fortunati con l'utilità "xf86config". Anche se Xconfigurator non è poi tanto user-friendly, vi permette di avere un maggior controllo sul processo di configurazione.

Se proprio la sfortuna è dalla *vostra* parte allora dovrete editare il file "/etc/X11/XF86Config" provando a modificare i vari parametri. In questo caso potreste aver bisogno di aiuto da parte della comunità Linux (si veda la Sezione 13.3 per maggiori dettagli). Comunque sappiate che nella maggior parte dei casi Xconfigurator svolge il suo lavoro egregiamente.

Dopo aver fatto funzionare X, potreste lamentarvi della scarsità di colori vividi. Infatti, X usa in modo predefinito un'intensità di 8-bit per pixel ("*bpp*"). Potrete modificare tale intensità, a patto che il vostro hardware la supporti.

Le varie intensità di colore sono elencate nel file "/etc/X11/XF86Config", che appare così:

```
Subsection "Display"
    Depth      24
    Modes      "800x600" "1024x768"
    ViewPort   0 0
    Virtual    1024 768
EndSubsection
```

La sezione sopra mostra le possibili risoluzioni disponibili usando un'intensità di colore a 24-bit (800x600 e 1024x768, come si può vedere nella riga "Modes"); Queste risoluzioni possono essere cambiate "a volo" usando i tasti <Alt><+> e <Alt><->

Suggerimento: Suggerimento: in modo predefinito, X utilizza la risoluzione più bassa tra quelle elencate. Se ciò non vi piace, editate il file `/etc/X11/XF86Config` e invertite le risoluzioni (cioè "1024x768" "800x600").

Potete testare manualmente ogni intensità di colore digitando `startx -- -bpp 24` (per quella a 24-bit), in modo da verificare che tutto funzioni correttamente.

Se riuscite ad utilizzare una intensità di colore maggiore e volete usarla in modo predefinito, dovrete creare il file `/etc/X11/xinit/xserverrc` come segue:

```
exec X :0 -bpp 24
```

Ciò vi permetterà di usare X a 24 bpp (se avete problemi provate 16 o 32 invece di 24).

Assumendo che abbiate configurato X correttamente, digitate semplicemente, come qualunque utente, `startx`. L'X GUI si avvierà, e dopo che avete terminato la vostra sessione e siete usciti da X, tornerete alla console di Linux.

A scelta potete far partire X direttamente al boot di sistema. Ciò può risultare utile per coloro che non amano la noiosa console bianca e nera, o per quelli che vogliono avere poco a che fare con la riga di comando.

5.2. Usare l'X Desktop Manager

Se volete, potete usare l'X Desktop Manager ("`xdm`") per fare in modo che X Window parta automaticamente con il boot di sistema. Il vostro sistema Linux partirà sempre sotto X (benché possiate passare dalla GUI alla console con `<Ctrl>-<Alt>-<F1>`, e poi di nuovo alla GUI con `<Alt>-<F7>`). È un metodo molto facile, per voi e per i vostri utenti, di evitare di digitare ogni volta `startx`.

Per attivare `xdm`, editate il file `/etc/inittab` e cambiate la riga `"id:3:initdefault:"` in:

```
id:5:initdefault:
```

Tale cambiamento porterà Linux, al momento del boot, al run level 5 che avvierà `xdm`. Controllate anche che nel file `/etc/inittab` sia presente la seguente riga:

```
x:5:respawn:/usr/bin/X11/xdm -nodaemon
```

Se avete attivato `xdm` e volete usare un valore di "bpp" maggiore di quello di predefinito (cioè 8), e sempre la vostra scheda video e il vostro monitor lo supporti), modificate il file `/etc/X11/xdm/Xservers` come segue:

```
:0 local /usr/X11R6/bin/X -bpp 24
```

Questa modifica eseguirà `xdm` a 24 bits per pixel.

Vorrete inoltre editare il file `/etc/X11/xdm/Xsetup_0` e, usando il carattere `"#"` decommentate la riga che avvia `"xbanner"`:

```
#/usr/X11R6/bin/xbanner
```

Ciò impedirà la visualizzazione della schermata di `xdm` tra le sessioni KDE. È solo una questione estetica, ma...

Suggerimento: Suggerimento: talvolta potreste avere bisogno di tornare alla console (per esempio, alcuni giochi non funzionano sotto X). Esistono due modi per far ciò: per passare temporaneamente alla console, premete `<Alt><F1>`, e per tornare a X premete `<Alt><F7>`. Oppure, se volete uscire completamente da X (liberando

anche un po' di memoria), digitate `"/sbin/telinit 3"` come "root"; in questo modo direte a XDM di terminare. Per tornare alla situazione precedente, digitate `"/sbin/telinit 5"`.

5.3. Migliorare l'aspetto dei font sotto X

Francamente, X non ha avuto mai font particolarmente belli. E molta gente si è rassegnata a questa idea.

Fortunatamente, è possibile migliorare notevolmente l'aspetto e il numero di font che potete usare sotto X. Se avete, infatti, una copia di Windows, potrete prelevare i font TrueType in esso contenuti e usarli con X. Tutto ciò è reso possibile dall'uso di un font server come "xfs" oppure "xfs".

Red Hat 6.1 include già il supporto per "xfs", e quindi fornisce il supporto per font più accattivanti. Tuttavia vi sono un paio di cose da fare per migliorare le cose, come pure per utilizzare i font TrueType (se ne avete a disposizione).

Per abilitare il supporto dei font TrueType, create una directory (per esempio `"/usr/local/share/ttfonts"`) e copiateci tutti i font del vostro Windows (li potete trovare nella directory `"c:\windows\fonts"`).

Suggerimento: Suggerimento: Se non avete a disposizione font TrueType, potete scaricarli direttamente da Microsoft: <http://www.microsoft.com/typography/fontpack/default.htm> (<http://www.microsoft.com/typography/fontpack/default.htm>).

Per usare i font, dalla vostra nuova directory "ttfonts" digitate come root:

```
ttmkfdir -o fonts.scale  
mkfontdir
```

Successivamente, editate il file `"/etc/X11/fs/config"` e aggiungete la vostra nuova directory alle lista di quelle già esistenti. Inoltre, cambiate `default-point-size` da 120 a 140, che renderà i caratteri più leggibili.

Infine, uscite da X (se non l'avete già fatto), e riavviate il server xfs nel seguente modo:

```
/etc/rc.d/init.d/xfs restart
```

Riavviate ora X e godetevi i vostri nuovi font!

Per maggiori informazioni esiste un ottima risorsa chiamata *"XFree86 Font Deuglification Mini HOW-TO"* presso <http://www.frii.com/~meldroc/Font-Deuglification.html> (<http://www.frii.com/~meldroc/Font-Deuglification.html>).

5.4. Scegliere un Window Manager per X

Avrete bisogno, adesso, di scegliere un window manager. Il sistema X Window è semplicemente l'ambiente che permette la visualizzazione della grafica sul vostro hardware; il window manager è invece responsabile dell'aspetto di X e di come esso debba interagire con voi e con le vostre applicazioni.

La distribuzione Red Hat contiene diversi window manager, compresi fvwm, olvm, twm, AfterStep e altri. Quello predefinito, e ve ne accorgete quando lancerete X per la prima volta, è fvwm95, un ambiente simile a Windows 95 (adesso c'è un tema comune a KDE e GNOME).

Personalmente non mi aggrada molto, e vi suggerisco di usare GNOME o KDE (o addirittura entrambi!), le cui procedure d'installazione saranno affrontate nei prossimi due paragrafi.

5.5. Installazione e configurazione di GNOME

Il GNU Network Object Model Environment (GNOME) è un ambiente a finestre che abbellisce X window. Presenta molte qualità, compreso un buon numero di applicazioni che potrebbero esservi utili. Al momento in cui scrivo GNOME presenta ancora alcuni bug ma, comunque, è stabile e utilizzabile appieno.

Se usate Red Hat 6.1, l'ultima versione di GNOME (cioè l'ultima disponibile mentre sto scrivendo) fa parte della distribuzione. Altrimenti dovrete scaricare gli RPM più recenti del pacchetto. Tuttora, i file RPM per Red Hat 6.0 i386 si possono trovare su <ftp://ftp.gnome.org/pub/GNOME/RHAD/redhat-6.0/i386/> (o su un sito in mirror).

Nota: Se utilizzate Red Hat 6.0, dovrete essere avvertiti che la versione di GNOME inclusa presenta alcuni bug. Dovreste allora scaricare gli RPM più recenti dal sito FTP sopra indicato.

Quando siete in possesso di tutti i file necessari, potete installare GNOME digitando come "root" quanto segue:

```
rpm -Uvh gtk*.rpm *.rpm
```

(Questo comando si assicura che le librerie GTK siano installate, in modo da evitare eventuali errori di dipendenza).

Contrariamente a quanto si crede, GNOME *non* è propriamente un Window manager, ma piuttosto fornisce ad esso maggiori funzionalità. Quindi, dopo aver installato GNOME, dovrete decidere quale window manager adottare e creare il file ".xinitrc" nella vostra directory che provvederà a caricare il window manager adatto e ad avviare GNOME. Il file dovrebbe apparire più o meno così:

```
afterstep &  
exec gnome-session
```

Questo file caricherà AfterStep come window manager, e poi avvierà GNOME.

Maggiori informazioni sul GNU Network Object Model Environment possono essere reperite sul sito GNOME <http://www.gnome.org/>. Non dimenticate di dare un'occhiata agli screenshot su <http://www.gnome.org/screenshots/>.

5.6. Installazione e configurazione di KDE

Il K Desktop Package (KDE) è un altro window manager molto popolare ed è, al momento in cui scrivo, sicuramente più maturo di GNOME anche se sembra che abbia bisogno di più memoria RAM rispetto a quest'ultimo. Date un'occhiata all'ammontare della vostra memoria RAM: se avete meno di 64 Mb e 128 Mb di swap, la scelta migliore è usare GNOME.

Il primo passo da compiere per installare KDE è quello di scaricare gli RPM più recenti: cercate un mirror FTP su <http://www.kde.org/mirrors.html>. Scegliete quello più vicino alla vostra posizione geografica assicurandovi che esso venga aggiornato spesso (date un'occhiata alla lista dei mirror).

Quando avete trovato quello più adatto scaricate gli RPM relativi alla vostra versione di Red Hat e alla vostra piattaforma. Ad esempio, se utilizzate Red Hat 5.2 (o superiore) su una piattaforma Intel, dovrete scaricare il

pacchetto dalla directory `"/pub/mirrors/kde/stable/latest/distribution/rpm/RedHat-5.2/i386/"` del mirror FTP.

Una volta in possesso di tutti i file necessari, per installare KDE digitate, come “root” (assicurandovi di trovarvi nella directory che contiene i file rpm di KDE):

```
rpm -Uvh qt*.rpm
install-kde-1.1-base
```

Questi comandi installeranno innanzitutto le librerie Qt e poi il pacchetto di base di KDE. Fatto questo, uscite e rientrate nel sistema in modo da impostare il giusto path e digitate:

```
install-kde-1.1-apps
```

Tale comando installerà i programmi applicativi.

Questa procedura d’installazione è discussa più approfonditamente nel file `"readme-redhat-rpms.txt"` che dovrete trovare tra file di KDE che avete scaricato.

Se tutto è andato per il verso giusto e KDE è stato installato senza la comparsa di messaggi di errore, potreste voler configurare KDE come window manager predefinito per tutti i vostri utenti (cioè quello che sarà avviato dopo aver digitato `"startx"`). In tal caso digitate, da “root”, quanto segue:

```
/opt/kde/bin/usekde userid
```

(Assicurandovi di rimpiazzare *user id* con un user id reale!)

Maggiori informazioni sul K Desktop Environment possono essere reperite sul sito di KDE <http://www.kde.org/>. Fate un salto alla sezione screenshot su <http://www.kde.org/kde2shots.html>.

Capitolo 6. Operazioni generali per l'amministrazione di sistema

6.1. Account di Root

L'account di "root" è quello più privilegiato in un sistema Unix. Da' infatti la possibilità di compiere tutte le operazioni di amministrazione di sistema, come quelle che permettono di aggiungere un account, cambiare le password degli utenti, esaminare i file di log, installare software, ecc.

Quando usate questo account dovete fare molta attenzione. L'account di "root" non ha alcuna restrizione di sicurezza. Ciò significa che è facile svolgere compiti di amministrazione. Comunque, il sistema presuppone che voi sappiate cosa state facendo, e quindi farà quello che gli chiederete di fare, senza porre alcuna domanda. È facile quindi, scrivendo male un comando, cancellare un file di sistema fondamentale.

Quando siete entrati come "root", o state agendo come esso, il prompt della shell è il carattere '#' (se usate bash). Questo simbolo è come un avvertimento della potenza di questo account.

La regola generale è quella di non entrare come "root" a meno che non sia assolutamente necessario. Qualora siate "root" scrivete i comandi con attenzione e ricontrollateli due volte prima di premere invio. Uscite da "root" non appena avete finito di svolgere i vostri compiti. Infine (questa vale per ogni account, ma in particolar modo per quello di "root"), tenete al sicuro la vostra password.

6.2. Creare gli Account degli utenti

Attenzione

(La documentazione si riferisce a SLACKWARE. Necessita di aggiornamenti per RED HAT)

Questa sezione presuppone che stiate utilizzando le Shadow password sul vostro sistema Linux. Se non è così, dovrete considerare l'idea di farlo, dato che può aumentare di molto la sicurezza del sistema. È piuttosto facile installare la suite Shadow e il file di password in formato non-shadow verrà automaticamente convertito nel nuovo formato.

Ci sono due cose da fare per creare l'account di un nuovo utente. Innanzi tutto bisogna creare l'account stesso e poi bisogna fornirgli un alias per l'indirizzo di posta elettronica (sul mio posto di lavoro, usiamo la convenzione "Nome.Cognome@nome.nostro.dominio")

Per creare l'account, decidete la username da assegnare all'utente. Essa deve essere ad massimo di 8 caratteri e, possibilmente, dovrebbe essere il cognome, oppure il cognome e l'iniziale del nome se l'account esiste già (lo script adduser controllerà e vi impedirà di creare un doppio account con lo stesso nome).

Vi verranno poi chieste altre informazioni: il nome completo dell'utente, lo user group (di solito il valore predefinito), uno user id # (assegnato automaticamente), la home directory (assegnata automaticamente), la shell, alcuni valori per la scadenza della password e, in ultimo, la password desiderata (che non verrà mostrata sullo schermo; per ragioni di sicurezza, fate in modo che l'utente scelga una password con lunghezza compresa tra i 6 e gli 8 caratteri).

Tutte le informazioni dovrebbe essere inserite in caratteri minuscoli, ad eccezione del nome completo dell'utente, che può essere inserito nel modo desiderato (es. Joe Smith), e della password. Ricordate poi ai vostri utenti che devono

inserire la username e la password nello "stesso formato" in cui sono stati inseriti nel processo di creazione degli utenti.

Ecco un esempio in cui aggiungeremo un utente di nome Joe Smith:

```
mail:~# /sbin/adduser
User to add (^C to quit): smith
That name is in use, choose another.
User to add (^C to quit): smithj
Editing information for new user [smithj]
Full Name: Joe Smith
GID [100]:
Checking for an available UID after 500
First unused uid is 859
UID [859]:
Home Directory [/home/smithj]:
Shell [/bin/bash]:
Min. Password Change Days [0]:
Max. Password Change Days [30]: 90
Password Warning Days [15]:
Days after Password Expiry for Account Locking [10]: 0
Password [smithj]:</ FL1539
Retype Password:</ FL1539
Sorry, they do not match.
Password:</> FL1539
Retype Password:</ FL1539

Information for new user [smithj]:
Name: Joe Smith
Home directory: /home/smithj
Shell: /bin/bash
Password: <hidden>
Uid: 859      Gid: 100
Min pass: 0   maX pass: 99999
Warn pass: 7   Lock account: 0
public home Directory: no
Type 'y' if this is correct, 'q' to cancel and quit the program,
or the letter of the item you wish to change: Y
```

Il passo successivo consiste nel creare l'alias per gli account di posta. Ciò dà la possibilità alle persone di usare il loro nome dell'account come indirizzo e-mail, oppure il loro nome completo (Nome.Cognome) affinché il mondo esterno possa indovinare "facilmente" il loro indirizzo e-mail al momento del primo contatto.

Per aggiungere gli alias di posta, editate il file "/etc/aliases" come segue:

```
mail# pico -w /etc/aliases
```

Aggiungete il nuovo alias in fondo al file. Il formato per l'alias è:

```
First.Lastname:username
```

Chiedete all'utente se ha qualche preferenza (es. Joseph.Smith oppure Joe.Smith). Per l'utente Joe Smith dovremmo aggiungere:

```
Joe.Smith:smith
```

Quando avete finito, premete <Ctrl>-<x> e salvate il file. Digitate, poi, "newaliases" per aggiornare il database degli alias.

A questo punto l'account dell'utente è stato creato ed è pronto per essere usato. Potrebbe essere una buona idea ricordare all'utente che la username e la password devono essere inseriti in caratteri minuscoli, e qual è il suo indirizzo e-mail (es. "Joe.Smith@mail.mydomain.name").

6.3. Cambiare le password degli utenti

Per cambiare la password di un utente, usate "su" ed entrate come "root" e digitate "passwd user" (dove user è la username della password che volete cambiare). Il sistema vi chiederà di inserire una password, che non apparirà sullo schermo quando la digiterete.

Potete cambiare anche la vostra password digitando "passwd" (senza specificare una username). Vi verrà chiesta la vecchia password e, subito dopo, quella nuova.

6.4. Disabilitare gli account degli utenti

Per disabilitare gli account degli utenti, editate, come root, il file "/etc/shadow" (se utilizzate le shadow password; in caso contrario editate il file "/etc/passwd"), e sostituite la password (in forma criptata) con il carattere asterisco "*". Tutte le password Unix, indifferentemente dalla lunghezza (fino a un massimo di 8 caratteri), sono memorizzate, nel file delle password, con stringhe criptate di 13 caratteri. Quindi, sostituendo la password con l'asterisco "*", sarà impossibile per l'utente accedere al sistema.

Nota: Questo metodo comporta l'assegnazione di una nuova password all'utente qualora decidiate di riattivare l'account dopo aver sostituito la password con l'asterisco. Una soluzione molto gettonata tra gli amministratori di sistema è quella di anteporre l'asterisco "*" alla password criptata. Qualora dobbiate riattivare l'account basterà togliere l'asterisco.

Per maggiori informazioni sui file "/etc/passwd" e "/etc/shadow" si veda la Sezione 6.6 di seguito.

6.5. Rimuovere gli account degli utenti

Potrebbe succedere che vogliate eliminare completamente dal vostro server l'account di un utente.

Se siete un utente Red Hat, la maniera più facile per compiere questa operazione è quella di usare il comando "userdel", da digitare come "root". Ecco un esempio:

```
/usr/sbin/userdel baduser
```

Il comando sopra rimuoverà l'utente "baduser" dal file "/etc/passwd" e, se utilizzate il formato Shadow password (sarebbe consigliato farlo; si veda la la Sezione 6.6 per maggiori dettagli), dal file "/etc/shadow".

Nota: "/etc/group" non viene modificato, per evitare di rimuovere un gruppo al quale potrebbero appartenere anche altri utenti. Se ciò vi dà fastidio, potete editare il file group e rimuovere l'utente manualmente.

Se volete rimuovere anche l'home directory dell'utente, aggiungete l'opzione "-r" al comando "userdel". Per esempio:

```
/usr/sbin/userdel -r baduser
```

Vi suggerisco di non rimuovere direttamente un account, ma prima *disabilitatelo*, specialmente se state lavorando con un server aziendale con molti utenti. Dopo tutto, l'ex utente potrebbe un giorno chiedere di usare di nuovo il suo account, oppure chiedere di avere uno o due file memorizzati nella sua home directory. Oppure un *nuovo* utente (come, ad esempio, un nuovo impiegato che rimpiazza il precedente) potrebbe volere accedere ai file di quest'ultimo. In "ogni caso", accertatevi di avere sempre una copia di backup dell'home directory dell'ex-utente. Si Veda la Sezione 6.4 per informazioni su come disabilitare un account, e al Capitolo 8 per informazioni sulle procedure di backup.

6.6. Le password di Linux e il formato shadow

I sistemi Unix tradizionali mantengono le informazioni sugli account degli utenti, comprese le password criptate, in un file di testo chiamato `/etc/passwd`. Poiché tale file viene utilizzato da molti strumenti (come "ls") per visualizzare la proprietà dei file o altro, confrontando gli user id # con le user name, deve necessariamente essere leggibile. Ciò comporta alcuni rischi per la sicurezza.

Un altro modo per memorizzare le informazioni degli account, quello che io uso sempre, è utilizzare il formato shadow password. Esattamente come quello tradizionale, questo metodo memorizza le informazioni sugli account nel file `/etc/passwd`. Soltanto che la password viene memorizzata con un singolo carattere "x" (cioè non viene memorizzata veramente in questo file). Un secondo file, chiamato `/etc/shadow`, contiene le password criptate oltre ai valori di scadenza dell'account o della password, ecc. Il file `/etc/shadow` può essere letto solo da chi ha l'account di root, quindi molto più sicuro.

Mentre alcune distribuzioni di Linux vi obbligano ad installare la Shadow Password Suite che vi permette di utilizzare il formato shadow, Red Hat fa le cose più semplice. Per passare da un formato all'altro, digitate (come root):

```
/usr/sbin/pwconv Per passare al formato shadow  
/usr/sbin/pwunconv Per tornare al formato tradizionale
```

Con le shadow password, il file `/etc/passwd` contiene le informazioni sugli account e appare così:

```
smithj:x:561:561:Joe Smith:/home/smithj:/bin/bash
```

Ogni riga contiene campi separati dal carattere ":" e sono i seguenti:

- Username, fino a 8 caratteri. Case-sensitive e, di solito, tutti caratteri minuscoli.
- Una "x" nel campo password. Le Password sono memorizzate nel file `/etc/shadow`.
- User id numerico, assegnato dallo script "adduser". Unix utilizza questo campo oltre a quello, del gruppo, che segue per stabilire quali file appartengano all'utente.
- Group id numerico. Red Hat utilizza gli id di gruppo in un'unica maniera per aumentare la sicurezza sui file. Di solito l'id del gruppo è uguale allo User id.
- Nome completo dell'utente. Non sono sicuro di quale sia la lunghezza massima per questo campo, ma vi consiglieri di non usare più di 30 caratteri.
- La home directory dell'utente. Di solito `/home/username` (nell'esempio: `/home/smithj`). Tutti i file personali dell'utente, le pagine web, le e-mail inviate, sono memorizzati qui.

- Lo "shell account" dell'utente. Spesso impostato a `/bin/bash` che fornisce l'accesso alla shell bash (quella che preferisco).

Se non volete fornire degli shell account ai vostri utenti, potreste creare uno script chiamato `/bin/sorrysh`, per esempio, che mostrerà un messaggio di errore e non farà accedere l'utente. Impostate questo script come la loro shell predefinita.

Nota: Se l'account ha bisogno dell'"FTP" per aggiornare le pagine web o per altro, allora dovrete impostare lo shell account a `/bin/bash` e poi dovrete impostare dei permessi speciali nella home directory dell'utente per impedirgli di accedere alla shell. Si veda la Sezione 7.1 per maggiori dettagli.

Il file `/etc/shadow` contiene la password e le informazioni sulla scadenza degli account degli utenti, e appare così:

```
smithj:Ep6mckrOLChF.:10063:0:99999:7:::
```

Come già visto in precedenza, anche qui i campi sono separati dal carattere ":", e sono i seguenti:

- Username, massimo 8 caratteri. Case-sensitive e, di solito, tutti minuscoli. Con corrispondenza diretta alla username presente nel file `/etc/passwd`.
- Password, 13 caratteri criptati. Se il campo è vuoto (es. `::`) allora vuol dire che non c'è bisogno di password per accedere al sistema (caldamente sconsigliato); se il campo contiene un asterisco (es. `:*`) allora l'account è disabilitato.
- Il numero di giorni (dal 1° gennaio 1970) dall'ultima modifica della password.
- Il numero di giorni che devono passare prima che la password possa essere modificata (0 indica che può essere cambiata in qualsiasi momento)
- Il numero di giorni trascorsi i quali la password *deve* essere cambiata (99999 indica che l'utente può mantenere la stessa password per molti anni)
- Il numero dei giorni dopo i quali bisogna avvertire l'utente che la password è scaduta (7 per un'intera settimana).
- Il numero dei giorni dopo i quali la password scade e l'account viene disabilitato.
- Il numero di giorni dal 1° Gennaio 1970 trascorsi dalla disabilitazione di un account.
- Un campo riservato a possibili usi futuri.

6.7. Spegnimento e riavvio del sistema

Per spegnere il sistema da terminale, passate all'account di "root" (anche con il comando "su"). Quindi digitate `/sbin/shutdown -r now`. Potrebbe volerci un po' di tempo per terminare tutti i processi, ma alla fine Linux si chiuderà. Il computer si riavvierà da solo. Se avete di fronte la console, un metodo alternativo e più veloce consiste nel premere `<Ctrl>-<Alt>-`.

Potete anche spegnere il sistema senza che esso si riavvii automaticamente. Questo sistema può essere utile se, ad esempio, dovete togliere corrente al sistema e spostarlo da qualche altra parte. Per far ciò, sempre da "root", digitate `/sbin/shutdown -h now`. Linux si arresterà e mostrerà il messaggio "System halted". A questo punto potete togliere la corrente al computer.

Probabilmente è una buona idea spegnere il sistema solo quando siete alla console. Sebbene possiate farlo anche da remoto, se qualcosa va storto e il sistema non si riavvia correttamente, esso non sarà disponibile fin quando non agirete direttamente sull'unità di sistema (comunque, io non ho mai avuto problemi del genere).

Subito dopo il boot, Linux si avvierà automaticamente e caricherà tutti i servizi necessari compreso il supporto per il networking e per i servizi Internet.

Suggerimento: Suggerimento: Se volete dare una sorta di preavviso agli utenti online (cioè quelli che hanno effettuato l'accesso), potete sostituire la parola "now" con un valore di tempo. Potete anche personalizzare il messaggio di avvertimento. Per esempio: `/sbin/shutdown -r +5 Aggiornamento hardware` informerà gli utenti dell'imminente shutdown per il motivo specificato nel messaggio. Avranno poi, ad un certo intervallo di tempo l'uno dall'altro, ulteriori avvertimenti di chiedere i file e uscire dal sistema prima del verificarsi dello shutdown.

Capitolo 7. Questioni di amministrazione e configurazioni personalizzata

Sia per uso personale e sia sul lavoro, sono stato in grado di iniziare con una installazione standard di Linux Red Hat e fornire servizi apportando soltanto piccole modifiche (o anche nessuna) alle impostazioni di configurazione predefinite.

Comunque, avevo bisogno di fare piccoli cambiamenti per servizi extra, come Internet o servizi di condivisione file e stampanti, di cui avevo bisogno sul mio posto di lavoro. L'amministratore locale dovrebbe essere a conoscenza di quanto segue:

- Il file `/etc/rc.d/rc.local` viene eseguito all'avvio del sistema e contiene i servizi extra che avete aggiunto al vostro server e che devono essere avviati al momento del boot.
- Date un'occhiata in `/etc` per ogni cambiamento specifico di cui potreste aver bisogno:
 - `/etc/inetd.conf` (Dovreste assicurarvi che i servizi non necessari siano disabilitati, come `finger`, `echo`, `chargen`; inoltre potete effettuare dei cambiamenti relativi ai servizi di cui avete bisogno.)
 - `/etc/exports` (contiene una lista di host a cui è permesso montare i volumi NFS; si veda la Sezione 7.6 per maggiori informazioni)
 - `/etc/organization`, `/etc/nntpserver`, `/etc/NNTP_INEWS_DOMAIN` (impostateli in maniera appropriata)
 - `/etc/lilo.conf` (contiene informazioni sul boot loader LILO -- il processo che carica il kernel di Linux al momento del boot; si veda la Sezione 4.8 per maggiori informazioni)
 - `/etc/sudoers` (una lista di utenti a cui devono essere dati speciali privilegi, insieme ai comandi che possono utilizzare)
 - `/etc/named.boot` ((per l'uso di DNS; si veda la Sezione 7.2 per maggiori informazioni))
- Tutte le cose in `/usr/local/` (e subdirectory) sono pacchetti extra o modificazioni di quelli esistenti che avete installato qui, se avete installato tarball invece di RPM. (O almeno dovrete averle installate da qui). Questi file, soprattutto in `/usr/local/src/`, dovrebbero essere mantenuti aggiornati. Si veda il Capitolo 10 per maggiori informazioni.

7.1. Amministrazioni di un web server e di un HTTP caching proxy

Attenzione

(ATTENZIONE: NON FATE CASO A QUESTA SEZIONE!)

1. Create un utente Internet come fate normalmente. L'account di "shell" dovrebbe essere `/bin/bash` (dato che FTP richiede una shell valida).
2. `"cd /home ; chown root.root theuser"` Ciò rende la directory di "theuser" di proprietà di root, per ragioni di sicurezza.
3. `"cd /home/theuser ; mkdir www ; chown theuser.theuser"` questo crea la directory "www" directory, e imposta la proprietà in modo da poter leggerci e scriverci.

4. `echo "exit" > .profile` Questo crea un file `.profile` contenente solo la riga `exit`. Se l'utente prova a connettersi con telnet, verrà disconnesso immediatamente.
5. Fate un `ls -l` e assicuratevi che vi siano solo 2 file nella directory (senza contare `..` e `.`):
 - `.profile` (di proprietà di root.root)
 - `www` (di proprietà di theuser.theuser)

Tutti gli altri file possono essere cancellati (cioè `rm .less ; rm .lessrc`)

6. Se l'utente ha bisogno di poter inviare e-mail, potreste creare un file `.forward` che contiene semplicemente, come prima e unica riga, la giusta e-mail.

Questo è tutto. L'utente può usare l'FTP per aggiornare le pagine.

7.2. Configurazione e amministrazione di un Domain Name Server (DNS)

Sul mio posto di lavoro, usiamo Linux come server DNS. E funziona proprio bene. Questa sezione descriverà la configurazione delle tabelle DNS usando il pacchetto BIND 8.x incluso nella distribuzione Red Hat.

Nota: La versione 5.1 e precedenti di Red Hat 5.1 usavano il pacchetto BIND 4.x, il quale utilizzava un formato leggermente diverso per il file di configurazione. BIND 8.x offre maggiori funzionalità rispetto a BIND 4.x, e dato che 4.x non viene più sviluppato, dovrete probabilmente aggiornare il pacchetto BIND all'ultima versione. Installate semplicemente il pacchetto RPM di BIND (si veda la Sezione 10.1 per maggiori informazioni sull'uso dell'utilità) e convertite poi il vostro file di configurazione nel nuovo formato.

Fortunatamente il processo di conversione è semplice. Nella directory della documentazione che accompagna BIND (per esempio, `/usr/doc/bind-8.1.2/` per BIND versione 8.1.2), c'è un file chiamato `named-bootconf.pl`, che è un programma Perl eseguibile. Posto che abbiate Perl installato sul vostro sistema, potete usare questo programma per fare la conversione. Digitale i seguenti comandi da root:

```
cd /usr/doc/bind-8.1.2
./named-bootconf.pl < /etc/named.boot > /etc/named.conf
mv /etc/named.boot /etc/named.boot-obsolete
```

Dovreste avere adesso un file `/etc/named.conf` che funziona con BIND 8.x. Le vostre tabelle DNS non avranno bisogno di modifiche per la nuova versione di BIND, poiché il formato rimane lo stesso.

La configurazione dei servizi DNS sotto Linux richiede i seguenti passi:

1. Per attivare i servizi DNS, il file `/etc/host.conf` dovrebbe apparire come questo:

```
# Lookup names via /etc/hosts first, then by DNS query
order hosts, bind
# We don't have machines with multiple addresses
multi on
# Check for IP address spoofing
nospoof on
# Warn us if someone attempts to spoof
alert on
```

L'attivazione di un controllo extra per lo spoofing migliora le prestazioni dei lookup DNS (anche di pochissimo), quindi se non vi importa di ciò potrete disabilitare "nospool" e "alert".

2. Configurate il file "/etc/hosts" secondo i vostri bisogni. Di solito c'è poco da fare qui, ma per migliorare le prestazioni potete aggiungere qualunque host a cui accedete spesso (come i server locali) per evitare di compiere lookup DNS su di essi.
3. Il file "/etc/named.conf" deve essere configurato in modo da puntare alle vostre tabelle DNS come nell'esempio sotto.

Nota: (Gli indirizzi IP sono solo esempi e devono essere sostituiti con quelli della vostra classe!):

```
options {
// le tabelle DNS si trovano nella directory /var/named
    directory "/var/named";

// Inoltra ogni richiesta non risolta al nostro ISP name server
    // (Questo è solo un esempio di indirizzo IP -- non usatelo!)
forwarders {
123.12.40.17;
};

/*
 * Se c'è un firewall tra voi e i nameserver con cui volete dialogare
 *   * dovete decommentare la direttiva query-source
 *   * sotto. Versioni precedenti di BIND
 *   * usavano la porta 53, ma BIND 8.1 usa una porta senza privilegi
 *   * predefiniti.
 */
// query-source address * port 53;
};

// Attiva il caching e carica le informazioni del root server
zone "named.root" {
type hint;
file "";
};

// Tutte le nostre informazioni DNS sono memorizzate in /var/named/mydomain_name.db
// (es. if mydomain.name = foobar.com then use foobar_com.db)
zone "mydomain.name" {
type master;
file "mydomain_name.db";
allow-transfer { 123.12.41.40; };
};

// Lookup inversi per 123.12.41.*, .42.*, .43.*, .44.* class C's
// (sono solo esempi di Classe C -- non usateli!)
zone "12.123.IN-ADDR.ARPA" {
type master;
```

```
file "123_12.rev";
allow-transfer { 123.12.41.40; };
};

// Lookup inversi per 126.27.18.*, .19.*, .20.* class C's
// (sono solo esempi di Classe C -- non usateli!)
zone "27.126.IN-ADDR.ARPA" {
type master;
file "126_27.rev";
allow-transfer { 123.12.41.40; };
};
```

Suggerimento: Suggerimento: Prendete nota delle opzioni di `allow-transfer`, che limitano i trasferimenti di zona DNS a un dato indirizzo IP. Nel nostro esempio, permettiamo all'host 123.12.41.40 (probabilmente uno slave DNS server nel nostro dominio) di richiedere trasferimenti di zone. Se omettete questa opzione, chiunque su Internet potrà richiedere tali trasferimenti. Dato che queste informazioni vengono spesso usate da spammer e IP spoofer, vi raccomando caldamente di limitare i trasferimenti di zona eccetto per il vostro slave DNS server, oppure usate l'indirizzo di loopback "127.0.0.1".

4. Adesso potete impostare le vostre tabelle DNS nella directory `"var/named/"` come configurato al punto tre nel file `"etc/named.conf"`. Configurare i file del database DNS per la prima volta è il compito più gravoso e va oltre gli scopi di questa documentazione. Ci sono molte guide sia online sia in formato cartaceo. Per maggiori informazioni potete far riferimento ad esse. Comunque vi mostro qualche esempio:

Alcune informazioni presenti nel file di forward lookup `"var/named/mydomain_name.db"`:

```
; This is the Start of Authority (SOA) record. Contains contact
; & other information about the name server. The serial number
; must be changed whenever the file is updated (to inform secondary
; servers that zone information has changed).
    @ IN SOA mydomain.name. postmaster.mydomain.name. (
19990811 ; Serial number
3600 ; 1 hour refresh
300 ; 5 minutes retry
172800 ; 2 days expiry
43200 ) ; 12 hours minimum

; List the name servers in use. Unresolved (entries in other zones)
; will go to our ISP's name server isp.domain.name.com
IN NS mydomain.name.
IN NS isp.domain.name.com.

; This is the mail-exchanger. You can list more than one (if
; applicable), with the integer field indicating priority (lowest
; being a higher priority)
IN MX mail.mydomain.name.

; Provides optional information on the machine type & operating system
; used for the server
IN HINFO Pentium/350 LINUX
```

```
; A list of machine names & addresses
spock.mydomain.name.    IN A    123.12.41.40    ; OpenVMS Alpha
mail.mydomain.name.    IN A    123.12.41.41    ; Linux (main server)
kirk.mydomain.name.    IN A    123.12.41.42    ; Windows NT (blech!)

; Including any in our other class C's
twixel.mydomain.name.  IN A    126.27.18.161   ; Linux test machine
foxone.mydomain.name.  IN A    126.27.18.162   ; Linux devel. kernel

; Alias (canonical) names
gopher IN CNAME mail.mydomain.name.
ftp IN CNAME mail.mydomain.name.
www IN CNAME mail.mydomain.name.
```

Alcune informazioni nel file di reverse lookup `"/var/named/123_12.rev"`:

```
; This is the Start of Authority record. Same as in forward lookup table.
@ IN SOA mydomain.name. postmaster.mydomain.name. (
19990811 ; Serial number
3600 ; 1 hour refresh
300 ; 5 minutes retry
172800 ; 2 days expiry
43200 ) ; 12 hours minimum

; Name servers listed as in forward lookup table
IN NS mail.mydomain.name.
IN NS isp.domain.name.com.

; A list of machine names & addresses, in reverse. We are mapping
; more than one class C here, so we need to list the class B portion
; as well.
40.41 IN PTR    spock.mydomain.name.
41.41 IN PTR    mail.mydomain.name.
42.41 IN PTR    kirk.mydomain.name.

; As you can see, we can map our other class C's as long as they are
; under the 123.12.* class B addresses
24.42 IN PTR    tsingtao.mydomain.name.
250.42 IN PTR   redstripe.mydomain.name.
24.43 IN PTR    kirin.mydomain.name.
66.44 IN PTR    sapporo.mydomain.name.
```

```
; No alias (canonical) names should be listed in the reverse lookup
; file (for obvious reasons).
```

Può essere creato qualunque altro file di lookup inverso che ha bisogno di mappare gli indirizzi in un diversa classe B (come 126.27.*), e dovrebbe essere simile all'esempio sopra.

5. Assicuratevi che il demone `named` sia in esecuzione. Questo demone viene, di solito, avviato dal file `"/etc/rc.d/init.d/named"` al momento del boot del sistema. Potete anche avviarlo e fermarlo manualmente; digitate rispettivamente `"named start"` e `"named stop"`.

6. Qualunque cambiamento venga fatto alle tabelle DNS, il server DNS deve essere riavviato digitando `"/etc/rc.d/init.d/named restart"`. Se volete, poi, testare i cambiamenti che avete apportato, potete utilizzare uno strumento come `"nslookup"` per interrogare la macchina che avete aggiunto o cambiato.

Maggiori informazioni relative alla configurazione dei servizi DNS possono essere reperite nel *"DNS-HOWTO"* su <http://metalab.unc.edu/Linux/HOWTO/DNS-HOWTO-5.html>. [NdT: disponibile in italiano su <http://it.tldp.org/HOWTO/DNS-HOWTO-5.html>]

7.3. Autenticazione degli utenti internet con TACACS

Sul mio posto di lavoro, per l'autenticazione TACACS degli utenti Internet (che si connettono ai nostri modem che sono a loro volta collegati a un paio di access server Cisco 250x), utilizziamo la versione Vikas di `"xtacacsd"`.

Dopo aver compilato e installato il pacchetto Vikas (le versioni più recenti si trovano su <ftp://ftp.navya.com/pub/vikas>; non credo sia disponibile in formato RPM), dovrete aggiungere questa riga al file `"/etc/inetd.conf"` in modo che il demone venga caricato dal demone `inetd` ogni volta che si riceve una richiesta TACACS.

```
# TACACS is a user authentication protocol used for Cisco Router products.  
tacacs dgram udp wait root /etc/xtacacsd xtacacsd -c /etc/xtacacsd-conf
```

Dopo di che, dovrete editare il file `"/etc/xtacacsd-conf"` e personalizzarlo, se necessario, per il vostro sistema (comunque potrete utilizzare, probabilmente, le impostazioni predefinite così come sono).

Nota: Se state usando le shadow password (si veda la Sezione 6.6 per maggiori dettagli), avrete qualche problema con questo pacchetto. Sfortunatamente, PAM (Pluggable Authentication Module), che Red Hat utilizza per l'autenticazione degli utenti, non è supportato da questo pacchetto. La mia soluzione a questo problema è tenere un file `"passwd"` separato in `"/usr/local/xtacacs/etc/"` che combacia con quello presente in `/etc/` ma non è in formato shadow. Se scegliete questo metodo ricordatevi di impostare i permessi sull'altro file delle password in modo che sia leggibile solo da root:

```
chmod a-wr,u+r /usr/local/xtacacs/etc/passwd
```

Se usate davvero il formato shadow, dovrete certamente editare il file `"/etc/xtacacsd-conf"` e la posizione del file di password non shadow (posto che abbiate usato il metodo che vi ho suggerito sopra).

Il passo successivo è quello di configurare il vostro access server per autenticare i login, per i dispositivi desiderati (come i dial-up modem), con TACACS. Ecco un'esempio di come viene fatto:

```
mail:/tftpboot# telnet xyzrouter  
  
Escape character is '^]'.  
User Access Verification  
Password: ****  
xyzrouter> enable  
Password: ****  
xyzrouter# config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
xyzrouter(config)# tacacs-server attempts 3  
xyzrouter(config)# tacacs-server authenticate connections
```

```
xyzrouter(config)# tacacs-server extended
xyzrouter(config)# tacacs-server host 123.12.41.41
xyzrouter(config)# tacacs-server notify connections
xyzrouter(config)# tacacs-server notify enable
xyzrouter(config)# tacacs-server notify logouts
xyzrouter(config)# tacacs-server notify slip
xyzrouter(config)# line 2 10
xyzrouter(config-line)# login tacacs
xyzrouter(config-line)# exit
xyzrouter(config)# exit
xyzrouter# write
Building configuration...
[OK]
xyzrouter# exit
```

Connection closed by foreign host.

Tutti i messaggi di log relativi all'attività di TACACS saranno registrati in `"/var/log/messages"` per un'attenta lettura.

7.4. Servizi file e stampa in stile Windows con Samba

Linux può offrire servizi SMB (per esempio condivisioni in rete di file e stampante in stile WfW, Win95 e NT), usando il pacchetto Samba. Questa sezione descriverà come configurare le risorse condivise e come accedervi da macchine client.

Il pacchetto Samba è incluso nella distribuzione Red Hat, potete controllare se l'avete installato, e qual è la versione che avete, digitando:

```
rpm -q samba
```

Se non è installato, allora dovrete farlo usando l'utilità RPM. Si veda la Sezione 10.1 per informazioni su come fare.

I file più importanti di Samba dei quali dovrete occuparvi sono:

`/etc/smb.conf`

File di configurazione di Samba dove sono impostati i parametri relativi alle risorse condivise ed ad altre cose (si veda di seguito)

`/var/log/samba/`

Posizione del file di log di Samba

`/home/samba/`

Posizione suggerita per impostare le risorse condivise. Comunque, potete scegliere la posizione nel file system in cui avete più spazio e dove possiate sistemare comodamente i vostri file. Personalmente, imposto una grande partizione montata su `/archive/` e metto lì le mie condivisioni.

Il file `"/etc/smb.conf"` contiene le informazioni di configurazione sulle condivisioni di file e stampante. Le prime righe del file contengono le direttive di configurazione globale, che sono comuni a tutte le risorse condivise (salve che vengano ignorate su basi per-share), seguite dalle sezioni share.

L'installazione di Samba include un file `smb.conf` predefinito come può essere adatto ai vostri bisogni e necessita di pochi cambiamenti.

Ecco un esempio di questo file (che ho personalizzato pesantemente per mostrarvi alcune delle più importanti, e interessanti, opzioni):

```
# Righe comuni a tutti le parti (a meno che non vengano riscritte)
[global]
  # Numero di minuti di inattività prima che il client venga disconnesso
  # per evitare il consumo di risorse. Molti client verranno riconnessi
  # automaticamente, quindi è una buona idea attivare questa opzione.
  dead time = 10

  # Non permette agli utenti di connettersi come "root". :-)
  invalid users = root

# Specifica il guest account (share che non necessitano
# di password per connettersi. La username deve essere valida
# nel file /etc/passwd.
guest account = guest

# Specifica dove i file di log devono essere scritti. Il suffisso "%m"
# significa che i file di log verranno creati nel formato
# log.machine-name (es. "log.twixel")
log file = /usr/local/samba/logs/log.%m

# dimensione massima dei log, in Kilobytes.
max log size = 1000

# Password level 3 significa che il carattere minuscolo o maiuscolo non è un
# problema quando s'inserisce una password. Potrebbe essere un po' meno
# sicuro rispetto al livello 1 o 2, ma è un buon compromesso.
password level = 3

# Specifica che tutti gli share devono comparire nella browse list
# (Viene ignorata se su basi per-share).
browseable = yes

# Se attivata, potrete vedere le connessioni attive usando il
# comando "smbstatus".
status = yes

# Il livello di informazioni di debugging registrate nei file di log.
# Valori più alti generano maggiori informazioni (le quali, spesso,
# probabilmente non servono a molto).
debug level = 2

# Invierà ogni messaggio ricevuto sul server in stile Windows "POPUP"
# al postmaster via e-mail. Non molto utile, ma interessante dimostrazione
# di quello che può essere fatto.
message command = /bin/mail -s 'Message from %f on %m' postmaster < %s; rm %s &

# Questa è una forma di caching che, se attivata, può migliorare
```

```
# la lettura dei file.
read prediction = true

# Una lista di servizi che possono essere aggiunti automaticamente alla
# browse-list.
auto services = cdrom

# La posizione del vostro file "printcap", un file di testo che
# contiene le definizioni delle vostre stampanti.
printcap name = /etc/printcap

# Se attivata, tutte le stampanti nel file /etc/printcap saranno caricate
# nella browse-list.
load printers = yes

# Il comando per la stampa sotto Linux.
print command = lpr -r -P%p %s

# il comando mediante cui ottenere informazioni sulla coda di stampa
# (status della stampante).
lpq command = lpq -P%p

# Il comando per eliminare dalla coda, lavori di stampa
# non voluti.
lprm command = lprm -P%p %j

# Il livello al quale Samba parteciperà alle elezioni per il browsing.
# Generalmente impostata con un "valore alto" per fare in modo che Samba
# vinca sempre nella rete. :-)
os level = 34

# Qui stanno le share personali degli utenti. Se la username del client
# corrisponde a quella del server, essi possono accedere alla loro home
# directory (se inseriscono la password corretta).
[homes]
# I commenti appaiono nella browse list.
comment = Home Directories

# Questa confronta la username del client con quella della share.
# Se non conbaciano, non verrà mostrato alcuno share nella browse
# list.
user = %S

# Il percorso della share. Per esempio, "smithj" dovrebbe essere mappato
# "/home/smithj"
path = /home/%S

# Se attivata, permette l'accesso in lettura/scrittura alle share.
writeable = yes

# Solo un sinonimo inverso di "writeable". Non abbiamo davvero
# bisogno di tutti e due. :-)
read only = no
```

```
# Tenetelo disattivato in modo che ci voglia una password per accedere alle
# share.
public = no

# Non vogliamo che questa share (dopo tutto è privata) appaia nella
# browse-list degli altri utenti.
browseable = no

# Questa è una stampante accessibile pubblicamente, chiamata "hp_laser". Appare
# nelle browse list e può essere usata da ogni client.
[hp_laser]
# Il commento che appare nella browse-list.
comment = Main office printer (HP Laserjet 400)

# Lo username di chi può accedervi (guest significa tutti gli utenti).
user = guest

# Tutti i file di stampa generati saranno prima creati
# nella directory /tmp.
path = /tmp

# Non permettete la creazione di file eccetto attraverso le code di stampa.
writeable = no

# Imposta i permessi di conseguenza -- solo root accede
# ai processi di stampa.
create mode = 0700

# Se non attivato non c'è bisogno di password per accedere alle risorse.
public = yes

# Se attivato indica che questa è una stampante condivisa.
printable = yes

# Qui di seguito si fornisce l'accesso al un dispositivo CD-ROM.
[cdrom]
comment = Shared CD-ROM drive on Linux
user = guest
path = /cdrom
writeable = no
read only = true
browseable = yes
public = yes
guest ok = yes
```

Suggerimento: Suggerimento: Recenti versioni di Samba, dalla 2.0 in poi, forniscono un'ottima utilità di configurazione chiamata "swat", che rende tutto il processo molto più user-friendly. L'utilità si mette in ascolto sulla porta 901 TCP del vostro server, quindi per usarla puntato il vostro browser web favorito come segue:

```
mydomain.name:901
```

(Ovviamente, per usare SWAT avrete bisogno che sia in funzione un web server, come Apache. Si veda la Sezione 7.1 per maggiori informazioni)

Le ultime versioni di Samba hanno anche altre importanti caratteristiche in più rispetto alle versioni precedenti alla 2.0. È bene che aggiorniate tale pacchetto.

Un client deve avere un TCP/IP network stack in esecuzione per connettersi alle risorse condivise. Inoltre, per far funzionare il browsing, il protocollo TCP/IP deve essere legato a NETBEUI. Sotto Windows 95 ciò può essere configurato dall'icona "Network" del pannello di controllo.

Posto che il client sia stato configurato correttamente, dovreste poter vedere le condivisioni in "Risorse di rete" (o equivalente se non state usando Window95/NT). Potete accedere ai drive o da risorse di rete o digitando il loro percorso assoluto (es. "\\mail\cdrom"). Se la condivisione richiede una password, ve ne verrà chiesta una.

Maggiori informazioni su Samba possono essere reperite sulla Samba Home Page (<http://samba.anu.edu.au/samba/>).

7.5. Servizi file e di stampa in stile Macintosh con Netatalk

Linux può offrire anche servizi di condivisione con Apple (es. condivisione di file e stampante con Macintosh), usando il pacchetto Netatalk. Questa sezione descriverà come configurare le condivisioni, e come accedervi da macchine client.

Per usare Netatalk, dovrete avere, nel vostro kernel, il supporto per l'Appletalk networking. Gli stock kernel di Red Hat, di solito, includono questo supporto come modulo, oppure potete compilare un vostro kernel con tale supporto.

Nota: Assicurate che il supporto per Appletalk sia compilato come un *modulo* e non incluso come parte del kernel (si veda la Sezione 10.4 per informazioni su come aggiornare e personalizzare kernel Linux). Altrimenti, incontrerete difficoltà ad fermare e poi riavviare il demone Netatalk.

Una volta che vi siete assicurati che il vostro kernel supporti Appletalk, dovrete installare il pacchetto Netatalk. Poiché esso non è incluso nella distribuzione di Red Hat, dovrete scaricarne una copia. Il pacchetto si può trovare sul sito "contrib" di Red Hat su <ftp://ftp.redhat.com/contrib/libc6/i386/>.

Dopo averlo installato, potreste dover modificare uno o più file di configurazione in `/etc/atalk/`. La maggior parti di essi contiene esempi di configurazione e quindi c'è meno bisogno di documentarsi. I file sono:

`config`

Questo file contiene le informazioni di configurazione per mettere a punto il vostro demone Netatalk. Contiene variabili d'ambiente, e questo file viene letto dallo script di startup di Netatalk prima che il servizio venga avviato. Potete specificare il numero di connessioni simultanee, se consentire o meno guest login, ecc. Sicuramente vorrete modificare questo file a seconda delle vostre esigenze.

`atalk.conf`

Questo file contiene informazioni su quale interfaccia di rete usare, oltre al routing di Appletalk, name registration e altre informazioni correlate. Non avrete probabilmente bisogno di modificarlo; le informazioni sulla rete saranno rilevate e aggiunte a questo file la prima volta che avvierete il server Netatalk. Comunque, potreste voler aggiungere il nome del vostro server.

Nota: Digitate `man atalkd` per maggiori informazioni su questo file.

afpd.conf

Questo file vi permette di specificare parametri aggiuntivi che saranno passati a Netatalk per mezzo di opzioni a riga di comando. Potete specificare su quale porta e a quale indirizzo IP volete far girare il server Netatalk, aggiungere un messaggio di login che verrà mostrate agli utenti che si connettono, e altre opzioni. Non avrete bisogno di modificare questo file.

Nota: *Digitate "man afpd" per maggiori informazioni su questo file.*

papd.conf

Il file contiene le informazioni di configurazione per attivare la possibilità che gli utenti Mac possono eseguire lavori di stampa con le stampanti condivise. Non l'ho provato, quindi non posso darvi consigli.

Nota: *Digitate "man papd" per maggiori informazioni su questo file.*

AppleVolumes.default

Questo file elenca i file condivisi disponibili che un utente Mac vedrà dopo il login. Per attivare una condivisione, inserite il percorso della directory del file, seguito da un descrizione testuale. Per esempio:

```
~ "Home"  
/archive/busdept "Business Department Common Files"
```

(Quanto sopra offrirà due condivisioni per le connessioni degli utenti Mac: la loro home directory e l'area condivisa del business department.)

Suggerimento: Suggerimento: A Un buon trucco è di impostare le condivisioni con gli stessi percorsi sotto Samba, che offrirà la condivisione di file indipendentemente dalla piattaforma sia essa Mac o Windows. Si veda la Sezione 7.4 per informazioni sull'uso di Samba.

AppleVolumes.system

Anche questo file, come "AppleVolumes.default", contiene la lista dei file condivisi, la differenza è che questi saranno disponibili per *tutti* gli utenti, senza tener conto del fatto che essi abbiano o no effettuato un login. Contiene anche la mappatura di tipi di file. Non avrete bisogno di modificare tale file, a meno che non vogliate rendere disponibili a tutti altre condivisioni; è probabilmente un cattiva idea per la maggior parte della gente.

Una volta impostato tutto con le appropriate configurazioni, potete avviare i servizi Netatalk manualmente, digitando:

```
/etc/rc.d/init.d/atalk start
```

(I sistemi dovrebbero avviarsi automaticamente al boot di sistema).

Maggiori informazioni su Netatalk si possono ottenere dalla Home Page di Netatalk su <http://www.umich.edu/~rsug/netatalk/>. In più, potete consultare il Linux Netatalk HOWTO disponibile su <http://thehamptons.com/anders/netatalk/>.

7.6. Servizi Network File System (NFS)

Linux può agire sia come client e sia come server per file sistem condivisi usando il protocollo Network File System (NFS), che rappresenta lo standard per la fornitura di file system montati tra sistema Unix.

Nota: Per favore, siate consci del fatto che avere disponibile il servizio NFS può comportare rischi alla sicurezza. Personalmente, non raccomando mai di usarlo.

Per usare NFS, dovrete assicurarvi che il supprto per NFS sia stato incluso nel vostro kernel o nei moduli del kernel. Si veda la Sezione 10.4 per informazioni su come aggiornare e personalizzare un kernel Linux.

Le condivisioni NFS vengono configurate modificando il file `/etc/exports`. Ecco alcuni esempio che mostrano alcune delle opzioni disponibili:

```
/archive spock.mydomain.name(ro)
/archive2 spock.mydomain.name(ro)
/mnt/cdrom other.domain(ro)
/archive2 10.23.14.8(ro,insecure)
```

Le prime due righe permettono all'host "spock.mydomain.name" di accedere alle directory `/archive` e `/archive2` tramite NFS. Queste condivisioni sono di sola lettura (opzione `(ro)`). Per ragioni di sicurezza, è consigliabile applicare tale opzione a tutte le condivisioni NFS, quando possibile.

La terza riga permette ad ogni host nello spazio nome di dominio "domain.name" di accedere al drive CD-ROM. Ovviamente, è necessario prima montare il CD-ROM in `/mnt/cdrom`.

Nota: Usando l'opzione `(ro)` read-only per questo dispositivo può sembrare ridondante, comunque può impedire a qualcuno di scrivere su un vero file system nel caso il CD-ROM non dovesse essere montato.

Dopo che avete fatto i cambiamenti al file `/etc/exports`, avrete bisogno di riavviare il demone NFS. Per farlo, digitate:

```
/etc/rc.d/init.d/nfs restart
```

Potete anche configurare i mount point di NFS con lo strumento "Network Configurator" incluso nell'utilità "Linuxconf". Per maggiori informazioni sull'utilità Linuxconf, si veda la Sezione 7.7.

Troverete maggiori informazioni su NFS nell'"*NFS-HOWTO*" su <http://metalab.unc.edu/LDP/HOWTO/NFS-HOWTO.html> [NdT: disponibile in italiano su <http://it.tldp.org/HOWTO/NFS-HOWTO.html>], oltre che nelle man page su "nfsd" e "exports".

7.7. Configurazione dalla A alla Z con Linuxconf

Esiste un eccellente strumento chiamato "linuxconf" che può assolvere facilmente a molti compiti di configurazione. Linuxconf gira su ogni tipo di ambiente disponibile -- potete eseguirlo da console, con una sessione telnet e come uno strumento con interfaccia grafica sotto X; esso si adeguerà e si avvierà nel modo appropriato.

Se dovete sistemare l'orologio di sistema, le impostazioni di rete o dei file system, oppure altri tipi di compiti di amministrazione e configurazione, allora dovrete proprio provarlo. L'unico avvertimento è che, al momento in cui scrivo, lo strumento con interfaccia grafica presenta ancora alcuni "bug" e, qualche volta, potrebbe smettere di rispondere ai click del mouse. Comunque credo che le future revisioni lo renderanno più usabile.

Capitolo 8. Procedure di backup e restore

Effettuare backup in maniera regolare dovrebbe essere una delle priorità maggiori di un buon amministratore di sistema. Sebbene Linux sia un sistema operativo molto affidabile, i malfunzionamenti sono sempre dietro l'angolo. Potrebbero essere causati dall'hardware, da un'interruzione di corrente, o da altre cause inaspettate.

Più probabilmente saranno causati da errori umani, come risultato di modifiche o cancellazioni non volute di file cruciali. Se vi sono utenti sul vostro sistema, prima o poi qualcuno vi chiederà di recuperare un file cancellato inavvertitamente.

Se effettuate regolari backup, preferibilmente a cadenza giornaliera (almeno per quegli utenti i cui file sono spesso aggiornati), ridurrete drasticamente la probabilità che tali file vadano perduti.

Il modo più sicuro per fare dei backup è quello di registrarli su supporti come nastri, dischi removibili, CD masterizzabili, ecc., e riporli in un luogo diverso da quello in cui risiede il vostro sistema Linux. Può non essere molto pratico -- può darsi che non abbiate un luogo sicuro (magari anti-incendio) dove riporre i vostri backup! Oppure può darsi che non abbiate accesso ad un luogo diverso dal primo. Comunque, anche così i backup possono essere fatti lo stesso.

Sul mio posto di lavoro, faccio i backup di diversi server Linux. A seconda della situazione, alcuni di questi backup sono memorizzati su nastri, altri su server separati all'interno della rete, mentre altri vengono semplicemente scritti su partizioni separate (per se esempio, nel file system `/archive/`) da un cron automatico (forse perché il server si trova lontano e quindi è impossibile, o quanto meno poco pratico, andare ogni giorno per fare i backup).

A casa, non ho né un sistema di backup esterno, né tanto spazio su disco per memorizzare i backup. Quindi, faccio il backup solo dei miei file in `/home/` e dei file di configurazione personalizzati presenti in `/etc/`, scrivendoli su una partizione separata.

8.1. Procedure per il backup dei server

Esistono diversi metodi per effettuare dei backup con Linux. Tra questi vi sono gli strumenti da riga di comando, presenti in ogni distribuzione Linux, come `dd`, `dump`, `cpio` e `tar`. Sono inoltre disponibili altre utilità in modalità testo come `Amanda` e `Taper`, progettati per offrire una comoda interfaccia-utente per le operazioni di backup e restore. Ci sono poi utilità con interfaccia grafica come `KDat` e quelle commerciali come `BRU` e `PerfectBackup+`. Ognuna di queste soluzioni vi permetterà di mettere al sicuro i vostri dati.

Potete trovare una breve lista degli strumenti disponibili, con informazioni su dove reperirli, su "Linux Applications and Utilities Page" all'indirizzo <http://www.xnet.com/~blatura/linapp2.html#back>. Quando decidete di effettuare un backup, dovrete considerare questi fattori:

- *Portabilità* - Se per voi è importante la portabilità (cioè la possibilità di effettuare un backup su una distribuzione Linux o su una implementazione di Unix e, poi, fare il restore su un'altra, ad esempio, da Solaris a Linux Red Hat) probabilmente dovrete scegliere uno degli strumenti da riga di comando (es. `dd`, `dump`, `cpio`, o `tar`), per il semplice fatto che essi saranno disponibili su ogni sistema `*nix`.
- *Backup automatici* - Se ritenete importante che i backup vengano fatti in automatico, ad intervalli di tempo regolari, senza alcun intervento umano allora dovrete scegliere uno strumento che vi permette di fare tutto ciò.
- *Interfacce user-friendly* - Se per voi è importante avere un qualche tipo d'interfaccia, sia essa testuale o grafica, allora le utilità commerciali offrono quelle più semplici e anche il supporto tecnico.

- *Remote backups* - è importante per voi avere la possibilità di effettuare backup e restore da remoto? Se sì, allora dovrete optare per uno strumento a riga di comando oppure utilità in modalità testuale, invece di quelle con interfaccia grafica (a meno che non abbiate una connessione veloce e la possibilità di lanciare sessioni di X da remoto).
- *Network backups* - Dovete effettuare backup e restore su una rete? Allora, probabilmente, dovrete scegliere una delle utilità da riga di comando (come "tar") che supporta l'accesso di rete ai dispositivi di backup, oppure strumenti specializzati in questo come "Amanda" o altri strumenti commerciali.
- *Media types* - I backup possono essere immagazzinati su diversi media, come nastri, un altro hard-disk, ZIP drives o su CD masterizzabili. In questo caso dovrete confrontare i costi con l'affidabilità, la capacità di memorizzazione e la velocità di trasferimento.

Cautela

Quando fate un backup del vostro file system, *non* includete lo pseudo-file system `/proc`. I file in `/proc` non sono file veri e propri, ma semplicemente dei link che descrivono e puntano alle strutture-dati del kernel. Fare il backup di un file come `/proc/kcore` che è uno pseudo-file con l'intero contenuto della vostra memoria, è solo un spreco di spazio secondo me! :-). Dovreste, inoltre, evitare di fare il backup del file system `/mnt`, a meno che non vogliate fare il backup dei file del CD-ROM, floppy disk, file di rete condivisi, o di altri dispositivi montati.

Ovviamente, le procedure per effettuare un backup ed un restore differiscono, a seconda delle vostre scelte. Comunque, in questa sezione, vi mostrerò come effettuare dei backup con gli strumenti che uso maggiormente, cioè "tar" (che sta per "Tape Archiver") che funziona a riga di comando e permette la portabilità tra i vari sistemi *nix; e poi "KDat", un'utilità con interfaccia grafica presente in KDE (si veda la Sezione 5.6 per maggiori informazioni su KDE).

In ultimo, aggiungo che anche se lo strumento che avete scelto non offre la possibilità di effettuare backup automatici ogni tot tempo, potete utilizzare cron. Si veda la Sezione 9.4 per maggiori dettagli sull'uso di cron.

8.1.1. Backup con "tar":

Se decidete di usare "tar" per i vostri backup, avrete bisogno di un po' di tempo per studiare tutte le varie opzioni disponibili; digitate `man tar` per vedere la lista. Avrete inoltre bisogno di sapere come accedere ai media; sebbene tutti i dispositivi sono trattati come file nel mondo Unix, se volete scrivere su un nastro, il nome del "file" è il nome del dispositivo stesso (es. `/dev/nst0` per un tape-drive SCSI).

Il seguente comando effettuerà un backup dell'intero sistema Linux sul file system `/archive/`, ad eccezione dello pseudo file-system `/proc/` e di ogni file-system montato in `/mnt/`, il file system `/archive/` (non è il caso di fare il backup del backup stesso), e i file di cache di Squid (che secondo me non sono necessari):

```
tar -zcvpf /archive/full-backup-`date +%d-%B-%Y` .tar.gz \  
--directory / --exclude=mnt --exclude=proc --exclude=var/spool/squid .
```

Non fatevi intimorire dalla lunghezza del comando appena descritto! Dopo averlo scomposto nei suoi elementi, vedrete la bellezza e la potenza di questa utilità.

Il comando prevede l'opzione "z" (compressato; i dati di backup verranno compressi con "gzip"), "c" (crea; crea un nuovo archivio), "v" (verboso; mostra la lista dei file di qui viene fatto il backup), "p" (mantieni i permessi; le informazioni per la protezione dei file verranno "ricordate" per quando poi farete il restore). L'opzione "f" (file indica che il prossimo argomento sarà il nome del file di archivio che sta per essere scritto. Notate come per creare un

file con la data corrente, basta includere il comando "date". Una convenzione comune è quella di aggiungere il suffisso "tar" per archivi non compressi, e "tar.gz" per quelli compressi.

L'opzione "--directory" indica a tar di andare alla directory specificata ("/" nell'esempio) prima di iniziare il backup. L'opzione "--exclude" dice a tar di non includere nel backup le directory o i file specificati. In ultimo, il carattere "." dice a tar di fare il backup di tutto il contenuto della directory corrente.

Nota: È importante capire che le opzioni sono cAsE-sEnSiTiVe! Inoltre, molte delle opzioni possono essere specificate o con un singolo carattere (es. "f") o col nome completo dell'opzione (es. "file"). In caso di singola lettera bisogna anteporre il carattere "-", invece "--" nel caso di nome completo. Comunque guardate le pagine "man" per informazioni sull'uso di tar.

Un altro esempio, questa volta scrivendo solo specificati file-system (invece di scriverli *tutti* con le eccezioni, come dimostrate nell'esempio sopra) su un tape-drive SCSI:

```
tar -cvpf /dev/nst0 --label="Backup set created on `date +%d-%B-%Y`\" \
    --directory / --exclude=var/spool/ etc home usr/local var/spool
```

Nel comando sopra, l'opzione "z" (compresso) non viene usata. È *caldamente* raccomandato di non scrivere dati compressi su nastro, perché se i dati presenti su una porzione del nastro si danneggiano, perderete il vostro intero backup. Comunque, file d'archivio scritti senza compressione hanno un alto grado di recuperabilità, anche se porzione dell'archivio sono danneggiate.

Nota: Il dispositivo "/dev/nst0" non viene riavvolto dopo un backup. Quindi è possibile scrivere più backup su un solo nastro. (Potete riferirvi al dispositivo come "/dev/nst0", nel qual caso il nastro sarà automaticamente riavvolto al termine della scrittura del backup).

Dato che non possiamo specificare un filename per il backup, l'opzione "--label" può essere usato per scrivere alcune informazioni su backup nel file d'archivio stesso.

Infine, solo i file contenuti in "/etc/", "/home/", "/usr/local" e "/var/spool/" (ad eccezione dei file di cache di Squid) verranno scritti sul nastro.

Potete usare i seguenti comandi per riavvolgere e poi espellere un nastro:

```
mt -f /dev/nst0 rewind
mt -f /dev/nst0 offline
```

Suggerimento: Suggerimento: Avrete notato che il carattere "/" (slash) viene eliminato da tar quando un file d'archivio viene creato. Questo è il modo predefinito per tar, e serve ad impedire che voi sovrascriviate file critici con versioni più vecchie di essi. Potreste recuperare il file sbagliato nel processo di restore. Se proprio non vi piace potete specificare l'opzione "--absolute-paths", che manterrà gli slash. Comunque vi raccomando di non farlo, perché è *pericoloso*!

8.1.2. Backup con "KDat":

Se state usando KDE, credo che troverete molto utile e amichevole l'utilità "KDat". Anche perché, utilizza "tar" come motore. Quindi, i backup scritti con KDat possono essere letti sia con KDat stesso e sia con tar!! Questo fa di KDat un'ottima scelta.

Suggerimento: Suggerimento: Anche se scegliete di non usare o installare il pacchetto completo di KDE, potete *sempre* utilizzare KDat, sempre che abbiate installate le librerie Qt.

La prima volta che eseguirete il programma KDat, avrete bisogno di creare un profilo di backup. Tale profilo indica a KDat quali file del vostro sistema volete includere nel backup. Se volete, potete creare più di un profilo, a seconda delle vostre esigenze (per esempio, potete creare un profilo chiamato "*Full Backup*" per un backup completo del sistema, e "*Quick Backup*" per il backup dei soli file degli utenti).

Per creare un profilo, scegliete "Create Backup Profile" dal menu "File" (oppure cliccate con il tasto destro sulla cartella "Backup Profiles" e scegliete "Create Backup Profile". Sul lato destro della finestra di KDat potete impostare diverse cose, come il nome del profilo, il nome dell'archivio, le opzioni per tar, ecc. Cliccate sul menu "Help" per aver maggiori informazioni su tutte le varie impostazioni.

Per specificare quali file devono essere inclusi nel profilo, cliccate con il tasto sinistro sulla casella accanto alla cartella della directory "/". Questo permetterà di aggiungere al backup tutti i file della directory. Poi, cliccate sul piccolo "+" accanto alla cartella. Ciò permetterà di espandere la cartella, mostrando una lista di file. Potrete, in tal modo, escludere dal backup qualunque file; cliccate semplicemente con il tasto sinistro sulla casella accanto al file o directory che volete escludere. Per esempio, un backup completo avrà tutti i file e tutte le directory spuntate, ad eccezione di `/proc` (uno pseudo file system che contiene informazioni sul vostro sistema), `/mnt` (una directory dove di solito sono montati i lettori CD-ROM, di dischetti e le risorse di rete), e, se usate Squid, `/var/spool/squid` (i file di cache di Squid). Dopo aver selezionato i file giusti, cliccate sul profilo di backup che state creando e poi, sempre con tasto sinistro, sul bottone "Files >>" per spostare la lista dei file selezionati direttamente nel vostro profilo.

Nota: Se i dati da memorizzare del vostro server dovessero eccedere la capienza del supporto che avete scelto per archiviare i dati, dovrete creare profili di backup separati, uno per ogni parte del vostro backup.

Per fare il backup, inserite un nastro nel drive e scegliete "Mount Tape" dal menu "File" (oppure cliccate sull'icona a forma di nastro). Ciò *monterà* il nastro (in verità, poiché non è possibile montare tale dispositivo, quello che fa KDat è riavvolgere il nastro, cercare di leggere le informazioni nell'header, e in caso di successo, trovare il tape index sul vostro hard-disk. Altrimenti, KDat vi chiederà di formattare il nastro.

Nota: Se KDat continua a lamentarsi che non c'è il nastro nel drive e invece c'è, assicuratevi di aver selezionato correttamente il nome del dispositivo tra le preferenze; cliccate su "Edit" nel menu e scegliete "User Preferences".

Fatto questo, prima di iniziare il backup dovete prima scegliere il profilo che volete usare. Per avviare il backup, cliccate con il tasto destro sul profilo desiderato, e poi con il tasto sinistro sull'opzione "Backup". KDat vi mostrerà prima una finestra di dialogo con i dettagli del profilo che avete selezionato; cliccate su "Ok" per avviare il backup.

Con il backup in corso, KDat mostrerà una finestra di dialogo con alcune informazioni statistiche (tempo trascorso, dimensioni del backup, tempo stimato per il completamento, oltre al numero di file e i byte totali scritti), e i file che man mano vengono aggiunti al backup. Per fare un backup completo, con diversi Gb di dati, possono volerci diverse ore. Se volete, potete cliccare, in qualsiasi momento, sul bottone “Abort” per interrompere il backup.

Una volta completato il backup, potete smontare il nastro scegliendo “Edit” dal menu, e quindi “Unmount Tape”, oppure cliccare sull’icona a forma di nastro, che lo riavvolgerà e poi lo espellerà.

8.2. Procedure per il restore dei dati del server

Sicuramente, la cosa più importante dopo quella di effettuare dei backup regolarmente è la possibilità di averli a disposizione al momento di recuperare un file importante!

Ovviamente, come già detto nella Sezione 8.1, le procedure di restore saranno diverse a seconda di cosa avete usato per fare il backup. In questa sezione, parleremo dei metodi per recuperare i file dopo un backup con “tar” e “KDat”.

8.2.1. Restore con “tar”:

Il comando seguente recupererà tutti i file dall’archivio “full-backup-09-October-1999.tar.gz”, che è un esempio di backup del nostro sistema Linux (come creato nell’esempio della Sezione 8.1.1):

```
tar -zxvpf /archive/full-backup-09-October-1999.tar.gz
```

Il comando sopra estrarrà tutti i file contenuti nell’archivio compresso, mantenendo la proprietà e i permessi originali dei file. L’opzione “x” sta per estrai. (Le altre opzioni sono descritte nella Sezione 8.1.1).

Cautela

Estrarre i file da un archivio tar può essere pericoloso, e dovrebbe essere fatto con cautela. Forse i file sono stati archiviati senza l’indicazione del percorso (alcuni sviluppatori ignoranti distribuiscono i tarball dei loro software in questo modo), e quindi saranno estratti nella directory corrente. Forse i file sono stati archiviati con l’opzione “--absolute-paths” il che significa che verranno estratti nella loro posizione assoluta (anche se non lo volete). Oppure, forse i file sono stati archiviati *senza* gli slash (“/”) iniziali, che significa che i file verranno estratti nella directory corrente (anche se non lo volete). Questo dipende naturalmente da come sono stati fatti i backup. Per questo motivo vi raccomando assolutamente di provare il comando “tar” prima con l’opzione “t” (*type*), e poi sostituire “t” con “x” (*extract*) quando siete assolutamente certi che il comando farà quello che volete che faccia.

Se non avete bisogno di recuperare tutti i file di un archivio, potete specificare solo quelli che vi interessano, come nell’esempio:

```
tar -zxvpf /archive/full-backup-09-October-1999.tar.gz \
    etc/profile usr/local/bin/tolower
```

Il comando sopra farà il restore dei file “etc/profile” e “usr/local/bin/tolower” dall’archivio d’esempio.

Suggerimento: Suggerimento: Se state cercando di recuperare uno o pochi file dal vostro archivio, non avrete successo finché non specificherete l’*esatto* percorso della directory e del file così come è stato memorizzato nell’archivio. Ecco un esempio:

```
tar -ztpvf /archive/full-backup-09-October-1999.tar.gz \
| grep -i profile
```

Nell'esempio sopra, tutti i file contenuti nella archivio vengono elencati in base al nome. L'output risultante viene poi trasmesso al comando "grep" command (usando l'opzione "i" di grep per ignorare lettere maiuscole e minuscole, che mostrerà tutti i file contenenti "profile" nel loro percorso o nel filename. Una volta che avete determinato con certezza il nome del file che volete recuperare, potete specificarlo nel comando tar.

Come già detto nella Sezione 8.1, al momento della creazione di un file d'archivio, tar eliminerà gli slash ("/") dal percorso del file. Ciò significa che questi file potrebbero non andare a finire nello stesso posto dove si trovavano al momento del backup. Allora, o passate alla directory "/" root o usate l'opzione "--directory /"

Nota: A Una buona soluzione è fare il restore dei file desiderati in una directory diversa (per esempio la vostra home directory) e successivamente confrontare, spostare o aggiornare i file alla loro posizione originale.

8.2.2. Restore con "KDat":

Per recuperare uno o più file da un backup fatto con KDat, inserite il nastro nel drive, scegliete "Mount Tape" dal menu "File" (oppure cliccate sull'icona a forma di nastro).

KDat proverà a leggere le informazioni dell'header del nastro, e se avrà successo, cercherà di trovare il tape index che combacia con l'identificazione trovate nell'header. Questo tape index è memorizzato sul vostro hard-disk, ed è un file unico creato per ogni nastro di backup formattato da KDat, e viene aggiornato ogni volta che fate un backup.

Se manca il corrispondente tape index (forse state cercando di fare il restore di un backup fatto un un'altra macchina, o il file è stato cancellato o, in qualche modo, corrotto sul vostro hard-disk), KDat vi informerà di questo fatto e vi chiederà se volete ricreare l'index mediante lettura del nastro. Poiché avrete bisogno di farlo se vorrete recuperare i vostri file, non avete altra scelta che cliccare su "Yes".

Nota: Dopo che l'operazione è stata portata a termine, il nome del nastro sarà "Reindexed Tape". Dovrete sostituirlo con il nome originale.

Una volta che il tape index è stato letto con successo, può essere usato per selezione le directory o i file che volete recuperare dal backup, esattamente allo stesso modo che avete usato per creare i vostri profili di backup (si veda la Sezione 8.1 per istruzioni su come selezionare i file).

Dopo avere selezionato i file che vi interessano, avviate il processo di restore scegliendo "Restore..." tra le opzioni del menù "File" (o cliccate sull'icona a forma di nastro). KDat mostrerà una finestra di dialogo, permettendovi di confermare i file che saranno recuperati. Inoltre, potrete specificare la directory di destinazione dei file. Potrete, in tal modo, recuperare i file critici nella vostra home directory, e poi, in seguito, confrontarli, spostarli o aggiornarli alla loro posizione di destinazione. Questo è sicuramente il metodo più sicuro.

Per iniziare il processo di recupero, cliccate su "Okay". Kdat inizierà a scansionare il nastro e a recuperare i file.

Potreste aver bisogno di fare il restore di uno o più file da un archivio creato con KDat *senza* usare KDat. Forse perché volete farlo su un sistema senza interfaccia grafica, oppure attraverso un lenta connessione di rete

(l'esecuzione da remoto di KDat sarebbe impraticabile). Fortunatamente, KDat crea i suoi backup tramite "tar", uno strumento a riga di comando disponibile per ogni sistema *nix.

Dovreste essere in grado, con tar, di fare il restore dei vostri backup fatti con KDat, semplicemente usandolo, con qualsiasi opzione, come lo usereste con qualunque altro archivio tar. Ricordatevi, però, che i dati non sono memorizzati in formato compresso.

Nota: Quasi certamente otterrete un messaggio di errore quando proverete ad accedere, con tar, ad un backup fatto con KDat. Ciò dipende dall'header e dalle altre informazioni che KDat aggiunge al nastro al momento della formattazione. Ripete il comando tar due o tre volte per saltare direttamente all'inizio del file d'archivio.

8.3. Backup della configurazione di un router Cisco

Sul mio posto di lavoro, abbiamo una WAN che mette in comunicazione diverse postazioni remote. Queste hanno router Cisco connessi via ISDN o, in alcuni casi, Centrex data circuits, che forniscono connettività Internet e WAN. I router Cisco permettono di usare TFTP ("Trivial File Transfer Protocol") su un server di rete per leggere e scrivere file di configurazione. Ogni volta che la configurazione di un router viene cambiata, è importante salvare il file di configurazioni sul server Linux in modo da conservarne una copia di backup.

Sappiate che Red Hat disabilita di default il servizio TFTP, perché se non viene configurato correttamente, può compromettere la sicurezza del sistema. Il demone TFTP permette a chiunque di leggere e scrivere file senza effettuare alcuna autenticazione. Personalmente, il metodo che uso per mettere le cose a posto, è quello di creare una directory "/tftpboot/", di proprietà di root, e poi modificare, nel file "/etc/inetd.conf", la riga di configurazione esistente per specificare la posizione del file:

```
tftpd  dgram  udp    wait   root   /usr/sbin/tcpd  in.tftpd  /tftpboot
```

Nota: Aggiungere il percorso "/tftpboot" alla fine della riga sopra indica dove il demone TFTP può avere accesso ai file. Sebbene potete eliminare quest'ultima parte e permettere a TFTP di avere accesso a qualunque file del vostro sistema, questo potrebbe comprometterne la sicurezza e quindi, probabilmente, conviene non farlo.

Una volta che avete attivato il servizio TFTP, non dimenticate di digitare:

```
killall -HUP inetd
```

Il comando sopra riavvia il demone INETD in modo da rendere effettivi i cambiamenti che avete fatto al file inetd.conf.

Fare il backup di un file di configurazione di un router richiede 3 passaggi: impostare per un file esistente (o crearne uno nuovo) il permesso di scrittura, scrivere il file di backup, e poi ricambiare i permessi per limitare l'accesso al file. Ecco un esempio di una sessione di backup di un router:

```
mail:~# cd /tftpboot
mail:/tftpboot# chmod a+w xyzrouter-config
chmod: xyzrouter-config: No such file or directory
mail:/tftpboot# touch xyzrouter-config
```

```
mail:/tftpboot# chmod a+w loyola-config
mail:/tftpboot# telnet xyzrouter
```

```
Escape character is '^]'.
User Access Verification
Password: ****
xyzrouter> enable
Password: ****
xyzrouter# write network
Remote host []? 123.12.41.41
Name of configuration file to write [xyzrouter-config]?
Write file xyzrouter-config on host 123.12.41.41? [confirm]
Building configuration...
Writing xyzrouter-config !! [OK]
xyzrouter# exit
Connection closed by foreign host.
```

```
mail:/tftpboot# chmod a-wr,u+r xyzrouter-config
mail:/tftpboot# exit
```

In caso di malfunzionamento del router (a causa, per esempio, di un aumento improvviso di corrente elettrica durante un temporale), questi file di backup possono aiutare a ricaricare la configurazione del router. Ancora una volta, recuperare un file di configurazioni comporta 3 passaggi: impostare i permessi sul file esistente, caricare il file, e poi rimettere a posto i permessi per limitare l'accesso al file. Ecco un esempio:

```
mail:~# cd /tftpboot
mail:/tftpboot# chmod a+r xyzrouter-config
mail:/tftpboot# telnet xyzrouter
```

```
Escape character is '^]'.
User Access Verification
Password: ****
xyzrouter> enable
Password: ****
xyzrouter# config network
Host or network configuration file [host]?
Address of remote host [255.255.255.255]? 123.12.41.41
Name of configuration file [xyzrouter-config]?
Configure using loyola-config from 123.12.41.41? [confirm]
Loading xyzrouter-config from 123.12.41.41 (via BRI0): !
[OK - 1265/32723 bytes]
xyzrouter# write
xyzrouter# exit
Connection closed by foreign host.
```

```
mail:/tftpboot# chmod a-wr,u+r xyzrouter-config
mail:/tftpboot# exit
```

Capitolo 9. Compiti di amministrazione vari ed eventuali

Linux ha dimostrato di essere estremamente affidabile in questi ultimi quattro anni, quando l'ho utilizzato come Internet server, e ha richiesto un'amministrazione minima per farlo funzionare. Dove possibile, alcuni ripetitivi e noiosi compiti di amministrazione possono e potrebbero essere automatizzati con crontab e file di script. Tuttavia, per far sì che Linux continui a funzionare senza problemi, è necessario effettuare, di tanto in tanto, alcuni controlli. Tra cui:

9.1. Controllare lo spazio destinato alla memorizzazione dei dati

È importante controllare, di tanto in tanto, che rimanga, sui dischi, spazio a sufficienza. Usate il comando "df" per avere un rapporto sullo spazio disponibile. Apparirà come segue (le informazioni si riferiscono all'Internet Server del mio posto di lavoro):

Filesystem	1024-blocks	Used	Available	Capacity	Mounted on
/dev/sda1	1888052	135908	1654551	8%	/
/dev/sdd1	4299828	100084	3977246	2%	/archive
/dev/hda2	3048303	897858	1992794	31%	/archive2
/dev/hda1	11677	1380	9694	12%	/boot
/dev/sdc1	4299828	350310	3727020	9%	/home
/dev/sdb1	4299828	598504	3478826	15%	/usr
/dev/sda2	1888083	700414	1090075	39%	/var
/dev/scd0	593958	593958	0	100%	/cdrom

Questi file system sono abbastanza stabili in quanto presentano un andamento di crescita lento.

Il file system "/" (anche detto "root"), montato su /dev/hda1, contiene il kernel Linux, i driver per le periferiche e altre directory. È anche il posto dove vengono memorizzati i messaggi di posta degli utenti (*/var/spool/mail/*) e i file di log (*/var/adm/*), ma poiché i messaggi di posta vengono poi smistati e i file di log vengono riciclati, la capacità disponibile rimane abbastanza stabile (con una crescita stimata dell'1% al mese). I file di log vengono alternati e ripuliti su base settimanale, quindi avrete sempre a vostra disposizione un mese di informazioni log.

Suggerimento: Suggerimento: Se questo file system sta crescendo troppo rapidamente, concentrate la vostra attenzione sulla directory */var/spool/mail* -- cercate grandi caselle postali (qualcosa come "find */var/spool/mail -size +1000k*" mostrerà una lista di caselle con dimensioni maggiori di 1Mb). Se scovate un file più grande di 1Mb, l'utente probabilmente non sta scaricando la propria posta, fa parte di una grossa mailing list, oppure il client per le e-mail non è configurato per rimuovere la posta dal server. Contattate l'utente e/o cancellate il file di posta, usando "> mailbox", (per esempio ">smithj" per pulire la casella di posta di Joe Smith). Controllate anche la directory */tmp/*, che può aver bisogno, di tanto in tanto, di essere ripulita (i vecchi file *tin** rimasti dopo sessioni interrotte di lettura delle news, vecchi file di stampa, ecc).

Il file system *"/usr/* (cioè "user"), montato su /dev/hda2, contiene software installabili dall'utente, pagine web, ecc. Questo è il file system più grande, e cresce anche lentamente. Il file di log per le pagine web possono essere memorizzati anche qui, e aumentano di dimensione. Controllateli e accorciateli periodicamente. Sulle mie macchine, all'inizio di ogni mese i file correnti di log per il web vengono spostati nei log riassuntivi del mese (cioè

access_log.11 per i log di Novembre). Alla fine dell'anno tutti questi log vengono tutti cancellati e il ciclo ricomincia daccapo (il che significa che ogni 1° Gennaio avrete un consistente aumento dello spazio disponibile).

Suggerimento: Suggerimento: Se questo file system sta crescendo rapidamente, controllate le directory `"/usr/local/etc/httpd/logs"` e `"/usr/local/squid/logs/"` (se le avete). Potrebbero esserci file di log che stanno diventando troppo grandi (se, forse, il sito ha ricevuto un gran numero di visite). Se, però, i log vengono ripuliti regolarmente come succede a me, non dovrete avere problemi di spazio (in verità, poiché utilizzo i dati sul traffico del mio sito per analisi statistiche cerco di non cancellarli quando posso). Un altro posto dove cercare file potenzialmente cancellabili è `"/usr/tmp/"`.

Il file system `"/home/"`, (cioè lo spazio personale degli utenti), montato su `/dev/hda3`, contiene tutte le directory e i file personali degli utenti. A meno che non abbiate dato account di shell, molte di esse non saranno accessibili agli utenti (queste directory vengono create al momento della creazione degli account degli utenti, e possono essere successivamente utilizzate per mandare la posta agli utenti, ecc.). Comunque gli utenti, con o senza account di shell, che hanno pagine web personali, probabilmente le hanno memorizzate qui. In più, la pagine principali del server sono memorizzate qui nella directory `/home/httpd` (con Red Hat); mentre altre distribuzioni le mettono nel file system `/usr` (si veda la Sezione 7.1 per maggiori informazioni).

Questo file system è, probabilmente, quello che cresce più lentamente salvo che non offriate molti account di shell.

Suggerimento: Suggerimento: Se questo file system aumenta improvvisamente di dimensioni, è perché probabilmente uno dei vostri utenti sta aggiungendo pagine web o file binari al suo spazio personale. Controllate il file di log `"/var/adm/xferlog.*"`, che dovrebbe mostrarvi quale utente ha fatto aggiunte alle proprie pagine web.

Ho anche un file system `"/archive/"` montato su `/dev/hdb1`, che è un hard-disk in più da 1.02 Gb che può essere usato per molti scopi (per esempio file di dati, kit software, ecc). Utilizzo un buon 70% di esso per backup completi di sistema da disco a disco). Parlando in generale, potete aggiungere e montare le vostre periferiche come volete.

Ho anche un lettore CD-ROM, montato come `"/mnt/cdrom/"` su `/dev/scd0`, che è un CDROM SCSI 24X che può leggere ogni CD in formato ISO9660. Viene utilizzato principalmente per installare del software, ma i CD DOS/Windows possono essere montati e resi accessibili dalle risorse di rete di Windows 3.x/95/NT con Samba (si veda la Sezione 7.4 per maggiori informazioni).

Il comando `"rm"` cancellerà un file. La sintassi è `"rm nomefile"`. Se volete confermare prima di cancellare, usate l'opzione `"-i"` (cioè `"rm -i *"`). Vi verrà chiesta la conferma per ogni file, prima che venga cancellato.

Nota: Questo è quanto succede agli utenti normali, ma attenzione -- per l'utente root non verrà chiesta conferma prima di cancellare un file a meno che non specificiate l'opzione `"-i"`!

State attenti a quello che digitate, soprattutto quando siete `"root"`, perché potreste rimpiangere di aver cancellato il file sbagliato.

9.2. Gestire i processi

Di tanto in tanto vorrete poter vedere i processi che stanno girando su Linux. Per avere una lista di tali processi, digitate `"ps -aux"` e apparirà qualcosa del genere.

```

USER      PID %CPU %MEM  SIZE  RSS TTY STAT START   TIME COMMAND
bin        69  0.0  1.0   788   320 ?  S   Nov 30   0:00 /usr/sbin/rpc.portmap
frampton  10273 0.0  2.1  1136   664 p0 S   14:12   0:00 -bash
frampton  10744 0.0  1.1   820   360 p0 R   17:25   0:00 ps -aux
frampton  10745 0.0  0.8   788   264 p0 S   17:25   0:00 more
nobody    10132 0.0  1.8  1016   588 ?  S   13:36   0:00 httpd
nobody    10133 0.0  1.8   988   568 ?  S   13:36   0:00 httpd
nobody    10413 0.0  1.8  1012   580 ?  S   14:56   0:00 httpd
nobody    10416 0.0  1.8  1012   580 ?  S   14:56   0:00 httpd
nobody    10418 0.0  1.8  1012   588 ?  S   14:57   0:00 httpd
nobody    10488 0.0  1.7   976   556 ?  S   15:34   0:00 httpd
nobody    10564 0.0  1.8   988   564 ?  S   16:06   0:00 httpd
nobody    10600 0.0  1.8   988   564 ?  S   16:15   0:00 httpd
nobody    10670 0.0  1.8   988   568 ?  S   16:45   0:00 httpd
nobody    10704 0.0  1.7   976   552 ?  S   17:03   0:00 httpd
root       1  0.0  1.0   776   312 ?  S   Nov 30   1:13 init [3]
root       2  0.0  0.0    0     0 ?  SW  Nov 30   0:00 (kflushd)
root       3  0.0  0.0    0     0 ?  SW  Nov 30   0:00 (kswapd)

```

La lista mostra il proprietario del processo (“nobody” per servizi speciale come il web server, il numero di identificazione del processo, la % di CPU che il processo sta attualmente utilizzando, la % di memoria consumata, e altre informazioni correlate oltre ad un descrizione del compito stesso.

Per aver maggiori informazioni su un certo processo, digitate “ps pid” (dove “pid” è il numero di identificazioni del processo). Nell’esempio, “ps 10704” mostrerà:

```
10704 ? S 0:00 /usr/local/etc/httpd/httpd
```

Questo particolare processo è un web server (il web server Apache apparirà più volte nella lista dei processi; sul perché si veda la Sezione 7.1).

Se notate che un servizio non sta funzionando, potete usare “kill -HUP pid” (dove “pid” è il numero di identificazione del processo come mostrato nella lista ottenuta con “ps”). Per esempio, se i servizi Internet (un processo chiamato inetd, #123 nel nostro esempio) non stanno funzionando come dovrebbero, un “kill -HUP 123” (o meglio, usate il comando “killall” e poi specificate il nome del processo: “killall -HUP inetd”) dovrebbe far ripartire il processo. L’opzione -HUP del comando kill significa “hang up” (fermare l’attività, n.d.t.); il processo dovrebbe ricaricarsi.

Se non riuscite a risolvere il problema, arrestate il sistema e rifate il boot (si veda la Sezione 6.7 per maggiori informazioni).

Potreste avere la necessità di sospendere temporaneamente un processo, per poi riattivarlo più tardi. Per esempio, nel caso dobbiate masterizzare un CD. Poiché le periferiche IDE fanno molto uso della CPU, se essa è troppo occupata potreste ritrovarvi con un bel sottobicchiere invece del vostro CD! Questi due comandi servono,rispettivamente, a sospendere e a riprendere un processo.

```
kill -STOP 945
kill -CONT 945
```

Red hat offre una soluzione migliore per fermare e riavviare alcuni processi. Ne parleremo nella Sezione 9.3

9.3. Avviare e fermare i processi

La distribuzione Red Hat offre un modo leggermente più organizzato per gestire i processi. Invece di dar loro la caccia e poi "killarli" con l'id della tabella dei processi, Red Hat fornisce una serie di script nella directory `/etc/rc.d/init.d` che vi permetterà di avviare e fermare i processi come desiderate.

Per esempio, per arrestare il servizio "httpd" (web server Apache), eseguite semplicemente lo script httpd:

```
/etc/rc.d/init.d/httpd stop
```

Allo stesso modo, potete usare l'opzione "start" per avviare un servizio. Oppure, se avete apportato dei cambiamenti ad un file di configurazione e volete riavviare il servizio in modo che vengano mantenute tali modifiche, usate l'opzione "restart".

Nota: Sembrerà strano, ma l'opzione "restart" sembra non essere supportata da alcuni servizi

9.4. Automatizzare i compiti con cron e i file crontab

Come molti utenti Linux, potreste trovare necessario programmare, ogni certo periodo di tempo, di eseguire dei compiti ripetitivi. Potrebbe essere necessario eseguire tali compiti molto frequentemente, tipo una volta ogni minuto, oppure più di rado, tipo un volta all'anno. Questa programmazione può essere fatta usando la facilitazione di "cron".

Quelle in Linux sono abbastanza simili a quelle disponibile per altre implementazioni di Unix. Comunque, Red Hat ha adottato un sistema di pianificazione di compiti che è leggermente differente da quelli di altre distribuzioni Linux. Come il altre distribuzioni, le informazioni sono contenute nel file di sistema "crontab" (che si trova nella directory `/etc/`), con il seguente formato:

```
minute hour day month year command
```

Potete specificare ogni componente temporale come un numero intero (es. da 1 a 12 per i mesi), oppure inserire per uno o più componenti il carattere "*" che sarà interpretato come una wildcard (cioè, "*" nel mese significa che il comando si attiverà ad un dato giorno e ad una data ora di ogni mese). Vediamo qualche esempio:

```
# Mail the system logs at 4:30pm every June 15th.
30 16 15 06 * for x in /var/log/*; do cat ${x} | mail postmaster; done

# Inform the administrator, at midnight, of the changing seasons.
00 00 20 04 * echo 'Woohoo, spring is here!'
00 00 20 06 * echo 'Yeah, summer has arrived, time to hit the beach!'
00 00 20 10 * echo 'Fall has arrived. Get those jackets out. :-('
00 00 20 12 * echo 'Time for 5 months of misery. ;-('
```

Notate come i comandi che forniscono output in maniera standard (cioè, a terminale) come, nell'esempio, "echo", invieranno il loro output all'account di "root". Se volete evitarlo, fate in questo modo:

```
00 06 * * * echo 'I bug the system administrator daily at 6:00am!' >/dev/null
```

Oltre a "crontab", Red Hat aggiunge alcune directory:

```
/etc/cron.hourly/
```

```
/etc/cron.daily/  
/etc/cron.weekly/
```

Come suggerisce il nome, i file eseguibili possono essere messi in una di queste directory, per poi essere eseguiti a cadenza oraria, giornaliera o settimanale. Ciò permette di risparmiare un po' di tempo. Mettete lo script o il programma (o un link simbolico ad una memorizzato da qualche altra parte) nella directory appropriate e dimenticatevi di esso.

Capitolo 10. Aggiornare Linux e altre applicazioni

Per ottenere il massimo da Linux, come aggiungere alcune caratteristiche, eliminare potenziali bug e assicurarsi che non ci siano buchi nella sicurezza, è buona regola mantenere il vostro server sempre aggiornato -- compreso il kernel, i moduli e le applicazioni utente. Talvolta potrebbe essere necessario anche aggiornare le componenti hardware, magari con un disco più grande. Questo capitolo sarà incentrato proprio su questi argomenti.

10.1. Usare il Red Hat Package Manager (RPM)

La distribuzione Red Hat, incluso il kernel, le librerie e le applicazioni, è composta da file RPM. Un file RPM, anche conosciuto come “pacchetto” rappresenta un metodo per distribuire il software in modo che posso essere facilmente installato, aggiornato e cancellato. I file RPM contengono informazioni sul nome del pacchetto, la versione, altri file da cui dipendono (se ci sono), la piattaforma (come Intel, Alpha, ecc.) e la destinazione di default dei file dopo l’installazione.

L’utilità RPM è stata sviluppata inizialmente da Red Hat e distribuita come prodotto Open Source (cosa comune nel mondo Linux). Altri sviluppatori vi hanno poi aggiunto alcune funzionalità extra. Il metodo RPM è diventato molto popolare e viene usato, oltre ovviamente a Red Hat, anche da altre distribuzioni.

Le applicazioni popolari di Linux vengono quasi sempre rilasciate come file RPM. Comunque, nel mondo Unix il metodo di distribuzione standard dei pacchetti continua ad essere fatto con i c.d. “tarballs”. I tarball sono file che possono essere letti con l’utilità “tar”. Installare con tar risulta spesso più noioso rispetto a RPM. Allora, perché la gente continua a farlo? Sfortunatamente, talvolta ci vogliono alcune settimane prima che gli sviluppatori convertano l’ultima versioni di un pacchetto nel formato RPM (molti la rilasciano come tarball).

Se iniziate a installare o aggiornare il vostro sistema, o le vostre applicazioni con tar, il vostro database RPM diventerà antiquato. Certamente non è un buon affare (quando usavo Slackware utilizzavo esclusivamente tar --non c’era altra scelta-- e non era poi così scomodo), ma quando è possibile mi armo di pazienza e aspetto che un RPM diventi disponibile, oppure mando un richiesta cortese allo sviluppatore del pacchetto. (Potete anche fare voi i vostri file RPM e distribuirli agli altri; ciò risulterebbe senz’altro utile agli sviluppatori che non hanno l’abilità o il tempo di farli).

Un buon posto per verificare la disponibilità degli RPM di un software è il deposito degli RPM su <http://rufus.w3.org/linux/RPM/>. Esso è diviso in categorie che vi possono aiutare a trovare un certo file RPM, e contiene rimandi a migliaia di questi file.

Per interrogare un pacchetto, usate use “rpm -q pkg-name” (per esempio “rpm -q pine”). RPM vi mostrerà la versione del pacchetto già installato, oppure vi dirà che non lo avete installato.

Posto che il pacchetto sia già stato installato, ed è una versione precedente all’aggiornamento che avete scaricato, potete applicare l’aggiornamento con “rpm -Uvh pkg-name”. Se tutto va per il meglio, il pacchetto verrà automaticamente installato e sarà immediatamente pronto all’uso. Nel caso contrario, RPM vi fornirà una buona ragione (magari un pacchetto di supporto deve prima essere aggiornato). Ciò potrebbe darvi un po’ da pensare, ma problemi come questi sono molto facili da superare.

Se, invece, il pacchetto *non* è già installato, e voi decidete di farlo, digitate “rpm -ivh pkg-name”. Se c’è bisogno di altri pacchetti, RPM ve lo farà sapere.

Alcune volete, vorrete installare un pacchetto che è disponibile solo in formato sorgente. Infatti, a meno che non stiate installando pacchetti provenienti da fonte sicura (come il sito ftp di Red Hat) probabilmente *dovrete* installare da sorgente nel caso i binari contengano trojan e altre cose pericolose (sicuramente, anche un sorgente RPM può contenere queste cose, ma è poco probabile che accada perché verrebbero scoperti in poco tempo da un altro sviluppatore).

Per installare un pacchetto dal sorgente bisogna specificare lo switch "rebuild" all'utilità RPM. Per esempio:

```
rpm -ivh --rebuild foo.src.rpm
```

Il comando sopra dovrebbe configurare e compilare il pacchetto "foo", producendo un file binario RPM nella directory `/usr/src/redhat/RPMS/i386/` (posto che stiate utilizzando Linux su una piattaforma Intel). Potete poi installare il pacchetto normalmente.

In ultimo, se avete problemi a compilare un pacchetto in codice sorgente (forse avete bisogno di modificare un makefile, oppure cambiare un'opzione di configurazione, ecc.) seguite i seguenti passaggi (sempre riferiti al nostro pacchetto di esempio "foo") per compilare il sorgente, ottenere un nuovo pacchetto binario, e poi fare l'installazione dal binario:

```
rpm -ivh foo.src.rpm  
cd /usr/src/redhat/SPECS  
pico -w foo.spec
```

Fate tutte le modifiche che credete siano necessarie al file ".spec", a quindi digitate:

```
rpm -ba foo.spec
```

Questo ricostruirà il pacchetto usando qualunque modifica abbiate fatto al file ".spec". Come sopra, il risultante file binario RPM si troverà in `/usr/src/redhat/RPMS/i386/`, e potrete installarlo normalmente.

Dovreste dare un'occhiata alla documentazione di Red Hat per maggiori informazioni sugli RPM. È uno strumento così potente che vale la pena imparare anche i piccoli dettagli. La miglior risorsa di informazioni sugli RPM è "Maximum RPM", che è disponibile sia in forma cartacea sia in formato postscript su <http://www.rpm.org/maximum-rpm.ps.gz>. (Se decidete di stampare il documento postscript sappiate che avrete bisogno di *molta* carta!). È disponibile anche una guida di dimensioni più contenute, il "RPM-HOWTO", su <http://www.rpm.org/support/RPM-HOWTO.html>

10.2. Installare o aggiornare senza RPM

Talvolta, potreste aver bisogno di installare o aggiornare un'applicazione per cui non è disponibile il pacchetto RPM. Sicuramente è una operazione possibile (infatti, è quello che viene fatto comunemente nel cosiddetto mondo Unix "reale"), ma vi raccomanderei di farlo solo se ne avete proprio bisogno (per sapere perché, si veda la Sezione 10.1).

Se dovete installare qualche tarball, la regola pratica generale per l'installazione di software su grandi sistemi è di mettere le cose nel vostro filesystem `/usr/local/`. Quindi, scompattate i tarball in `/usr/local/src/`, con i risultanti binari che saranno probabilmente installati in `/usr/local/bin` e con i loro file di configurazioni in `/usr/local/etc/`. Seguire questo schema renderà l'amministrazione del vostro sistema un po' più facile (benché non così facile come su un sistema con solo RPM).

In ultimo, gli utenti finali che vogliono installare, per uso privato, del software proveniente da tarball, lo faranno probabilmente nella loro home directory.

Dopo aver scaricato il tarball dal vostro sito fidato, andate nella directory appropriata e scompattate l'archivio digitando (come root, se necessario) il comando come nell'esempio che segue:

```
tar zxvpf cardgame.tar.gz
```

Il comando sopra estrarrà tutti i file dall'archivio compresso, che nell'esempio è "cardgame.tar.gz". L'opzione "z" dice a tar che l'archivio è compresso con gzip (quindi omettete l'opzione se il vostro tarball non è compresso); l'opzione "x" dice a tar di estrarre tutti i file. L'opzione "v" sta per verbose, che mostra tutti i filename man mano che vengono estratti. L'opzione "p" mantiene i permessi originali che i file avevano al momento di creare l'archivio. In ultimo, l'opzione "f" dice a tar che il successivo argomento è il nome del file. Non dimenticate che le opzioni di tar sono cAsE-sEnSiTiVe.

Cautela

Come specificato nella Sezione 8.2.1, vi raccomando di usare l'opzione "t" per visualizzare il contenuto dell'archivio prima di procedere all'estrazione dei file. Far ciò potrebbe evitare di estrarre i file in posizioni non volute o, anche peggio, la sovrascrittura inavvertita di altri file già esistenti.

Una volta installato il tarball nella giusta directory, troverete certamente un file "README" oppure "INSTALL" tra quelli installati, con ulteriori istruzioni su come preparare il pacchetto per l'utilizzo. Quasi sicuramente, dovrete inserire dei comandi simili a questi:

```
./configure  
make  
make install
```

Il comando sopra dovrebbe configurare il software e assicurarsi che il vostro sistema abbia le necessarie librerie e funzionalità necessarie al compilamento del pacchetto, compilare tutti i file sorgente in binari eseguibili, e poi installare i binari e ogni altro file di supporto nella posizione giusta. Le procedure che dovrete seguire possono, sicuramente, variare da software a software, quindi leggete attentamente ogni documentazione inclusa.

Ancora un volta, a meno che non sia assolutamente necessario, vi raccomando di evitare i tarball e usare gli RPM se potete.

10.3. Strategie per mantenere un sistema aggiornato

Di tanto in tanto, potreste venire a conoscenza, da varie fonti, di aggiornamenti significativi per il kernel Linux o per le applicazioni utente. Queste fonti possono essere riviste specializzate, newsgroups, pagine web, ecc.

Probabilmente la migliore risorsa online che un amministratore Linux dovrebbe --anzi no, *deve* -- spesso consultare è il sito web <http://freshmeat.net/>. Esso contiene descrizioni di nuovi progetti e di nuove applicazioni Open Source, documentazione, e altre cose di interesse per la comunità Linux.

Un'altra risorsa per tenersi aggiornato su comunicazioni di nuove applicazioni è il newsgroup comp.os.linux.announce (news:comp.os.linux.announce). Questo newsgroup contiene messaggi relativi a nuove applicazioni, ad alcuni aggiornamenti per il kernel o per le applicazioni, a pagine web, ecc. disponibili per Linux. Si tratta di un newsgroup moderato e quindi ha un "alto tasso di" affidabilità.

Non tutti gli annunci di aggiornamenti dei prodotti vengono fatti su comp.os.linux, comunque. Quindi, oltre a tale newsgroup, è sicuramente una buona idea visitare le pagine web o i siti FTP relativi alle applicazioni che state utilizzando.

10.4. Aggiornamenti del kernel Linux

Di tanto in tanto potrebbe essere saggio aggiornare il kernel di Linux. Ciò vi permetterà di stare al passo con le nuove caratteristiche e con l'eliminazione di alcuni bug man mano che sono disponibili. Oppure, forse, state facendo girare Linux su un nuovo, o particolare, hardware; oppure volete attivare alcune caratteristiche per le quali è richiesto un kernel su misura.

Questa sezione descriverà come aggiornare e personalizzare un nuovo kernel. Non è così difficile come potreste credere!

Gli annunci di nuove versioni di kernel possono essere trovati in diversi modi, compresi il newsgroup `comp.os.linux.announce` (`news:comp.os.linux.announce`) e i siti web <http://freshmeat.net/> e <http://slashdot.org/>

Tenete conto, per favore, che attualmente ci sono due "correnti" di sviluppo del kernel -- una riguarda le versioni "stabili", mentre l'altra riguarda le versioni "in sviluppo". Per applicazioni cruciali, come un Internet server, è altamente consigliato far ricorso alle versioni stabili, lasciando perdere i kernel in sviluppo.

La differenza tra le due correnti è che, i kernel di sviluppo contengono driver non ancora testati per l'hardware, file system e altre cose. Tali kernel sono utilizzati solo da hacker -- cioè gente a cui non importa fare il reboot del sistema quando un bug mostra la sua brutta faccia.

I kernel stabili introducono nuove caratteristiche e nuovi driver solo dopo che sono state abbondantemente testate. Servono inoltre ad eliminare ogni bug che è stato trovato e corretto.

Le due correnti utilizzano numeri di versione diversi, in modo che sia possibile distinguerle. I kernel stabili hanno il secondo numero pari (per esempio 2.0.35, 2.0.36, 2.2.4) mentre nei kernel di sviluppo il secondo numero è dispari (es. 2.1.120, 2.1.121, 2.3.0).

L'ultimo kernel stabile è sempre reso disponibile in codice sorgente e in formato binario pre-compilato su sito FTP <ftp://ftp.redhat.com/redhat/updates/>. Scaricate il kernel desiderato per la vostra versione e piattaforma (per esempio, dovrete andare nella directory `/6.1/i386/` e scaricare i file `kernel-*.i386.rpm` per la versione 6.1 su piattaforma Intel):

Nota: Non avete bisogno di scaricare i sorgenti del kernel se non avete intenzione di personalizzare il vostro kernel. (si veda la Sezione 10.6 per informazioni su come personalizzare il kernel).

Se doveste aver bisogno di usare un kernel non ancora disponibile in RPM, allora potete trovare gli ultimi kernel sul sito Ftp <ftp://ftp.kernel.org>, nella directory `/pub/linux/kernel/` (<ftp://ftp.kernel.org/pub/linux/kernel/>). Andate alla subdirectory della versione principale (es. `"v2.0"`), che contiene tutte le versioni del kernel fino a quella attuale. Scaricate il kernel desiderato (per esempio, il tarball compresso per la versione 2.0.36 si chiamerà `"linux-2.0.36.tar.gz"` per la piattaforma Intel) e scompattatelo nella directory `"/usr/src"`.

Nota: Molte delle applicazioni installate dagli utenti senza RPM dovrebbero essere scompattate, di regola, in `"/usr/local/src/"`, ma qui si parla di kernel e quindi faremo un'eccezione. :-)

Siate consapevoli del fatto che se decidete di aggiornare il kernel con un tarball, dovrete sicuramente configurarlo, compilarlo ed installarlo da voi. A meno che non abbiate proprio bisogno dell'ultimo kernel di sviluppo, vi raccomando *vivamente* di fare l'aggiornamento con i file RPM forniti da Red Hat -- che sono già pre-configurati e pre-compilati, sebbene possiate compilare un kernel su misura anche da file RPM.

10.5. Aggiornare il kernel fornito da Red Hat

Il metodo di gran lunga più facile per aggiornare il vostro kernel è utilizzare uno stock kernel RPM fornito da Red Hat. Questi file RPM contengono codice di kernel binario pre-compilato, con il supporto per una grande varietà di hardware e caratteristiche popolari.

Installare uno stock kernel è facile e comporta pochi rischi. Digitate semplicemente, da root, la seguente sequenza di comandi:

```
rpm -Uvh kernel-2.0.36.i386.rpm
cd /boot
ls
```

Prendete note del nome del nuovo kernel, come riportato dal comando "ls". Prestate attenzione al file "vmlinuz"; per esempio, la terza release RPM del kernel 2.0.36 apparirà come "vmlinuz-2.0.36-3".

Adesso, editate il file di configurazione di LILO (digitate: "pico -w /etc/lilo.conf") e cambiate la riga "image=/boot/..." in modo che punti al nuovo file del kernel. Fatto ciò, digitate "/sbin/lilo". Se LILO dà un messaggio di errore, controllate che il nome del file in "lilo.conf" corrisponda a quello presente nella directory "/boot/".

Cautela

Non dimenticate questo passo!

Il comando sopra prevede che utilizzate la piattaforma Intel e usiate LILO per il boot del vostro sistema. Si veda la Sezione 4.8 per maggiori informazioni su LILO.

Dopo che avete aggiornato il vostro stock kernel e le informazioni nel vostro boot loader, dovrete essere in grado di spegnere e riavviare il sistema con il nuovo kernel (si veda la Sezione 6.7 per informazioni su come spegnere il sistema).

10.6. Costruire un kernel personalizzato

Se usate Linux su un sistema dotato di hardware o volete usare caratteristiche non supportate dallo stock kernel, o forse volete ridurre la quantità di memoria occupata dal kernel per utilizzare al meglio la memoria del vostro sistema, allora potreste trovare necessario personalizzare il vostro kernel.

Aggiornare il kernel comporta configurare i moduli desiderati, compilare il kernel e i moduli, e finalmente installare l'immagine del kernel. Tutto ciò è seguito da un reboot del sistema (tenendo le dita incrociate!) per caricare il nuovo kernel. Potete trovare la documentazione nel file "README" che accompagna ogni pacchetto kernel. Ulteriori informazioni possono essere reperite nella subdirectory "Documentation/". Un file particolarmente utile è "Configure.help" che contiene informazioni dettagliate sulle opzioni disponibili per la compilazione del kernel e dei moduli.

Quello che segue è un esempio dimostrativo per la messa a punto di un kernel personalizzato, versione 2.0.36 su piattaforma Intel. Di solito costruire un kernel personalizzato è solo questione di configurazione, compilazione e installazione, ma talvolta (di solito in caso di nuovo hardware) è necessario scaricare driver aggiuntivi nel caso il vostro hardware non sia ancora supportato dalla versione del kernel che state compilando.

Il primo passo è quello di scaricare e installare il codice sorgente del kernel o tramite RPM o con tarball. Si veda la Sezione 10.4 per scoprire come ottenere i file appropriati.

Dopo di che, usate l'utilità "rpm" (oppure "tar") per installare i file "kernel source" e "headers". Per esempio, per installare i file RPM del kernel 2.0.36-3:

```
rpm -Uvh kernel-source-2.0.36-3.i386.rpm kernel-headers-2.0.36-3.i386.rpm
rpm -Uvh kernel-ibcs-2.0.36-3.i386.rpm
```

se Linux è su un notebook, probabilmente installerete anche il file "kernel-pcmcia-cs-2.0.36-3.i386.rpm" che contiene caratteristiche per la gestione dell'alimentazione.

Dopo aver installato i file del kernel, dovreste trovare l'albero del sorgente del kernel nella directory "/usr/src/linux".

Il passo seguente è quello di scaricare ogni driver addizionale (se applicabile) e installarli nel nuovo albero del sorgente del kernel. Per esempio, per avere il supporto del controller Mylex DAC960 per hardware RAID, dovrò scaricare il driver dal sito <http://www.dandelion.com/>. Sfortunatamente, tale driver viene spesso fornito come tarball e quindi dovreste usare l'utilità "tar". Per esempio.

```
cd /usr/src/
tar zxvpf DAC960-2.0.0-Beta4.tar.gz
```

Dovete leggere la documentazione fornita con il driver. Per esempio, il driver DAC960 comprende un file "README" che fornisce istruzioni su dove mettere i nuovi file scaricati e come applicare la patch al kernel:

```
mv README.DAC960 DAC960.[ch] /usr/src/linux/drivers/block
patch -p0 < DAC960.patch
```

Poi, assicuratevi che i link simbolici del vostro sistema siano coerenti con il nuovo albero del kernel. In realtà, ciò deve essere fatto una sola volta, quindi quanto segue deve essere fatto solo se non avete mai compilato prima un kernel personalizzato.

```
mail:/usr/src# cd /usr/include
mail:/usr/include# rm -rf asm linux scsi
mail:/usr/include# ln -s /usr/src/linux/include/asm-i386 asm
mail:/usr/include# ln -s /usr/src/linux/include/linux linux
mail:/usr/include# ln -s /usr/src/linux/include/scsi scsi
```

Nota: Quanto visto sopra non è più necessario per le versioni di kernel 2.2.x o superiori.

Il passo successivo è configurare le impostazioni del kernel. Questa è la parte più importante. Se disabilitate le impostazioni sbagliate, potreste non avere più il supporto per alcune caratteristiche o per l'hardware di cui avete bisogno. Comunque, se attivate le impostazioni sbagliate, aumenterete le dimensioni del kernel e sprecherete la preziosa memoria del vostro sistema (probabilmente è meglio sbagliare su quest'ultimo punto che non sul primo).

Il miglior modo per compilare correttamente il kernel è sapere di quali caratteristiche avrete bisogno, e quale hardware avete nel vostro sistema. Dopo che avrete sperimentato un po' di volte la personalizzazione del kernel, questo processo diventerà "banale" e non vi intimorirà più!

Digitate quanto segue per iniziare il processo di configurazione:

```
mail:/usr/include# cd /usr/src/linux
mail:/usr/src/linux# make mrproper
mail:/usr/src/linux# make menuconfig
```

Potete digitare "make xconfig" invece di "make menuconfig" se avete in esecuzione il sistema X Window; si veda il Capitolo 5 per informazioni su come far funzionare X.

Per configurare il vostro kernel, passate attraverso le varie configurazioni e selezionate (attivate) quelli di cui avete bisogno, e deselezionate (disattivate) quelli inutili. Potete scegliere tra l'averne un determinato supporto integrato nel kernel, o averlo come modulo che viene caricato e scaricato dal Kernel a seconda dei bisogni. (Se compilate qualche caratteristica di cui avete bisogno al momento del boot del sistema (come un driver SCSI), come modulo, avrete bisogno di creare una immagine ram disk o il vostro sistema non si avvierà. Questo viene fatto con il comando "mkinitrd"; questa procedura viene descritta più avanti nel documento.

Quando passate tra le varie configurazioni, potete selezionare <Help> per sapere a cosa serve una determinata opzione.

Dopo aver configurato il vostro kernel, digitate quanto segue per compilarlo:

```
mail:/usr/src/linux# make dep ; make clean
mail:/usr/src/linux# make bzImage
mail:/usr/src/linux# make modules
```

Se state *ricompilando* lo stesso kernel che avevate prima (2.0.36-3 nell'esempio), probabilmente vorrete spostare i moduli esistenti in una directory di backup; ecco il comando:

```
mail:/usr/src/linux# mv /lib/modules/2.0.36-3 /lib/modules/2.0.36-3-backup
```

Adesso, digitate questo comando per installare i nuovi moduli:

```
mail:/usr/src/linux# make modules_install
```

Adesso bisogna copiare il kernel nella directory "/boot/" e usare LILO per aggiornare il boot record in modo che il nuovo kernel venga riconosciuto. I comandi che seguono effettueranno una copia di backup del kernel esistente, copieranno il kernel nuovo e poi aggiorneranno il boot record di LILO:

```
mail:/usr/src/linux# cd /boot
mail:/boot# cp vmlinuz vmlinuz.OLD
mail:/boot# cp /usr/src/linux/arch/i386/boot/bzImage vmlinuz-2.0.36
mail:/boot# /sbin/lilo
```

Infine, dovrete editare il file "/etc/lilo.conf" e assicurarvi che "image" punti al nuovo kernel. Dovrete aggiungere anche una sezione che punti al backup del kernel, chiamato, ad esempio, "OldLinux". Ecco un esempio:

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=50
image=/boot/vmlinuz
label=Linux
root=/dev/hdb1
read-only
image=/boot/vmlinuz.OLD
label=OldLinux
    read-only
```

Aggiungendo le informazioni sul kernel di backup, in caso il nuovo kernel non dovesse avviarsi regolarmente (può darsi che un dispositivo non sia stato riconosciuto, oppure un demone non si avvia come dovrebbe), potete semplicemente digitare "oldLinux" per avviare il vecchio kernel e scoprire il problema.

Nota: Come detto prima se avete compilato una caratteristica in modo che venga avviata come modulo, dovrete creare una immagine ram disk iniziale per fare il boot del vostro sistema. Non dimenticate di compilare il kernel con il supporto per questa immagine iniziale.

La procedura per creare e usare un immagine ram disk iniziale è la seguente:

- Aggiungete al file "/etc/lilo.conf" una riga per fare il boot dell'immagine RAMdisk iniziale:

```
image=/boot/vmlinuz
    label=Linux
    root=/dev/hdb1
    initrd=/boot/initrd-2.2.4-4.img
    read-only
```

- Il dispositivo loopback deve essere caricato prima che voi possiate usare il comando mkinitrd. Assicuratevi che il modulo del dispositivo loopback sia caricato:

```
/sbin/insmod loop
```

Se ottenete un messaggio di errore circa l'impossibilità di caricare il modulo loopback, potreste aver bisogno di specificare il percorso completo del modulo per il kernel *corrente* che il vostro sistema sta ancora facendo girare, per esempio "/lib/modules/2.0.35/loop".)

- Usate il comando "mkinitrd" per creare l'immagine:

```
/sbin/mkinitrd /boot/initrd-2.0.36-3.img 2.0.36-3
```

- Eseguite "/sbin/lilo" per aggiornare il vostro boot loader.

A questo punto, spegnete il sistema e fate il boot del nuovo kernel!

```
mail:/boot# /sbin/shutdown -r now
```

Se il kernel si rifiuta di partire completamente, non fatevi prendere dal panico! Utilizzate il boot disk che avete creato durante il processo di installazione di Linux. Se non avete copie di questo disco, dovrete riuscire a crearne uno dal CD di Red Hat. Inserite il dischetto nel drive e fate un reboot. Quando si veda il prompt, digitate:

```
mount root=/dev/hda1
```

Il comando sopra presuppone che la vostra partizione "/" (root) si trovi su /dev/hda1.

Linux dovrebbe avviarsi normalmente (sebbene finché usate il kernel del boot disk, non tutti i servizi o i dispositivi possono funzionare correttamente), e potrete recuperare il vostro vecchio kernel e reinstallare le informazioni del boot loader LILO (cioè "mv /vmlinuz.old /vmlinuz ; /sbin/lilo"), quindi spegnere e riavviare. Potete in un secondo tempo provare a ricompilare il kernel con differenti opzioni e riprovare a farlo funzionare.

10.7. Passare ai kernel Linux 2.2.x

Il kernel Linux 2.2.0 è stato rilasciato il 25 Gennaio 1999 e presenta molte nuove caratteristiche, oltre al miglioramento delle prestazioni e al supporto per l'hardware. Ogni sistema Linux esistente può essere aggiornato con uno di questi kernel come è stato descritto nella Sezione 10.4 (con avvertimenti).

Questa sezione descriverà come aggiornare il vostro sistema Red Hat con i nuovi kernel. Poiché la Red Hat 6.0 (e superiore) già comprende il nuovo kernel e il supporto per i pacchetti, essa potrà essere d'aiuto a quelli di voi che utilizzano ancora una versione precedente, come la 5.2. Quasi certamente, toglierò questa sezione dalla future versioni di questo documento, quando probabilmente la maggior parte degli utenti sarà migrata verso la versione 6.0 o successive.

Attenzione

Se decidete di aggiornare il vostro vecchio sistema in modo che supporti i nuovi kernel, sappiate che poiché tale processo implica l'aggiornamento di un certo numero di pacchetti, è possibile che qualcosa non vada per il verso giusto. Tenete, comunque, sempre a portata di mano dei backup recenti. Se non avete esperienza nell'aggiornamento dei file con RPM e nella compilazione dei kernel, forse dovrete passare direttamente alla Red Hat 6.1.

Potete scegliere tra l'aggiornamento dello stock kernel fornito da Red Hat, o l'aggiornamento mediante compilazione di un kernel personalizzato. Vi raccomando di provare prima con lo stock kernel, e poi a costruire un kernel personalizzato. (Si veda la Sezione 10.5 per maggiori informazioni).

Per utilizzare l'ultima versione del kernel, è necessario, innanzi tutto, aggiornare le utilità e le librerie. Red Hat ha identificato i pacchetti che bisogna aggiornare per supportare il nuovo kernel, e ha messo i file RPM appropriati sul sito FTP <ftp://ftp.redhat.com/redhat/updates/5.2/kernel-2.2/i386/> (per gli utenti di Red Hat 5.2 su piattaforma i386).

Un ottimo sito web con informazioni sugli strumenti necessari per passare a 2.2.x, è disponibile su <http://www-stu.calvin.edu/~clug/users/jnieho38/goto22.html>; Cercherò di farvi un riassunto delle informazioni (le voci con davanti "***" indicano le cose che devono essere aggiornate per Red Hat 5.2; quelle senza, vanno *probabilmente* bene ma è comunque meglio controllarle).

- **** initscripts-3.78-2.4** o superiore (digitate "rpm -q initscripts" per controllare la versione)
- **** modutils-2.1.121** o superiore (digitate "rpm -q modutils" per controllare la versione)
- **** mount-2.9-0** o superiore (digitate "rpm -q mount" per controllare la versione)
- **gcc-2.7.2.3** o superiore ("rpm -q gcc")
- **binutils-2.8.1.0.23** o superiore ("rpm -q binutils")
- **libc-5.4.46** o superiore (Red Hat utilizza le più nuove "glibc". Non necessarie.)
- **glibc-2.0.7-6** o superiore ("rpm -q glibc")
- **ld.so 1.9.9** o superiore ("ls -l /lib/ld.so.*")
- **libg++-2.7.2.8** o superiore ("rpm -q libg++")
- **procps-1.2.9** o superiore ("rpm -q procps")
- **** procinfo-15** o superiore ("rpm -q procinfo")
- **psmisc-17** o superiore ("rpm -q psmisc")
- **** net-tools-1.50** o superiore ("rpm -q net-tools")
- **loadlin-1.6** o superiore (Serve solo se avviate Linux da DOS usando Loadlin. Non sono sicuro sul metodo per il controllo del numero di versione; per stare sicuri scaricate l'ultima versione.)
- **sh-utils-1.16** o superiore ("rpm -q sh-utils")
- **autofs-3.1.1** o superiore ("rpm -q autofs")

- `nfs-server2.2beta37` o superiore ("`rpm -q nfs-server`"; serve solo se usate NFS per condividere file.)
- `bash-1.14.7` o superiore ("`rpm -q bash`")
- `ncpfs-2.2.0` o superiore ("`rpm -q ncpfs`"; serve solo se montate file system Novell.)
- `kernel-pcmcia-cs-3.0.6` o superiore ("`rpm -q kernel-pcmcia-cs`"; serve solo per computer portatili che hanno bisogno del support per la scheda PCMCIA.)
- `ppp-2.3.5` o superiore ("`rpm -q ppp`"; serve solo se vi connettete ad internet con un modem e PPP.)
- `dhcpcd-1.3.16-0` o superiore ("`rpm -q dhcpcd`"; serve solo se avete bisogno di un client DHCP per connettervi ad Internet, come con un cable modem).
- `** util-linux-2.9.0` ("`rpm -q util-linux`")
- `setserial-2.1` o superiore ("`rpm -q setserial`")
- `ipfwadmin/ipchains` (serve solo se fate un IP firewalling; leggete la guida "*IPCHAINS-HOWTO*" su <http://isunix.it.iltu.edu/resources/ldp/HOWTO/IPCHAINS-HOWTO.html>.) [NdT: disponibile in italiano su <http://it.tldp.org/HOWTO/IPCHAINS-HOWTO.html>]

Dovreste scaricare e aggiornare ogni pacchetto usando RPM (si veda la Sezione 10.1 per informazioni su come usare RPM).

Cautela

Aggiornare il pacchetto "modutils" renderà i moduli non più funzionanti per i vecchi kernel 2.0.x! Quindi, non aggiornatelo finché non avete installato in nuovo kernel in "`/usr/src/linux`".

Dopo aver aggiornato i vostri strumenti di sistema, potete installare i sorgenti del kernel. Potete reperirli anche sul sito FTP di Red Hat; Vi raccomando di scaricare quelli forniti come aggiornamenti per Red Hat 6.1: <ftp://ftp.redhat.com/redhat/updates/6.1/i386/>. Digitate, poi, quanto segue:

```
rpm -Uvh kernel-source*.rpm kernel-headers*.rpm
```

Adesso che i sorgenti del nuovo kernel sono stati installati, potete aggiornare in tutta tranquillità anche il pacchetto modutils. Tuttavia, il nuovo kernel non usa più il modulo "kerneld" per il caricamento dei moduli richiesti. Quindi, dovete disabilitare questo modulo prima di aggiornare modutils. Per far ciò, digitate da "root":

```
/sbin/chkconfig kerneld off
/etc/rc.d/init.d/kerneld stop
rpm -Uvh modutils*.rpm
```

Dovreste, adesso, essere in grado di configurare, compilare e installare il vostro kernel 2.2 (si veda la Sezione 10.6 per maggiori informazioni). Potreste rimanere alquanto sorpresi dal gran numero di nuovi parametri di configurazione. Prendetevi un po' di tempo e leggetevi l'help per ogni nuova opzione che non conoscete.

Con un po' di fortuna, la prossima volta che avvierete il vostro sistema, vi troverete a cimentarvi con l'ultimissima versione del kernel di Linux!

Potete trovare tante altre informazioni su queste procedure direttamente sul sito di Red Hat: <http://www.redhat.com/corp/support/docs/kernel-2.2/kernel2.2-upgrade.html>.

10.8. Configurare il web server Apache

Sul mio posto di lavoro, utilizziamo il pacchetto Apache per fornire servizi web. Apache è un web server completo che offre completo supporto a HTTP 1.1 standard, proxy caching, pagine web con autenticazione di password, e

molte altre cose. Apache è uno dei più popolari web server disponibili (secondo un studio recente di Netcraft, più del 54% di tutti i siti web di Internet usano Apache o suoi derivati), e offre prestazioni paragonabili, o anche meglio, rispetto a quelli commerciali.

(In costruzione. :-p)

Per mantenervi aggiornati sulle novità e sulla correzione di alcuni bug di Apache è consigliabile, di tanto in tanto, aggiornare il vostro server. Il sito web di Apache è <http://www.apache.org/> e contiene informazioni sulle ultime versioni.

10.9. Configurare il demone Squid HTTP caching proxy

Sul mio posto di lavoro, utilizziamo il pacchetto Squid per fornire il proxy caching delle pagine web. Squid offre prestazioni elevate di caching di client web, e supporta anche FTP, Gopher, e richieste HTTP. In più, Squid può essere collegato gerarchicamente ad altri proxy server basati su Squid, in modo da semplificare il caching delle pagine.

Ci sono, attualmente, due versioni di Squid. Una, quella “regolare”, sembra funzionare egregiamente su macchine con molta RAM. La seconda, “*SquidNOVM*” è adatta per macchine con meno RAM (vi suggerisco di usare questa versione se avete 64 Mb, o meno, di RAM). Sostanzialmente, la versione “NOVM” usa meno memoria al costo di più file di classificazione. È quella che uso, e funziona bene.

(In costruzione :-p)

Per restare aggiornati sulle ultime novità e sulla correzione di alcuni bug è consigliabile, di tanto in tanto, aggiornare il vostro server Squid. Maggiori informazioni su Squid a <http://squid.nlanr.net/Squid/>.

10.10. Configurare il demone per le e-mail Sendmail

Utilizzo il pacchetto Sendmail per fornire servizi di e-mail. Sendmail è il gestore di posta per definizione, infatti è talmente popolare che più dell’80% dell’e-mail su Internet vengono gestite da esso, da una o da entrambe le parti. Si occupa di tutto e non riesco ad immaginarmi un server Internet senza di esso (un altro server di posta, chiamato Qmail, sembra essere abbastanza popolare, ma non ho ancora trovato una ragione per passare ad esso).

Per restare aggiornati sulle ultime novità e sulla correzione di alcuni bug e soprattutto, per ragioni di sicurezza, è consigliabile, di tanto in tanto, aggiornare Sendmail. In più, l’ultimissima versione di Sendmail comprende eccellenti strumenti anti-spam che potrebbero aiutarvi a impedire che utenti non autorizzati abusino del vostro server di posta.

Questa sezione descriverà alcune delle cose che dovrete fare se avete intenzione di utilizzare Sendmail come server per le e-mail in entrata. Vi descriverò un possibile scenario. Se, invece, non ne avete bisogno per la posta in entrata ma solo per quella in uscita, allora dovrete...((ho bisogno di informazioni, a questo punto!)).

Consideriamo che voi abbiate l’ultima versione di Sendmail (8.9.3 al momento in cui scrivo) installata e funzionante.

Poiché è presente nella distribuzione di Red Hat, Sendmail di solito contiene informazioni di configurazione adatte per funzionare con la maggior parte delle configurazioni dei server. Tuttavia, potreste dovere editare il file `"/etc/sendmail.cf"` per personalizzare alcune parametri secondo i vostri bisogni. Tutto ciò, comunque, va oltre gli scopi di questo testo.

Tuttavia una cosa che reputo utile, al fine di ostacolare gli spammer, è quella di apportare un paio di modifiche:

```
O PrivacyOptions=authwarnings  
change to:
```

```
O PrivacyOptions=authwarnings,noexpn,novrfy

O SmtpgreetingMessage=$j Sendmail $v/$Z; $b
change to:
O SmtpgreetingMessage=$j Sendmail $v/$Z; $b NO UCE C=xx L=xx
```

La prima modifica impedisce agli spammer di usare i comandi di sendmail "EXPN" e "VRFY". Ho scoperto che questi comandi sono spesso utilizzati da individui disonesti. Il secondo cambiamento modifica il banner che Sendmail mostra subito dopo aver ricevuto una connessione. Dovete cambiare "xx" in "C=xx L=xx" con i codici del vostro paese e della vostra località. Per esempio, io userò "C=CA L=ON" per Ontario, Canada. (Il secondo cambiamento non dà alcun effetto, ma è stato raccomandato dalle persone del newsgroup news.admin.net-abuse.email (news:news.admin.net-abuse.email) come precauzione di tipo legale).

Successivamente, se il vostro server di posta avrà un host name diverso da quello della macchina sul quale sta girando, potrete aggiungere uno o più alias nel file "/etc/sendmail.cw". Per esempio, se avete un sistema che si chiama "kirk.mydomain.name" impostato per scambiare la posta per mydomain.name, e volete che l'indirizzo della posta in entrata sia nel formato "user@mydomain.name" per smistarla agli utenti di "kirk", aggiungete semplicemente questo alias:

```
mydomain.name
```

Infine, se volete limitare l'accesso, al servizio sendmail, di un dominio (o sotto-dominio), potete editare il file "/etc/mail/access" e aggiungere le informazioni sul dominio e il tipo di limitazioni. Per esempio:

```
some.domain REJECT
hax0r.another.domain 550 Contact site administrator at (555) 555-1234.
```

L'esempio sopra rifiuterà tutte le connessioni e-mail dal sito "some.domain", come pure dalla macchina con nome "hax0r.another.domain", mostrando un messaggio.

Dopo aver effettuato modifiche a questo file, dovrete aggiornare il file "access.db" e riavviare sendmail in questo modo:

```
/usr/sbin/makemap hash /etc/mail/access.db < /etc/mail/access
/etc/rc.d/init.d/sendmail restart
```

Suggerimento: Se siete preoccupati per un possibile uso illecito delle e-mail, potete reperire utili informazioni dal progetto "Mail Abuse Prevention System" (MAPS) che si occupa proprio di questo; consultate il sito web <http://www.mail-abuse.org/>

Se state usando Sendmail 8.9 o superiore, il supporto RBL è già compreso, ma di default non attivo. Per attivarlo aggiungete quanto segue al file sendmail.mc:

```
FEATURE(rbl)
```

Poi riconfigurate e riavviate il demone Sendmail.

Maggiori informazioni su <http://www.mail-abuse.org/rbl/usage.html>.

Talvolta un dominio può finire nella lista RBL nonostante vogliate continuare a comunicare con esso. Potrebbe forse essere vitale per voi comunicare con alcuni utenti di domini presenti nella black-list. In questo caso, Sendmail vi permette di ignorare questi domini in modo da continuare a ricevere le loro e-mail. Editate semplicemente il file "/etc/mail/access" nel modo descritto inserendo le informazioni sul dominio. Per esempio:

```
blacklisted.domain OK
```

Non dimenticate di aggiornare il vostro file `access.db` (descritto sopra)!

Se decidete di iscrivervi all'RBL, vi consiglio di informare i vostri utenti in modo che, se non si dovessero trovare d'accordo con la vostra decisione, possano fare i preparativi per usare un altro servizio.

Per maggiori informazioni su Sendmail, date un'occhiata alle FAQ su: <http://www.sendmail.org/faq/>.

Capitolo 11. Linux in azienda

Dato che Linux si è fatto una solida reputazione grazie alla sua stabilità e affidabilità, viene usato per applicazioni molto importanti sia nella aziende e sia nel mondo scientifico.

Questo capitolo tratterà le questioni più rilevanti riguardo all'utilizzo di Linux nelle aziende, come la messa appunto delle prestazioni per grossi carichi di lavoro, il mantenimento al sicuro dei vostri dati tramite le tecnologie RAID e infine, una discussione generale su come passare da un server ad un altro.

11.1. Messa a punto delle prestazioni

(In costruzione. :-p)

11.2. Alta disponibilità con RAID

Quando la necessità di immagazzinare dati cresce, diventa talvolta necessario aggiungere dischi a più elevata capacità. Il calcolo delle probabilità afferma che quando il numero dei componenti hardware destinati a immagazzinare dati aumenta, aumenta anche la probabilità di qualche malfunzionamento. Quindi, un sistema con un solo hard-disk ha solo il 25% di probabilità di rompersi rispetto ad un sistema con quattro dischi. [Almeno teoricamente :-)]

Fortunatamente questi malfunzionamenti possono essere gestiti tranquillamente e, soprattutto, senza periodi morti, usando una tecnica chiamata "Redundant Array of Inexpensive Disks" (*RAID*) (letteralmente "Eccesso di dischi a buon mercato" n.d.t.) che utilizza uno dei diversi metodi di distribuzione di dati su più dischi. La ridondanza permette di recuperare automaticamente i dati in caso di malfunzionamento di un disco.

Questa sezione descriverà l'installazione e la configurazione di un apparato RAID tramite il controller Mylex AcceleRAID DAC960. Sono rimasto molto impressionato non solo dalle prestazioni e dalla stabilità del controller, ma anche dal supporto tecnico che ho avuto da Mylex -- devo dire che sono molto ben disposti verso Linux! Comunque esiste una grande varietà di hardware RAID per Linux, e RAID può essere implementato nei software mediante il kernel di Linux. Il tipo d'implementazione di RAID più utilizzato è, probabilmente, il RAID level 5.

Il primo passo per usare un controller RAID sotto Linux è quello di aggiungere al kernel il driver per il nuovo hardware. Il driver per Mylex DAC960 può essere scaricato dal sito web di Dandelion Digital Linux su <http://www.dandelion.com/Linux/DAC960-2.0.tar.gz>.

L'ultimo passo per utilizzare un apparato RAID sotto Linux è quello di servirsi dell'utilità "fdisk" per creare partizioni valide. Per tale operazione vale lo stesso discorso fatto per usare dischi IDE o SCSI. Si veda la Sezione 4.3 per informazioni sulle impostazioni della partizioni.

Nota: Il driver DAC960 supporta massimo 7 partizioni per ogni disco logico. Se avete bisogno di altre, dovrete definire dischi logici multipli nell'utilità di configurazioni di RAID (premete <Alt>-<R> al momento del boot per entrare nel setup).

Uno volta che siete in grado di vedere il vostro apparato RAID, dovrete inizializzare ogni area di swap e ogni file system che volete definire. Quanto segue è un esempio di inizializzazione di un area di swap sulla terza partizione del secondo disco, così come un file system (ext2) sulla prima partizione del primo disco:

```
/sbin/mkswap -c /dev/rd/c0d1p3
/sbin/swapon /dev/rd/c0d1p3
/sbin/mkfs.ext2 -c /dev/rd/c0d0p1
```

Nota: Note: L'opzione "-c" nei comandi "mkswap" e "mkfs.ext2" attivano il controllo dei bad-block quando vengono creati gli swap/file system. Questo *sostanzialmente* comporta maggior tempo per completare il processo, ma è una buona soluzione per effettuare questi controlli.

Per ogni nuova area di swap, dovrete aggiungere un riga al file "/etc/fstab" per fare in modo che vengano utilizzate fin dal successivo boot-up. Nel caso del nostro esempio, dovrete aggiungere la seguente riga:

```
/dev/rd/c0d1p3 swap swap defaults 0 0
```

Infine, dopo che i vostri file system sono stati inizializzati, potete creare i mount point e spostare sul sistema, come meglio desiderate, i vostri enormi file system. È un buona idea verificare, per alcuni giorni, che tutto funzioni bene prima di usarlo in un ambiente di produzione.

Per maggiori informazioni sul controller Mylex AcceleRAID visitate il sito web <http://www.mylex.com/> e le pagine relative al driver Dandelion Digital DAC960 su <http://www.dandelion.com/Linux/DAC960.html>. Per altre informazioni su RAID visitate il sito web Linux High Availability su <http://linas.org/linux/raid.html>.

11.3. Migrazione di Server e questioni di scalabilità

Con il supporto per molti dispositivi hardware e grazie ad una comprovata velocità e affidabilità, Linux è in prima linea per quanto riguarda la possibilità di soddisfare ogni possibile esigenza. Compreso il passaggio ad una configurazioni SMP (*Symmetric Multi Processing*) per grandi elaborazioni, RAID levels da 0 a 5 (in modalità sia hardware sia software), ecc.

Ogni tanto potreste ritenere che al vostro server Linux gli stia stretto l'hardware su cui gira. Allora, o lasciate il vostro server con l'hardware esistente oppure aggiornato (nel qual caso chiudete i servizi, fate il backup dei vostri dati, eseguite le modifiche e, se ne avete bisogno, effettuate il restore dei dati), oppure più radicalmente spostate il server verso un nuovo hardware.

Questa sezione sarà incentrata sull'ultimo aspetto, quando sposterete i vostri servizi da un vecchio server ad uno nuovo. Ci sono diverse strategie di migrazione, ma cercherò di darvi delle linee guida da seguire per fare in modo che i vostri sforzi abbiano successo con pochi fastidi per i vostri utenti.

- Preparate bene il vostro nuovo server; installate e configurate Linux in modo che tutto il nuovo hardware venga supportato e che ogni demone e ogni caratteristica del kernel di cui avete bisogno (come il firewall) sia attivata. Maggiori dettagli nel Capitolo 4 e nella Sezione 10.6.
- Impostate i vostri servizi (come il web server Apache web server, Samba o Netatalk) e provateli per diversi giorni per assicurarvi che tutto funzioni come si deve. Maggiori dettagli nella Sezione 7.4 e nella Sezione 7.5. Non dimenticate di fare gli stessi eventuali cambiamenti che avete fatto nella directory "/etc/", compreso "/etc/rc.d/" anche sul nuovo server. È oltretutto importante trasferire le informazioni su gli account degli utenti presenti nei file "/etc/passwd", "/etc/group" e "/etc/shadow", se utilizzate le shadow password!
- Chiudete i servizi sul vostro vecchio server, di modo che l'attività di aggiornamento dei file sia ridotta all'osso. Non vorrete mica che i vostri utenti trasferiscano le loro pagine web e ricevano le e-mail sul vecchio server mentre

state reintroducendo i dato su quello nuovo ?! Come root, potete arrestare la maggior parte dei servizi con il seguente comando:

```
killall httpd atalkd smbd nmbd squid sendmail ftpd
```

In questo modo chiuderete il web server, i servizi di file & print, il server di posta e il servizio FTP (quello sopra è solo un esempio, controllate la lista dei vostri processi e terminate tutti i processi che ritenete opportuno; si veda la Sezione 9.2 per maggiori informazioni).

Potreste anche voler editare il file `/etc/inetd.conf` sul vostro vecchio server, e decommentare con il carattere `#` qualunque servizio (FTP, IMAP, e i servizi POP3) che potrebbe andare a finire negli aggiornamenti del file system. Quindi, come root, digitate:

```
killall -HUP inetd
```

Il comando sopra ricaricherà i wrapper TCP (wrapper di sicurezze per i servizi Internet) in modo che non saranno caricate le future connessioni a qualunque servizio abbiate disabilitate nel file `/etc/inet.conf`).

- Ora dovrete essere in grado di spostare i dati da un sistema ad un altro. Probabilmente, avrete fornito il vostro nuovo server tutto l'occorrente per funzionare, compreso ogni software di cui avete bisogno e che non è incluso nella vostra distribuzione Red Hat. Quindi, avrete probabilmente bisogno di fare il backup di ogni dato presente in `/home`, `/var/spool` e `/archive`, se possibile. Di seguito vi fornisco un esempio di comando che utilizza l'utilità `tar` per effettuare un file compresso di backup dei dati:

```
cd /
tar zcvpf /tmp/backup_data.tar.gz --exclude=var/spool/squid \
    home archive var/spool
```

Ciò creerà un file compresso di backup, in formato tar, di nome `/tmp/backup_data.tar.gz` contenente i filesystem `/archive`, `/home` e `/var/spool` (o subdirectory, dipende da come avete configurato il vostro sistema). Assicuratevi di avere abbastanza spazio per il backup, altrimenti scrivetelo da qualche altra parte!

Suggerimento: Potete usare l'utilità `du` per aiutarvi a determinare di quanto spazio abbiate bisogno. Per esempio, per determinare lo spazio necessario per le directory `/archive/` e `/home/` digitate:

```
du -h -s /archive /home
```

Tenete presente il comando sopra vi fornirà le dimensioni effettive dei vostri dati, ma se usate l'opzione `z` di `tar` per comprimere il file immagine, avrete probabilmente bisogno di meno spazio. Considerate l'output del comando `du` come indicazione di massima sullo spazio necessario.

- Adesso potete fare il restore dei dati, contenuti nel file tar, sul vostro nuovo server. Potete farlo direttamente su NFS (si veda la Sezione 7.6 per maggiori informazioni su come configurare NFS), oppure utilizzate FTP per trasferire il file e poi scompattarlo localmente. Ecco un esempio di come fare il ripristino dei dati di cui abbiamo fatto il backup poco fa:

```
cd /
tar zxvpf /tmp/backup_data.tar.gz
```

- Successivamente, se necessario, cambiate i vostri indirizzi IP in modo che al vecchio indirizzo compaia il vostro nuovo server.

- Infine, chiudete e riavviate il vostro server per assicurarvi che non appaiano messaggi di errore. Si veda la Sezione 6.7 per maggiori informazioni.

Quando avete finito, controllate che tutto funzioni correttamente! In caso contrario potete sempre riattivare qualunque servizio sul vecchio server in modo che gli utenti possano continuare ad utilizzarli mentre voi risolvete i problemi sul server nuovo. (Considerate, però, che se deciderete di farlo vi toccherà ripetere, dall'inizio, tutti i passi descritti sopra).

Capitolo 12. Strategie per mantenere un server sicuro

Linux può essere certamente considerato come sicuro o almeno più sicuro di altri sistemi operativi. Il crescente interesse per Linux ha fatto sì che molti crackers spendessero molte energie nel tentativo di trovarvi delle falle. Ci sono stati, in tempi passati, alcuni exploit, ma la natura open di Linux ha permesso di porvi riparo molto rapidamente, con soluzioni temporanee o con aggiornamenti software.

Non pretendo di essere un esperto di questioni di sicurezza ma, quanto meno, me ne sono interessato dato che credo che siano fondamentali per rendere un sistema quanto più sicuro possibile.

Sebbene ci siano stati alcuni exploit, trovati in alcuni servizi, che avrebbero potuto permettere ai crackers di accedere ad un sistema (ad esempio quello del demone IMAP), credo sia più probabile che qualche cracker penetri un sistema *dall'interno*. Rispetto ai pochi servizi che comunicano con il mondo esterno, ci sono *migliaia* di comandi e di utilità, disponibili dalla shell, che probabilmente contengono bug che consentono di aggirare le misure di sicurezza (anche se devo ammettere di aver scoperto che uno dei server da me mantenuti è stato compromesso attraverso un servizio esterno).

Per questa ragione, vi raccomando di dare account di shell agli utenti solo se assolutamente necessario. Anche se considerate i vostri utenti persone completamente affidabili, basta che uno di essi abbia una password molto facile. Un cracker esterno, sfruttando la debolezza di questa password, potrebbe agire con tutta calma cercando di scoprire poi altri punti deboli.

Fortunatamente potete far cose che aumenteranno sensibilmente la sicurezza del vostro sistema Linux. Poiché una discussione dettagliata sulle questioni di sicurezza esula dallo scopo di questa documentazione, la lista che segue fornisce brevi indicazioni su cosa fare per aumentare la sicurezza:

- *Aggiornare gli strumenti di sistema, le applicazioni ed il kernel*: la causa più comune di irruzione nei sistemi dipende dal mancato mantenimento di un server sempre aggiornato. Effettuare regolari aggiornamenti del kernel, degli strumenti e delle utilità garantisce l'eliminazione, dal vostro sistema, di elementi per i quali sono già noti degli exploit. Per informazioni su come mantenere un server sempre aggiornato, si veda la Sezione 4.9 e la Sezione 10.3.
- *Shadow passwords*: vi consiglio caldamente di utilizzare le Shadow password; passare a questo formato è davvero molto *facile*. Maggiori dettagli nella Sezione 6.6.
- *Uso intelligente delle password*: assicuratevi che le password, *specialmente* quelle degli utenti a cui fornite accesso alla shell, siano difficili da individuare e cambiate spesso. Inoltre, se usate server multipli, resistete alla tentazione di utilizzare sempre la stessa password (altrimenti, se un cracker accede ad un server dopo aver scoperto un password, potrebbe accedere facilmente anche a tutti gli altri).
- *Usate la secure shell (ssh)*: passate a "ssh" invece di "telnet". Telnet non è sicuro per due ragioni: Primo, le sessioni non sono criptate, quindi tutto quello che viene trasmesso, compreso password e username, è in chiaro. Secondo, la prima cosa che fa un cracker è quella di provare a connettersi ad un porta telnet aperta.

Ssh fornisce connessioni criptate e compresse, offre quindi più sicurezza rispetto a telnet. Potete utilizzare un server ssh (che permette connessioni sicure in entrata) anche come client (per connessioni, in uscita, sicure) sotto Linux. Potete reperire il pacchetto RPM su <ftp://ftp.replay.com/pub/replay/redhat/i386/>. Avrete bisogno dei seguenti file (è possibile che siano disponibili versioni più recenti al momento in cui state leggendo):

- `ssh-1.2.27-5i.i386.rpm` (<ftp://ftp.replay.com/pub/replay/redhat/i386/ssh-1.2.27-5i.i386.rpm>) Il pacchetto di base.

- ssh-clients-1.2.27-5i.i386.rpm (<ftp://ftp.replay.com/pub/replay/redhat/i386/ssh-clients-1.2.27-5i.i386.rpm>)
Client per connessioni verso l'esterno.
- ssh-extras-1.2.27-5i.i386.rpm (<ftp://ftp.replay.com/pub/replay/redhat/i386/ssh-extras-1.2.27-5i.i386.rpm>)
Alcuni pratici script Perl.
- ssh-server-1.2.27-5i.i386.rpm (<ftp://ftp.replay.com/pub/replay/redhat/i386/ssh-server-1.2.27-5i.i386.rpm>)
Server per le connessioni in entrata.

Nota: Il file RPM di SSH elencati sopra si riferiscono alla versione internazionale. Se abitate negli Stati Uniti o in Canada, potete scegliere di scaricare i pacchetti per gli U.S.A. (che potrebbero avere algoritmi di criptazione più robusti); questi pacchetti hanno il suffisso "us" invece di quello "i" subito dopo i numeri della versione. Per la legge U.S., è *illegale* esportare prodotti molto complessi per la criptazione fuori dagli Stati Uniti o dal Canada. Speriamo che un giorno gli imbecilli che fanno parte del dipartimento di giustizia degli U.S.A. escano dal tunnel e tolgano questa stupida restrizione. Red Hat non include SSH nella sua distribuzione appunto per questo motivo, infliggendo a *tutti* molta sofferenze).

Se i vostri utenti Windows dovessero lamentarsi di non riuscire più a connettersi al vostro sistema, fategli sapere che esistono alcuni client ssh completamente gratuiti:

“TeraTerm Pro” client software

<http://hp.vector.co.jp/authors/VA002416/teraterm.html>

“TTSSH” client software

<http://www.zip.com.au/~roca/download.html>

“Cryptlib” client software

<http://www.doc.ic.ac.uk/~ci2/ssh>

“Putty” client software

<http://www.chiark.greenend.org.uk/~sgtatham/putty.html>

Nota: Se decidete di passare a ssh assicuratevi di installarlo e usarlo su *tutti* i vostri server. Avere cinque server sicuri e uno no è solo un perdita di tempo, *specialmente* se siete abbastanza stupidi da usare la stessa password per più di un server.

- *Accesso limitato ai servizi esterni:* successivamente, dovete editare i file `"/etc/hosts.allow"` e `"/etc/hosts.deny"` per limitare l'accesso a servizi su host esterni. Di seguito vi fornisco un esempio di come limitare l'accesso telnet e ftp. Innanzitutto il file `"/etc/hosts.allow"`:

```
# hosts.allow
```

```
in.telnetd: 123.12.41., 126.27.18., .mydomain.name, .another.name
in.ftpd: 123.12.41., 126.27.18., .mydomain.name, .another.name
```

Questo permetterà connessioni telnet e ftp a tutti gli host con classi IP 123.12.41.* e 126.27.18.*, oltre che ai domini mydomain.name e another.name.

Quindi, il file `/etc/hosts.deny`:

```
# hosts.deny
in.telnetd: ALL
in.ftpd: ALL
```

- *Chiudete e disinstallate ogni servizio non necessario*: Editate il file `/etc/inetd.conf` e disabilitate (cioè decommentate con il carattere "#") ogni servizio non necessario (se state usando ssh, come raccomandato sopra, potreste voler disabilitare il servizio telnet). Fatto ciò, digitate come root `/etc/rc.d/init.d/inet restart` per riavviare il demone inetd con le nuove impostazioni.
- *Installate un security detection system*: Considerate l'idea di installare programmi di sicurezza come "Tripwire" (<http://www.tripwiresecurity.com/>) che può scoprire eventuali intrusioni, e "Abacus Sentry" (<http://www.psionic.com/abacus/>) che può aiutare a prevenirle.
- *Normale diligenza*: Tenete gli occhi aperti sul vostro sistema effettuando, a caso, controlli sulla sicurezza (esaminando ad esempio i file delle password, la lista dei vostri processi, oppure controllando i file di log per verificare la presenza di dati sospetti). In più riferite, alla autorità preposte, ogni tentativo di irruzione. Lo so che potrebbe essere una scocciatura, soprattutto se il vostro sistema riceve molti attacchi in una settimana, ma questi report servono a scoraggiare, con la prospettiva di dover scontare una pena, i possibili cracker. Inoltre, assicurano maggior sicurezza anche a sistemi di altre persone (che potrebbe essere stati a loro volta compromessi).
- Posto che installiate e aggiorniate i vostri strumenti di sistema e le vostre applicazioni ricorrendo all'uso dell'utilità "RPM", potreste voler controllare l'integrità dei pacchetti installati con il seguente comando:

```
rpm --verify -a > /tmp/rpm-audit.txt
```

Il comando sopra confronterà tutti i file importanti con il database RPM del vostro sistema e indicherà, con un '5', tutti i file che sono stati modificati. Di seguito un esempio di un possibile output:

```
S.5...T /bin/ls
S.5...T /usr/bin/du
.....G. /dev/tty5
.....U.. /dev/vcs5
.....U.. /dev/vcsa5
S.5...T c /etc/lynx.cfg
S.5...T c /etc/sendmail.cf
```

Nell'esempio, potete vedere una lista di sette file, quattro dei quali sono stati modificati. Naturalmente ci saranno, con tutta probabilità, molti file modificati se avete provveduto a personalizzare il vostro sistema secondo le vostre necessità. Un breve controllo dei file `/etc/lynx.cfg` e `/etc/sendmail.cf`, a vista o da backup, potrebbero rivelare i cambiamenti legittimi che avete apportato al vostro sistema.

Notate, comunque, che due dei file modificati dell'esempio sono *eseguibili binari*. È probabile che questi due binari, i comandi "ls" e "du", siano adesso dei trojan che un cracker ha installato per scopi malevoli. L'uso del comando "diff" tra i binari modificati e quelli recuperati da un backup o da RPM potrebbe rivelare differenze di dimensione oppure altro; ulteriori evidenze della presenza di trojan.

(Per maggiori informazioni sugli "RPM", si veda la Sezione 10.1)

Per ulteriori informazioni su questioni di sicurezza, una risorsa eccellente, intitolata "Securing RedHat 5.x" è disponibile su <http://redhat-security.ens.utulsa.edu/>. Una eccellente risorsa sulla criptazione con Linux, e sui i software relativi, su <http://replay.com/redhat/> (<http://replay.com/redhat/>).

Capitolo 13. Aiuto! Il paradiso mi annoia!

Linux si sta guadagnando una reputazione a livello mondiale per le sue prestazioni e per la sua affidabilità. Tuttavia, nessun sistema è perfetto, e prima o poi potreste incappare in qualche imprevisto. Fortunatamente, anche se potrebbero verificarsi dopo mesi (o non dopo giorni o settimane come per NT), sono decisamente molto rari.

13.1. Installare Linux su hardware non supportato

(In costruzione :-p)

13.2. File System corrotto dopo un crash di sistema o un'interruzione di corrente elettrica

Anche se Linux è un sistema operativo stabile, potrebbe verificarsi, in maniera del tutto inaspettata, un crash di sistema (vuoi per un bug del kernel oppure per la mancanza di corrente elettrica). Il vostro file system non sarà stato "smontato" e al riavvio di Linux verrà automaticamente controllato, alla ricerca di errori.

Nella maggior parte dei casi, il controllo del file system permette di scoprire e riparare le anomalie in maniera del tutto automatica. Fatto questo, il processo di boot di Linux continuerà normalmente.

Se il problema, invece, è più grave (perché ad esempio per un problema hardware), il controllo del file system potrebbe non essere in grado di riparare il problema automaticamente. Questo è il caso tipico di un file system corrotto. In questo caso il processo di boot della Red Hat mostrerà un messaggio di errore e vi fornirà una shell per permettervi di risolvere i problemi del sistema manualmente.

Dato che la shell smonta prima tutti i file system, e poi monta il file system root "di sola lettura", avrete la possibilità di controllare a fondo il file system con le apposite utilità. Potrete eseguire `e2fsck` sui file system corrotti e ciò dovrebbe consentirvi di risolvere tutti i problemi.

Dopo che avrete (si spera) messo a posto i problemi di ogni file system, uscite semplicemente dalla shell per fare il reboot del sistema e provare a farlo ripartire.

Naturalmente, in caso di problemi che non permettono di recuperare il file system, dovrete utilizzare:

- Il boot/root disk d'emergenza, *AND/OR*
- Il LILO boot disk d'emergenza, *AND*
- Una recente copia di backup dei vostri file più importanti!

13.3. A chi rivolgersi per chiedere aiuto

Dato che Linux viene sviluppato dai membri della comunità internet, il miglior modo per essere aiutati è quello di inviare un messaggio ad uno dei seguenti newsgroup (in Italiano `it.comp.os.linux.*`)

Messaggi vari non coperti da altri gruppi

`comp.os.linux.misc` (`news:comp.os.linux.misc`)

Tutto ciò che riguarda il networking sotto Linux

`comp.os.linux.networking` (news:comp.os.linux.networking)

Tutto ciò che riguarda la sicurezza sotto Linux

`comp.os.linux.security` (news:comp.os.linux.security)

Installazione e amministrazione di Linux

`comp.os.linux.setup` (news:comp.os.linux.setup)

Ognuno può esprimere la propria opinione:-p

`alt.linux.sux` (news:alt.linux.sux)

Per tutti i topic che non riguardano Linux nello specifico, esiste una varietà di gruppi nella gerarchia comp.* che potrebbe esservi utili. Ecco alcuni di essi:

Prodotti Cisco router/access-server

`comp.dcom.sys.cisco` (news:comp.dcom.sys.cisco)

Domande varie sui web server

`comp.infosystems.www.servers.misc` (news:comp.infosystems.www.servers.misc)

Domande su unix (non specifiche su Linux)

`comp.os.unix` (news:comp.os.unix)

Il protocollo SMB (WfW/95/NT-style file/print services)

`comp.protocols.smb` (news:comp.protocols.smb)

Ci sono anche altre risorse sul web che potrebbero essere utili. Fate una ricerca con la parola "Linux" o visitate uno di questi siti:

Risorse Linux

<http://www.linuxresources.com/>

Il Progetto di documentazione Linux

<http://metalab.unc.edu/LDP/>

Deposito di pacchetti RPM

<http://rufus.w3.org/linux/RPM/>

La mappa dei software per Linux

<http://www.boutell.com/lsm>

Guide per applicazioni e utilità Linux

<http://www.xnet.com/~blatura/linapps.shtml>

LinuxHardware.net: Driver di supporto ad hardware

<http://www.linuxhardware.net/>

Team per il supporto a Linux

<http://www.ch4549.org/lust>

Quartier generale per le informazioni alla versione 2 di Linux

<http://www.linuxhq.com/>

La Home Page di Samba (WfW/95/NT-style file/print services)

<http://samba.anu.edu.au/samba/>

Il web server Apache

<http://www.apache.org/>

Il demone per il proxy caching HTTP Squid

<http://squid.nlanr.net/Squid/>

Ci sono tantissime mailing list per trovare una risposta alle vostre domande. Potete trovarle con una semplice ricerca sul web (ad esempio: se scrivete "*linux raid mailing list*" potrete trovare mailing list che si occupano di RAID sotto Linux). Di solito per iscriversi ad una di esse basta mandare un e-mail all'indirizzo fornito per la sottoscrizione, inserendo la parola "*subscribe*" nel corpo del messaggio.

Red Hat Mailing Lists

Liste disponibili per Red Hat: <http://www.redhat.com/> (<http://archive.redhat.com/>)

GNOME Mailing Lists

Liste disponibili per GNOME: <http://www.gnome.org/mailling-lists/index.shtml>

KDE Mailing Lists

Liste disponibili per KDE: <http://www.kde.org/contact.html>

Linux SCSI Mailing List

Indirizzo di sottoscrizione: linux-scsi-request@vger.rutgers.edu (<mailto:linux-scsi-request@vger.rutgers.edu>)

Linux RAID Mailing List

Indirizzo di sottoscrizione: linux-raid-request@vger.rutgers.edu (<mailto:linux-raid-request@vger.rutgers.edu>)

Infine potrebbe essere interessante visitare questi due siti, che io "consulto quotidianamente". SlashDot si occupa delle ultime notizie tecnologiche in generale, ma con un certo riguardo a Linux. Invece FreshMeat offre una lista aggiornata delle applicazioni Open Source che stanno per essere rilasciate.

SlashDot: News per nerds

<http://slashdot.org/>

FreshMeat: Annunci di applicazioni Open Source

<http://freshmeat.net/>

13.4. Riferimenti ad altra documentazione

Ci sono tonnellate di documentazione disponibile per Linux e per le sua applicazioni. Molte di queste possono essere reperite sul web e nelle librerie della vostra città, ma vi accorgete che una grande quantità di utile documentazione è già a vostra disposizione, caricata direttamente come parte della procedura d'installazione di Red Hat.

Le "pagine man" sono indispensabile per capire il funzionamento di qualunque comando. Per esempio, se volete capire come utilizzare l'utilità "tar" basta che digitiate "man tar" ed ecco apparire una lunga descrizione di tar comprensiva di tutte le possibili opzioni.

Potete trovare informazioni più generali nella directory `/usr/doc/`. Troverete delle subdirectory con documentazione su utilità e comandi, le FAQ (Frequently Asked Questions) e gli HOWTO con tante informazioni sugli argomenti più disparati, come il settaggio per il networking o l'implementazione del supporto per la lingua giapponese.

Date un'occhiata anche alla directory `/usr/info/` che contiene tutorial sulle utilità, le librerie e le applicazioni come emacs.

In ultimo, visitate il Red Hat User's Frequently Asked Questions (FAQ) su <http://www.pobox.com/~aturner/RedHat-FAQ/> che contiene moltissime informazioni specifiche per la distribuzione Red Hat.