Red Hat Enterprise Linux 4

Reference Guide

Red Hat Enterprise Linux 4: Reference Guide


Red Hat, Inc.

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

rhel-rg(IT)-4-Print-RHI (2004-09-25T17:13)

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

Sommario

Introduzione i

1. Modifiche al manuale i
2. Informazioni specifiche sull'architettura ii
3. Ricerca della documentazione idonea ii
    3.1. Documentazione per gli utenti inesperti ii
    3.2. Documentazione per i più esperti iv
    3.3. Documentazione per i guru di Linux iv
4. Convenzioni del documento iv
5. Attivate la vostra sottoscrizione vii
    5.1. Fornite un login di Red Hat viii
    5.2. Fornite il numero della vostra sottoscrizione viii
    5.3. Collegate il vostro sistema viii
6. Utilizzo del mouse viii
7. Copiare e incollare i testi con X ix
8. Prossimamente ix
    8.1. Inviateci i vostri suggerimenti! ix

I. Riferimento del sistema i

1. Processo di avvio, init e spegnimento 1
    1.1. Il processo di avvio 1
    1.2. Esame dettagliato del processo di avvio 1
    1.3. Esecuzione di programmi aggiuntivi durante l'avvio 6
    1.4. SysV Init Runlevels 6
    1.5. Arresto del sistema 8
2. Il boot loader GRUB 9
    2.1. Boot loader e architettura del sistema 9
    2.2. GRUB 9
    2.3. Installazione di GRUB 11
    2.4. Terminologia 11
    2.5. Interfacce di GRUB 13
    2.6. Comandi 14
    2.7. File di configurazione del menu di GRUB 16
    2.8. Modifica dei runlevel all'avvio 17
    2.9. Risorse aggiuntive 18
3. Struttura del filesystem 19
    3.1. Perché condividere una struttura comune? 19
    3.2. Panoramica sull'FHS (Filesystem Hierarchy Standard) 19
    3.3. Posizione dei file speciali sotto Red Hat Enterprise Linux 24
4. La directory `sysconfig` 27
    4.1. File contenuti in `/etc/sysconfig/` 27
    4.2. Directory presenti all'interno della directory `/etc/sysconfig/` 40
    4.3. Risorse Addizionali 40
5. Il filesystem `proc` 43
    5.1. Un filesystem virtuale 43
    5.2. File di livello superiore all'interno del filesystem `proc` 44
    5.3. Directory all'interno di `/proc` 60
    5.4. Usando il comando `sysctl` 79
    5.5. Risorse aggiuntive 79
6. Utenti e gruppi 81
    6.1. Tool per la creazione di utenti e gruppi 81
    6.2. Utenti standard 82
    6.3. Gruppi standard 83
    6.4. User Private Group 85
    6.5. Password Shadow 86
    6.6. Risorse aggiuntive 87

7. Il sistema X Window ... 89
7.1. La release X11R6.8 ... 89
7.2. Ambienti desktop e Window Manager ... 90
7.3. File di configurazione del server X ... 91
7.4. Font ... 97
7.5. Runlevel e X ... 100
7.6. Risorse aggiuntive ... 102
II. Riferimento dei servizi di rete ... 105
8. Interfacce di rete ... 107
8.1. File di configurazione per la rete ... 107
8.2. File di configurazione delle interfacce ... 108
8.3. Script di controllo delle interfacce ... 115
8.4. File di funzione di rete ... 116
8.5. Risorse addizionali ... 116
9. Network File System (NFS) ... 119
9.1. Come funziona ... 119
9.2. Come avviare e arrestare NFS ... 122
9.3. Configurazione del server NFS ... 123
9.4. File di configurazione del client NFS ... 126
9.5. Sicurezza e NFS ... 130
9.6. Risorse aggiuntive ... 131
10. Server HTTP Apache ... 133
10.1. Server HTTP Apache 2.0 ... 133
10.2. Migrazione dei file di configurazione del Server HTTP Apache 1.3 ... 134
10.3. Dopo l'installazione ... 145
10.4. Avvio e arresto di `httpd` ... 145
10.5. Direttive di configurazione in `httpd.conf` ... 147
10.6. Moduli predefiniti ... 163
10.7. Aggiunta di moduli ... 164
10.8. Host virtuali ... 164
10.9. Risorse aggiuntive ... 166
11. E-mail ... 169
11.1. Protocolli Email ... 169
11.2. Tipi di programmi e-mail ... 171
11.3. Mail Transport Agents ... 172
11.4. Mail Delivery Agents ... 181
11.5. Mail User Agents ... 188
11.6. Risorse aggiuntive ... 189
12. BIND (Berkeley Internet Name Domain) ... 193
12.1. Introduzione a DNS ... 193
12.2. `/etc/named.conf` ... 194
12.3. File zone ... 201
12.4. Uso di `rndc` ... 206
12.5. BIND: caratteristiche avanzate ... 208
12.6. Errori comuni da evitare ... 209
12.7. Risorse aggiuntive ... 210
13. LDAP (Lightweight Directory Access Protocol) ... 213
13.1. Perchè usare LDAP? ... 213
13.2. Terminologia di LDAP ... 214
13.3. Demoni e utility di OpenLDAP ... 214
13.4. File di configurazione di OpenLDAP ... 217
13.5. La directory `/etc/openldap/schema/` ... 217
13.6. Panoramica sulla configurazione di OpenLDAP ... 218
13.7. Configurazione di un sistema per l'autenticazione usando OpenLDAP ... 220
13.8. Migrazione delle directory dalle release precedenti ... 222

13.9. Risorse aggiuntive ... 222
14. Samba ... 225
14.1. Introduzione ... 225
14.2. Demoni di Samba e Servizi correlati ... 225
14.3. Tipi di server Samba e file `smb.conf` ... 227
14.4. Modalità di sicurezza di Samba ... 236
14.5. Database d'informazione sull'account di Samba ... 238
14.6. Browsing della rete di Samba ... 239
14.7. Samba con il supporto di stampa CUPS ... 241
14.8. Programmi di distribuzione di Samba ... 242
14.9. Risorse aggiuntive ... 248
15. FTP ... 251
15.1. Il File Transport Protocol ... 251
15.2. Sever FTP ... 252
15.3. File installati con `vsftpd` ... 253
15.4. Avvio e arresto di `vsftpd` ... 253
15.5. Opzioni di configurazione `vsftpd` ... 255
15.6. Risorse aggiuntive ... 263
III. Riferimento alla sicurezza ... 265
16. Moduli di autenticazione PAM ... 267
16.1. I vantaggi dei PAM ... 267
16.2. File di configurazione PAM ... 267
16.3. Formato del file di configurazione PAM ... 267
16.4. Esempi di file di configurazione PAM ... 270
16.5. Creazione dei moduli PAM ... 272
16.6. Conservazione delle credenziali di gestione e di PAM ... 272
16.7. PAM e proprietà dei dispositivi. ... 273
16.8. Risorse aggiuntive ... 275
17. Wrapper TCP e `xinetd` ... 277
17.1. Wrapper TCP ... 277
17.2. File di configurazione dei Wrapper TCP ... 278
17.3. `xinetd` ... 284
17.4. File di configurazione `xinetd` ... 285
17.5. Risorse aggiuntive ... 290
18. `iptables` ... 293
18.1. Filtraggio dei pacchetti ... 293
18.2. Differenze tra `iptables` e `ipchains` ... 295
18.3. Opzioni utilizzate all'interno dei comandi `iptables` ... 295
18.4. Come salvare le regole `iptables` ... 302
18.5. Script di controllo di `iptables` ... 303
18.6. `ip6tables` e IPv6 ... 305
18.7. Risorse aggiuntive ... 305
19. Kerberos ... 307
19.1. Che cos'è Kerberos? ... 307
19.2. Terminologia di Kerberos ... 308
19.3. Funzionamento di Kerberos ... 310
19.4. Kerberos e PAM ... 311
19.5. Configurazione di un server Kerberos 5 ... 311
19.6. Configurazione di un client Kerberos 5 ... 313
19.7. Risorse aggiuntive ... 314
20. Protocollo SSH ... 317
20.1. Caratteristiche di SSH ... 317
20.2. Versioni del Protocollo SSH ... 318
20.3. Sequenza degli eventi di una connessione SSH ... 318
20.4. File di configurazione OpenSSH ... 320

20.5. Shell più che sicura ... 321
20.6. Richiesta di SSH per le connessioni remote ... 323
20.7. Risorse aggiuntive ... 323
21. SELinux ... 325
21.1. Introduzione a SELinux ... 325
21.2. File relativi a SELinux ... 325
21.3. Risorse aggiuntive ... 328
IV. Appendici ... 331
A. Parametri generali e moduli ... 333
A.1. Come specificare i parametri del modulo ... 333
A.2. Parametri SCSI ... 334
A.3. Parametri Ethernet ... 334
Indice ... 339
Colophon ... 355

Introduzione

Benvenuti alla *Red Hat Enterprise Linux Reference Guide*.

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

Vi consigliamo di consultare questa guida se desiderate saperne un po' di più sul funzionamento del sistema Red Hat Enterprise Linux. Gli argomenti trattati sono i seguenti:

- Il processo di avvio
- La struttura del filesystem
- Il sistema X Window
- Servizi di rete
- Strumenti di sicurezza

1. Modifiche al manuale

Questo manuale è stato riorganizzato per chiarezza e ampliato con le nuove caratteristiche di Red Hat Enterprise Linux 4. Tra le modifiche si trovano:

Un nuovo capitolo su Samba

Il nuovo capitolo *Samba* affronta i diversi demoni Samba e le diverse opzioni di configurazione. Un ringraziamento particolare a **John Terpstra**, per il suo contributo al completamento di questo capitolo.

Un nuovo capitolo SELinux

Il nuovo capitolo *SELinux* affronta i diversi file di SELinux, insieme alle opzioni di configurazione. Un ringraziamento particolare a **Karsten Wade**, per il suo contributo al completamento di questo capitolo.

Un capitolo sul file system `proc` aggiornato

Il capitolo sul file system `proc` include informazioni aggiornate sul kernel 2.6. Un ringraziamento particolare a **Arjan van de Ven**, per il suo contributo al completamento di questo capitolo

Un capitolo aggiornato sul Network File System (NFS)

Il capitolo *Network File System (NFS)* è stato completamente modificato e riorganizzato in modo da includere NFSv4.

Un capitolo aggiornato Il sistema X Window

Il capitolo *Il sistema X Window* è stato modificato in modo da includere le informazioni sulla release X11R6.8, sviluppata dal team X.Org.

Prima di leggere questa guida, assicuratevi di conoscere i contenuti relativi alle problematiche per l'installazione presenti nella *Red Hat Enterprise Linux Installation Guide*, i concetti di base per la gestione contenuti nella *Red Hat Enterprise Linux Introduzione al System Administration*, le istruzioni relative alla personalizzazione che potete trovare nella *Red Hat Enterprise Linux System Administration Guide*, e le istruzioni relative alla sicurezza presenti nella *Red Hat Enterprise Linux Security Guide*. Questa guida contiene argomenti complessi idonei per utenti esperti.

Le versioni HTML, PDF, e RPM del manuale sono disponibili sul CD di documentazione di Red Hat Enterprise Linux e online su http://www.redhat.com/docs/.

Nota Bene

Anche se questo manuale riporta le informazioni più aggiornate, vi consigliamo di leggere le *Release Note di Red Hat Enterprise Linux*, per informazioni che potrebbero non essere state incluse prima della finalizzazione di questa documentazione. Tali informazioni possono essere trovate sul CD #1 di Red Hat Enterprise Linux e online su http://www.redhat.com/docs/.

2. Informazioni specifiche sull'architettura

Se non diversamente riportato, tutte le informazioni contenute in questo manuale valgono solo per i processori x86 e per i processori che contengono le tecnologie Intel® Extended Memory 64 Technology (Intel® EM64T) e AMD64. Per informazioni specifiche all'architettura, fate riferimento a *Red Hat Enterprise Linux Installation Guide*.

3. Ricerca della documentazione idonea

È consigliabile consultare la documentazione più adatta al vostro livello di conoscenza, in caso contrario rischiate di non trovare le informazioni che cercate. La *Red Hat Enterprise Linux Reference Guide* tratta gli aspetti e le opzioni più tecniche del sistema Red Hat Enterprise Linux. Questa sezione vi aiuterà a stabilire se questo manuale contiene le informazioni di cui avete bisogno oppure se consultare altri manuali Red Hat Enterprise Linux o risorse online.

Gli utenti di Red Hat Enterprise Linux possono essere suddivisi in tre gruppi, in base al livello di esperienza. Per ogni categoria di appartenenza è indicato il tipo di documentazione da consultare. Per sapere da dove inziare, determinate il vostro livello di esperienza:

Nuovi utenti di Linux

Questi utenti non hanno mai utilizzato un sistema operativo Linux o simile oppure lo conoscono appena, ma potrebbero saper usare altri sistemi operativi (per esempio Windows). Se è il vostro caso consultate la Sezione 3.1.

Utenti con qualche nozione di Linux

Questi utenti hanno già installato e utilizzato Linux in precedenza (ma non Red Hat Enterprise Linux) oppure hanno un po' di esperienza con altri sistemi operativi simili a Linux. Vi riconoscete in questo tipo di utente? Allora consultate la Sezione 3.2.

Utenti esperti di Linux

Questi utenti hanno installato e usato Red Hat Enterprise Linux in precedenza. Se appartenete a questa categoria, consultate la Sezione 3.3.

3.1. Documentazione per gli utenti inesperti

Per chi non conosce Linux, la quantità di informazioni disponibili su qualsiasi argomento, come la stampa, l'avvio del sistema o il partizionamento del disco fisso, può sembrare enorme. All'inizio è op-

portuno raccogliere una base minima di informazioni sul funzionamento di Linux, prima di affrontare argomenti più complessi.

Innanzitutto dovete reperire della documentazione utile. Infatti, senza la documentazione adatta non sarete in grado di far funzionare il vostro sistema Red Hat Enterprise Linux nel modo desiderato e ciò può divenire fonte di frustrazione.

Vi suggeriamo di cercare le seguenti documentazioni:

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

  Ricordatevi che non occorre imparare a memoria tutti i comandi disponibili con Linux. Esistono diversi modi per facilitare la ricerca del comando specifico di cui avete bisogno per l'esecuzione di un compito. È importante conoscere solo il modo generale in cui Linux funziona, cioè il compito che dovete eseguire e come accedere allo strumento che vi fornisce le istruzioni necessarie per eseguire il comando.

La *Red Hat Enterprise Linux Installation Guide* e *Red Hat Enterprise Linux Guida passo dopo passo*, costituiscono un valido riferimento per installare e configurare correttamente un sistema Red Hat Enterprise Linux. La *Red Hat Enterprise Linux Introduzione al System Administration* è l'ideale per coloro che stanno imparando i concetti di base per la gestione del sistema. Iniziate con questi due libri e utilizzateli come base su cui costituire le vostre conoscenze di Red Hat Enterprise Linux. Vi accorgerete che molti concetti più complessi avranno per voi un senso, poiché avrete già interiorizzato le informazioni di base.

Oltre a leggere i manuali di Red Hat Enterprise Linux esistono molte altre fonti eccellenti dove trovare informazioni gratuite o poco costose:

3.1.1. Introduzione ai siti Web di Linux

- http://www.redhat.com/ —Sul sito di Red Hat, sono disponibili alcuni link per il Linux Documentation Project (LDP), le versioni online dei manuali Red Hat Enterprise Linux, le FAQ (Frequently Asked Questions), un database per aiutarvi nella ricerca del gruppo di utenti Linux più vicino a voi, informazioni tecniche nel Support Knowledge Base di Red Hat e altro ancora.
- http://www.linuxheadquarters.com/ — Il sito Web del quartier generale di Linux, visualizza alcune guide che illustrano passo dopo passo i numerosi compiti di Linux.

3.1.2. Introduzione ai newsgroup di Linux

Potete entrare a far parte di un newsgroup leggendo gli interventi di altri, tentando di risolvere i problemi e ponendo domande. Gli esperti di Linux sono sempre disposti ad aiutare i nuovi utenti su varie problematiche — specialmente se si formulano le domande nella giusta sede. Se non potete accedere a un'applicazione che permette di leggere le news, visitate il sito http://groups.google.com/. Esistono comunque decine di newsgroup correlati a Linux, tra cui:

- linux.help — un ottimo riferimento in cui ricevere aiuto da altri utenti di Linux.
- linux.redhat — Questa newsgroup si occupa principalmente di problematiche legate a Red Hat Enterprise Linux.
- linux.redhat.install — in questo newsgroup potete porre quesiti relativi all'installazione oppure trovare soluzioni già sperimentate da altri in relazione a problemi simili ai vostri.
- linux.redhat.misc — per chi ha domande o richieste che non rientrano nelle categorie tradizionali.
- linux.redhat.rpm — Per chi ha problemi con l'uso di RPM per raggiungere obiettivi particolari.

3.2. Documentazione per i più esperti

Se avete già utilizzato altri prodotti Linux, probabilmente avete una conoscenza di base dei comandi più utilizzati. Potreste aver installato il vostro sistema Linux e magari aver scaricato e installato software ottenuto tramite Internet. Tuttavia, dopo l'installazione, potreste avere delle difficoltà con la configurazione.

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

Quando installate un software che non è trattato nella *Red Hat Enterprise Linux System Administration Guide*, è sempre consigliabile controllare cosa hanno fatto gli utenti che vi hanno preceduto in circostanze simili. I documenti HOWTO della Linux Documentation Project, disponibili all'indirizzo http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html, contengono aspetti particolari di Linux, a partire da un kernel di basso livello fino all'uso di Linux per stazioni radio amatoriali.

Se siete interessati ad affrontare argomenti più specifici riguardanti il sistema di Red Hat Enterprise Linux, allora *Red Hat Enterprise Linux Reference Guide* risulta essere la soluzione migliore.

Se siete preoccupati delle problematiche riguardanti la sicurezza, *Red Hat Enterprise Linux Security Guide* rappresenta una fonte molto importante — che affronta in termini concisi, le strategie e le pratiche migliori per rendere sicuro Red Hat Enterprise Linux.

3.3. Documentazione per i guru di Linux

Se siete interessati ad affrontare argomenti più specifici riguardanti il sistema di Red Hat Enterprise Linux, allora *Red Hat Enterprise Linux Reference Guide* risulta essere la soluzione migliore.

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

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

4. Convenzioni del documento

Consultando il presente manuale, vedrete alcune parole stampate con caratteri, dimensioni e stili differenti. Si tratta di un metodo sistematico per mettere in evidenza determinate parole; lo stesso stile

grafico indica l'appartenenza a una specifica categoria. Le parole rappresentate in questo modo includono:

`comando`

I comandi di Linux (e altri comandi di sistemi operativi, quando usati) vengono rappresentati in questo modo. Questo stile indica che potete digitare la parola o la frase nella linea di comando e premere [Invio] per invocare il comando. A volte un comando contiene parole che vengono rappresentate con uno stile diverso (come i file name). In questi casi, tali parole vengono considerate come parte integrante del comando e, dunque, l'intera frase viene visualizzata come un comando. Per esempio:

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

`file name`

I file name, i nomi delle directory, i percorsi e i nomi del pacchetto RPM vengono rappresentati con questo stile grafico. Ciò significa che un file o una directory particolari, sono rappresentati sul vostro sistema da questo nome.Per esempio:

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

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

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

applicazione

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

Utilizzate **Mozilla** per navigare sul Web.

[tasto]

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

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

[tasto]-[combinazione]

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

La combinazione dei tasti [Ctrl]-[Alt]-[Backspace] esce dalla vostra sessione grafica e vi riporta alla schermata grafica di login o nella console.

testo presente in un'interfaccia grafica

Un titolo, una parola o una frase trovata su di una schermata dell'interfaccia GUI o una finestra, verrà mostrata con questo stile: Il testo mostrato in questo stile, viene usato per identificare una particolare schermata GUI o un elemento della schermata GUI, (per esempio il testo associato a una casella o a un campo). Esempio:

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

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

Quando vedete una parola scritta con questo stile grafico, si tratta di una parola posta per prima in un menu a tendina. Facendo clic sulla parola nella schermata GUI, dovrebbe comparire il resto del menu. Per esempio:

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

Se dovete digitare una sequenza di comandi da un menu GUI, essi verranno visualizzati con uno stile simile al seguente esempio:

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

pulsante di una schermata o una finestra dell'interfaccia grafica

Questo stile indica che il testo si trova su di un pulsante in una schermata GUI. Per esempio:

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

`output del computer`

Il testo in questo stile, indica il testo visualizzato ad un prompt della shell come ad esempio, messaggi di errore e risposte ai comandi. Per esempio:

Il comando `ls` visualizza i contenuti di una directory. Per esempio:

```
Desktop                about.html       logs          paulwesterberg.png
Mail                   backupfiles      mail          reports
```

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

`prompt`

Un prompt, ovvero uno dei modi utilizzati dal computer per indicare che è pronto per ricevere un vostro input. Ecco qualche esempio:

```
$
```

```
#
```

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

```
leopard login:
```

`input dell'utente`

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

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

`replaceable`

Il testo usato per gli esempi, il quale deve essere sostituito con i dati forniti dal"utente,è visualizzato con questo stile. Nel seguente esempio, il *<numero della versione>* viene mostrato in questo stile:

La directory per la fonte del kernel è `/usr/src/`*`<version-number>`*`/`, dove *<version-number>* è la versione del kernel installato su questo sistema.

Inoltre, noi adottiamo diverse strategie per attirare la vostra attenzione su alcune informazioni particolari. In base all'importanza che tali informazioni hanno per il vostro sistema, questi elementi verranno definiti nota bene, suggerimento, importante, attenzione o avvertenza. Per esempio:

Nota Bene

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

Suggerimento

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

Importante

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

Attenzione

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

Avvertenza

Fate attenzione a rimuovere solo le partizioni necessarie per Red Hat Enterprise Linux. Rimuovere altre partizioni può comportare una perdita dei dati oppure una corruzione dell'ambiente del sistema.

5. Attivate la vostra sottoscrizione

Prima di poter accedere alle informazioni sulla gestione del software e sul servizio, e prima di poter consultare la documentazione di supporto inclusa con la vostra registrazione, è necessario attivare la vostra sottoscrizione registrandovi con Red Hat. Il processo di registrazione include le seguenti fasi:

- Fornire un login di Red Hat
- Fornire il numero della vostra sottoscrizione
- Collegare il vostro sistema

La prima volta che eseguirete un avvio dell'installazione di Red Hat Enterprise Linux, vi verrà richiesto di registrarvi con Red Hat usando l'**Agent Setup**. Seguendo le diverse prompt dell'**Agent Setup**, sarete in grado di completare le fasi necessarie alla registrazione, attivando così la vostra sottoscrizione.

Se non siete in grado di completare la registrazione durante l'**Agent Setup** (il quale necessita di un accesso di rete), allora provate il processo di registrazione online di Red Hat disponibile su http://www.redhat.com/register/.

5.1. Fornite un login di Red Hat

Se non siete in possesso di un login di Red Hat, allora sarete in grado di crearne uno quando vi verrà richiesto durante l'**Agent Setup**, oppure online su:

```
https://www.redhat.com/apps/activate/newlogin.html
```

Un login di Red Hat vi permette di accedere a:

- Aggiornamenti software, errata e gestione tramite Red Hat Network
- Risorse per il supporto tecnico di Red Hat, documentazione, e Knowledgebase

Se avete dimenticato il vostro login di Red Hat, potete trovarlo online su:

```
https://rhn.redhat.com/help/forgot_password.pxt
```

5.2. Fornite il numero della vostra sottoscrizione

Il numero della vostra sottoscrizione si trova all'interno del pacchetto da voi ordinato. Se tale pacchetto non include il suddetto numero, allora la vostra sottoscrizione è già stata attivata, per questo motivo potete saltare questa fase.

Potete fornire il numero della vostra sottoscrizione quando richiesto durante l'**Agent Setup**, oppure visitando http://www.redhat.com/register/.

5.3. Collegate il vostro sistema

Il Red Hat Network Registration Client sarà utile per il collegamento del vostro sistema in modo tale da permettervi di ottenere gli aggiornamenti, e la gestione dei diversi sistemi. Sono diponibili tre diversi modi per eseguire tale collegamento:

1. Durante l'**Agent Setup** — Controllare le opzioni **Invia informazioni hardware** e **Invia un elenco del pacchetto del sistema** quando richiesto.
2. Dopo il completamento dell'**Agent Setup** — Dal **Menu Principale**, andate su **Tool di sistema**, per poi selezionare **Red Hat Network**.
3. Dopo il completamento dell'**Agent Setup** — Inserire il seguente comando dalla linea di comando come utente root:
   - `/usr/bin/up2date --register`

6. Utilizzo del mouse

Per Red Hat Enterprise Linux è previsto l'utilizzo di un mouse a tre tasti. Se avete un mouse a due tasti, dovreste selezionare l'emulazione del terzo tasto durante il processo di installazione. Se avete attivato questa funzione, premendo contemporaneamente i due tasti del mouse ottenete lo stesso effetto dato dalla pressione del terzo tasto (quello centrale).

In questo documento, se vi viene richiesto di fare clic con il mouse su qualche elemento, significa che dovete utilizzare il tasto sinistro. Quando occorre usare il tasto destro o quello centrale, vi viene esplicitamente indicato (qualora il mouse sia stato configurato per un utente mancino le impostazioni sono, naturalmente, invertite).

La locuzione "drag-and-drop" può risultarvi familiare. Se vi viene indicato di trascinare e lasciare un oggetto all'interno del desktop GUI, dovete fare clic su qualcosa e, tenendo premuto il tasto del mouse, trascinare l'oggetto spostando il mouse in una nuova posizione. Una volta raggiunto il punto desiderato, per depositare l'oggetto dovete semplicemente rilasciare il tasto del mouse.

7. Copiare e incollare i testi con X

Copiare e incollare parti di testo è semplice se utilizzate il mouse e il sistema X Window. Per copiare un testo, evidenziatelo facendo clic e trascinatelo col mouse fin dove necessario. Per incollare la selezione in un altro punto, fate clic con il tasto centrale del mouse nel punto desiderato.

8. Prossimamente

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

Ovviamente potete contribuire anche voi!

8.1. Inviateci i vostri suggerimenti!

Se individuate un errore nella *Red Hat Enterprise Linux Reference Guide* o se avete qualche idea per migliorare il manuale, inviateci suggerimenti! Inviate un report in Bugzilla (http://bugzilla.redhat.com/bugzilla/) in merito al componente *rhel-rg*.

Assicuratevi di menzionare l'identificatore del manuale:

```
rhel-rg(IT)-4-Print-RHI (2004-09-25T17:13)
```

Se menzionate l'identificatore del manuale, sapremo esattamente a quale versione vi riferite.

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

I. Riferimento del sistema

Per gestire il sistema nel modo migliore, è importante conoscere i suoi componenti e la loro affinità. Questa sezione evidenzia molti aspetti importanti del sistema. Affronta il processo d'avvio, la struttura di base del file system, la posizione di file e file system importanti del sistema, e i concetti di base dietro gli utenti e i gruppi. In aggiunta, il sistema X Window viene affrontato in dettaglio.

Sommario

1. Processo di avvio, init e spegnimento 1
2. Il boot loader GRUB 9
3. Struttura del filesystem 19
4. La directory `sysconfig` 27
5. Il filesystem `proc` 43
6. Utenti e gruppi 81
7. Il sistema X Window 89

Capitolo 1.

Processo di avvio, init e spegnimento

Uno degli aspetti più importanti di Red Hat Enterprise Linux è il metodo utilizzato per avviare e arrestare il sistema operativo. Gli utenti sono liberi di configurare diversi aspetti del processo di avvio incluso la specificazione dei programmi lanciati al momento dell'avvio. In modo simile, l'arresto del sistema interrompe i processi in modo organizzato e configurabile, anche se la personalizzazione di questo processo è raramente necessaria.

La comprensione del funzionamento dei processi di avvio e di arresto non solo vi consente di effettuare una personalizzazione, ma vi aiuta a trovare una soluzione ai problemi legati all'avvio o allo spegnimento del sistema.

1.1. Il processo di avvio

Di seguito sono riportate le fasi principali del processo di avvio per un sistema x86:

1. Il sistema BIOS (Basic Input/Output System) controlla il sistema e avvia il boot loader della prima fase nel file MBR del disco fisso primario.
2. Il boot loader della prima fase viene caricato in memoria e consente di avviare il boot loader della seconda fase dalla partizione `/boot/`.
3. Il boot loader della seconda fase carica il kernel in memoria, che a suo turno carica tutti i moduli e monta la partizione root di sola lettura.
4. Il kernel trasferisce il controllo del processo di avvio al programma `/sbin/init`.
5. Il programma `/sbin/init` carica tutti i servizi e gli strumenti user-space e monta tutte le partizioni elencate in `/etc/fstab`.
6. All'utente viene presentato una schermata di login per il sistema di Linux appena installato.

Poichè la configurazione del processo di avvio è più comune della personalizzazione del processo di arresto, la parte restante di questo capitolo presenterà in modo dettagliato il funzionamento del processo di avvio e come può essere personalizzato in base alle vostre esigenze.

1.2. Esame dettagliato del processo di avvio

L'inizio del processo di avvio varia in base alla piattaforma utilizzata. Tuttavia, quando il kernel viene rilevato e caricato dal boot loader, il processo di avvio di default è identico per tutte le architetture. Questo capitolo si dedica principalmente all'architettura x86.

1.2.1. Il BIOS

Quando un computer x86 viene avviato, il processore controlla il *BIOS* o *Basic Input/Output System* alla fine della memoria del sistema, eseguendolo in un secodno momento. Il BIOS controlla non solo la prima fase del processo di avvio, ma fornisce l'interfaccia di livello inferiore alle periferiche. Per questo motivo è scritto in una memoria permanente in sola lettura e può sempre essere utilizzato.

Altre piattaforme utilizzano programmi diversi per eseguire attività di livello inferiore, in minima parte equivalenti a quelle del BIOS di un sistema x86. Per esempio i computer con processore Itanium utilizzano la *shell Extensible Firmware Interface* (*EFI*).

Dopo il caricamento, il BIOS esamina il sistema, cerca e controlla le periferiche e cerca un dispositivo valido per avviare il sistema. Di solito controlla le unità floppy ed i CD-ROM presenti alla ricerca di supporti avviabili, se non riesce ad eseguire tale operazione, verifica il disco fisso. Nella maggior parte dei casi, la sequenza delle unità utilizzate per l'avvio, è controllata da una particolare configurazione del BIOS, eseguendo una ricerca sul dispositivo master IDE sul bus IDE primario. Il BIOS carica in memoria qualsiasi programma presente nel primo settore di questo dispositivo, denominato *MBR* o *Master Boot Record*. L'MBR ha dimensioni pari a soli 512 byte e contiene le istruzioni in codice macchina per l'avvio del computer oltre alla tabella delle partizioni. Al termine dell'operazione il BIOS passa il controllo a qualsiasi programma che si trova nell'MBR.

1.2.2. Il boot loader

Questa sezione si dedica in particolare al boot loader di default per la piattaforma x86, GRUB. A seconda dell'architettura del sistema, il processo di avvio può differire leggermente. Per ulteriori informazioni sui boot loader diversi da x86, consultate la Sezione 1.2.2.1. Per maggiori informazioni sulla configurazione e sull'uso di GRUB, controllare il Capitolo 2.

Un boot loader per la piattaforma x86 è caratterizzato da almeno due fasi. La prima delle quali è rappresentata da una piccola porzione del codice binario della macchina dell'MBR. L'unico obiettivo di questa fase è quello di rilevare il boot loader secondario e caricare la prima parte in memoria.

GRUB ha il vantaggio di poter leggere ext2 e ext3 [1] e carica il file di configurazione — `/boot/grub/grub.conf`— al momento dell'avvio. Per ulteriori informazioni su come modificare questo file, consultate la Sezione 2.7.

Suggerimento

Se aggiornate il kernel mediante **Red Hat Update Agent**, il file di configurazione per il boot loader verrà aggiornato automaticamente. Per ulteriori infomazioni su Red Hat Network fate riferimento all'URL riportato di seguito: https://rhn.redhat.com/.

Quando il boot loader secondario è in memoria, viene visualizzata la schermata grafica che mostra i diversi sistemi operativi o i kernel che sono stati configurati per l'avvio. Su questa schermata un utente può usare i tasti direzionali per scegliere quale sistema operativo o kernel vuole avviare e premere [Invio]. Se nessun tasto è premuto, il boot loader carica la selezione di default dopo un determinato periodo di tempo.

Nota Bene

Se avete installato il supporto per il kernel (SMP) Symmetric Multi-Processor, numerose opzioni saranno disponibili al primo avvio del sistema. In questa situazione GRUB visualizza `Red Hat Enterprise Linux (<versione-kernel>-smp)`, il kernel di SMP, e `Red Hat Enterprise Linux (<versione-kernel>)`, per singoli processori.

Se si verificassero dei problemi con il kernel SMP, provate a selezionare il kernel non-SMP dopo il riavvio.

1. GRUB legge i filesystem ext3 come ext2, non facendo caso al file journal. Per ulteriori informazioni sul file system ext3, consultate il capitolo intitolato *Il File System ext3* nella *Red Hat Enterprise Linux System Administration Guide*.

Quando il boot loader della seconda fase ha determinato quale kernel avviare, esso rileva il kernel binario corrispondente nella directory `/boot/`. Il kernel binario viene chiamato usando il formato seguente — `/boot/vmlinuz-<versione-kernel>` (dove `<versione-kernel>` corrisponde alla versione del kernel specificata nelle impostazioni del boot loader).

Per instruzioni su come usare il boot loader per fornire argomenti della linea di comando al kernel, consultate il Capitolo 2. Per maggiori informazioni su come modificare il runlevel al prompt del boot loader, consultate la Sezione 2.8.

Il boot loader colloca quindi in memoria una o più immagini *initramfs*. Successivamente il kernel decomprime etrasferisce queste immagini dalla memoria a `/boot/`, un file system virtuale basato sulla RAM tramite il comando `cpio`. *initramfs* viene usato dal kernel per caricare tutti i driver ed i moduli necessari per avviare il sistema. Questa operazione è particolarmente importante se disponete di unità SCSI o se i sistemi utilizzano il file system ext3.

Dopo avere caricato in memoria il kernel e l'immagine `initramfs`,il boot loader trasferisce il controllo del processo di avvio al kernel.

Per una panoramica più dettagliata sul boot loader GRUB, consultate Capitolo 2.

1.2.2.1. I boot loader ed altre architetture

Dopo il caricamento e il trasferimento del processo di avvio al comando `init`, la stessa sequenza di eventi si verifica in ogni architettura. La differenza principale tra ogni processo di avvio, consiste nell'applicazione utilizzata per trovare e caricare il kernel.

Per esempio, l'architettura Itanium utilizza il boot loader ELILO, l'architettura eServer pSeries di IBM usa YABOOT, i sistemi s390 e eServer zSeries di IBM usano il boot loader z/IPL.

Consultate *Red Hat Enterprise Linux Installation Guide* specifica per queste piattaforme e per informazioni su come configurare i relativi boot loader.

1.2.3. Il kernel

Una volta caricato, il kernel inizializza e configura immediatamente la memoria del computer e configura quindi i vari elementi hardware collegati al sistema, incluso tutti i processori e i sottosistemi I/O, oltre a tutti i dispositivi di memorizzazione. Cerca quindi l'immagine `initramfs` compressa in una posizione predeterminata della memoria, la decomprime direttamente su `/sysroot/`, e carica tutti i driver necessari. Successivamente inizializza i dispositivi virtuali relativi al file system, come LVM o il software RAID prima di completare i processi `initramfs` e liberare tutta la memoria occupata.

Dopo l'inizializzazione di tutti i dispositivi del sistema da parte del kernel, viene creato un dispositivo root, montata la partizione root di sola lettura e liberata la memoria non utilizzata.

Il kernel risulta così caricato in memoria e operativo. Tuttavia, senza alcuna applicazione che consenta all'utente di fornire un input significativo al sistema, il kernel non è molto utile.

Per configurare l'ambiente utente, il kernel esegue il programma `/sbin/init`.

1.2.4. Il programma `/sbin/init`

Il programma `/sbin/init` (chiamato anche `init`) coordina la fase restante del processo di avvio e configura l'ambiente per l'utente.

Quando il comando `init` viene eseguito, diventa il genitore di tutti i processi che si avviano automaticamente sul sistema. Innanzitutto esegue lo script `/etc/rc.d/rc.sysinit` che imposta il percorso dell'ambiente, attiva lo swap, controlla i filesystem e si occupa di tutti i processi che vanno eseguiti per l'inizializzazione del sistema. Per esempio, la maggior parte dei sistemi utilizza un orologio, così `rc.sysinit` legge il file di configurazione `/etc/sysconfig/clock` per inizializzare l'orologio

dell'hardware. Un altro esempio potrebbe essere quello con il quale è necessario inizializzare processi speciali per le porte seriali, `rc.sysinit` può eseguire anche il file `/etc/rc.serial`.

Il comando `init` esegue lo script `/etc/inittab`, il quale descrive il modo attraverso il quale il sistema dovrebbe esssere impostato in ogni *SysV init runlevel*.I runlevel sono degli stati, o *modalità*, definiti dai servizi elencati nella directory di SysV `/etc/rc.d/rc`<*x*>`.d/`, dove <*x*> è il numero del runlevel. Per maggiori informazioni sui runlevel SysV init, consultate la Sezione 1.4.

Successivamente il comando `init` imposta la libreria di funzione della fonte, `/etc/rc.d/init.d/functions`, per il sistema il quale a sua volta configura il modo di avvio o come eliminare e determinare il PID di un programma.

A questo punto il programma `init` avvia tutti i processi di background cercando nella relativa directory `rc` il runlevel specificato come predefinito in `/etc/inittab`. Le directory `rc` sono numerate in modo da corrispondere ai runlevel che rappresentano. Per esempio `/etc/rc.d/rc5.d/` è la directory per il runlevel 5.

Quando si esegue l'avvio dal runlevel 5, il programma `init` cerca nella directory `/etc/rc.d/rc5.d/` per determinare quali processi iniziare e arrestare.

Di seguito è riportato un esempio che illustra un runlevel 5, la directory `/etc/rc.d/rc5.d/`:

```
K05innd -> ../init.d/innd
K05saslauthd -> ../init.d/saslauthd
K10dc_server -> ../init.d/dc_server
K10psacct -> ../init.d/psacct
K10radiusd -> ../init.d/radiusd
K12dc_client -> ../init.d/dc_client
K12FreeWnn -> ../init.d/FreeWnn
K12mailman -> ../init.d/mailman
K12mysqld -> ../init.d/mysqld
K15httpd -> ../init.d/httpd
K20netdump-server -> ../init.d/netdump-server
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwhod -> ../init.d/rwhod
K24irda -> ../init.d/irda
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
K30spamassassin -> ../init.d/spamassassin
K34dhcrelay -> ../init.d/dhcrelay
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K36lisa -> ../init.d/lisa
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K46radvd -> ../init.d/radvd
K50netdump -> ../init.d/netdump
K50snmpd -> ../init.d/snmpd
K50snmptrapd -> ../init.d/snmptrapd
K50tux -> ../init.d/tux
K50vsftpd -> ../init.d/vsftpd
K54dovecot -> ../init.d/dovecot
K61ldap -> ../init.d/ldap
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
```

```
K70aep1000 -> ../init.d/aep1000
K70bcm5820 -> ../init.d/bcm5820
K74ypserv -> ../init.d/ypserv
K74ypxfrd -> ../init.d/ypxfrd
K85mdmpd -> ../init.d/mdmpd
K89netplugd -> ../init.d/netplugd
K99microcode_ctl -> ../init.d/microcode_ctl
S04readahead_early -> ../init.d/readahead_early
S05kudzu -> ../init.d/kudzu
S06cpuspeed -> ../init.d/cpuspeed
S08ip6tables -> ../init.d/ip6tables
S08iptables -> ../init.d/iptables
S09isdn -> ../init.d/isdn
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13irqbalance -> ../init.d/irqbalance
S13portmap -> ../init.d/portmap
S15mdmonitor -> ../init.d/mdmonitor
S15zebra -> ../init.d/zebra
S16bgpd -> ../init.d/bgpd
S16ospf6d -> ../init.d/ospf6d
S16ospfd -> ../init.d/ospfd
S16ripd -> ../init.d/ripd
S16ripngd -> ../init.d/ripngd
S20random -> ../init.d/random
S24pcmcia -> ../init.d/pcmcia
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
S27ypbind -> ../init.d/ypbind
S28autofs -> ../init.d/autofs
S40smartd -> ../init.d/smartd
S44acpid -> ../init.d/acpid
S54hpoj -> ../init.d/hpoj
S55cups -> ../init.d/cups
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S58ntpd -> ../init.d/ntpd
S75postgresql -> ../init.d/postgresql
S80sendmail -> ../init.d/sendmail
S85gpm -> ../init.d/gpm
S87iiim -> ../init.d/iiim
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
S90xfs -> ../init.d/xfs
S95atd -> ../init.d/atd
S96readahead -> ../init.d/readahead
S97messagebus -> ../init.d/messagebus
S97rhnsd -> ../init.d/rhnsd
S99local -> ../rc.local
```

Nessuno degli script che avvia e arresta realmente i servizi si trova nella directory `/etc/rc.d/rc5.d/`. Tutti i file in `/etc/rc.d/rc5.d/` sono *link simbolici* diretti a script che si trovano nella directory `/etc/rc.d/init.d/`. I link simbolici sono utilizzati in ciascuna delle directory `rc` per fare in modo che i runlevel possano essere riconfigurati creando, modificando ed eliminando i link simbolici senza influire sugli script a cui fanno riferimento.

Il nome di ciascun link simbolico inizia con `K` o `S`. I link `K` sono processi che vengono terminati, mentre quelli che iniziano con `S` vengono avviati.

Il comando `init` arresta innanzitutto i link simbolici `K` della directory eseguendo il comando `/etc/rc.d/init.d/<comando> stop`, in cui *<comando>* è il processo da terminare. Avvia quindi tutti i link simbolici `S` eseguendo il comando `/etc/rc.d/init.d/<comando> start`.

Suggerimento

Al termine dell'avvio del sistema, è possibile accedere come root ed eseguire gli stessi script per avviare e interrompere i servizi. Per esempio il comando `/etc/rc.d/init.d/httpd stop` interrompe Server HTTP Apache.

Ciascuno dei link simbolici è numerato in modo da stabilire l'ordine di avvio. Potete modificare l'ordine in cui i servizi vengono avviati o interrotti cambiando questo numero. Più il numero è basso, prima il servizio corrispondente viene avviato. I link simbolici che presentano lo stesso numero, vengono avviati in base ad un ordine alfabetico.

Nota Bene

Una delle ultime cose che il programma `init` esegue, è il file `/etc/rc.d/rc.local`. Questo file è utile per la personalizzazione del sistema. Per ulteriori informazioni sulla personalizzazione del sistema usando il file `rc.local` consultate la Sezione 1.3.

Dopo che il comando `init` è andato avanti attraverso la directory appropriata `rc` per la ricerca del runlevel, lo script `/etc/inittab` crea un processo `/sbin/mingetty` per ciascuna console virtuale (prompt di login) di ogni runlevel. I runlevel da 2 a 5 hanno le sei console virtuali, mentre il runlevel 1, (in modalità utente singolo), dispone di una sola console virtuale, e i runlevel 0 e 6 non ne hanno alcuna. Il processo `/sbin/mingetty` apre delle linee di comunicazione per i dispositivi *tty* [2], ne imposta la modalità, visualizza il prompt di login, riceve il nome dell'utente e inizializza il processo di login per quell'utente.

Nel runlevel 5 `/etc/inittab` esegue uno script chiamato `/etc/X11/prefdm`. Lo script `prefdm` esegue il display manager X preferito[3] — `gdm`, `kdm`,o `xdm`, in base al contenuto del file `/etc/sysconfig/desktop/`.

Una volta terminato, il sistema è operativo sul runlevel 5, mostrando anche una schermata di login.

1.3. Esecuzione di programmi aggiuntivi durante l'avvio

Lo script `/etc/rc.d/rc.local` viene eseguito dal comando `init` al momento dell'avvio oppure ogni qualvolta si modifica il runlevel. Aggiungendo dei comandi nella parte inferiore dello script risulta essere più semplice eseguire le operazioni necessarie come l'avvio dei servizi speciali oppure l'inizializzazione dei dispositivi senza scrivere degli script complessi all'interno della directory `/etc/rc.d/init.d/`, creando quindi dei link simbolici.

Lo script `/etc/rc.serial` viene usato se le porte seriali devono essere impostate al momento dell'avvio. Questo script esegue i comandi `setserial` per configurare le porte seriali del sistema. Per ulteriori informazioni, consultate la pagina man `setserial`.

2. Per maggiori informazioni sui dispositivi `tty`, consultate la Sezione 5.3.11.
3. Consultare la Sezione 7.5.2 per maggiori informazioni sui display manager.

1.4. SysV Init Runlevels

Il sistema di runlevel SysV init fornisce un processo standard per controllare quale software viene avviato o interrotto dal comando `init` per un runlevel particolare. SysV è stato scelto perché è più semplice da utilizzare e più flessibile del processo tradizionale a stile BSD.

I file di configurazione di SysV init si trovano in `/etc/rc.d`. In questa directory troverete gli script `rc`, `rc.local`, `rc.sysinit` , e facoltativamente gli script `rc.serial` e le seguenti directory:

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

La directory `init.d` contiene gli script utilizzati dal comando `/sbin/init` per il controllo dei servizi. Ciascuna delle directory numerate rappresenta i sei runlevel di default configurati per default in Red Hat Enterprise Linux.

1.4.1. Runlevel

Il concetto dietro i runlevel SysV init si basa sul fatto che è possibile utilizzare sistemi diversi in modi differenti. Per esempio, un server opera in modo più efficiente sulle risorse del computer creato dal sistema X Window, se esso non presenta alcun sovraccarico. Altre volte, un amministratore di sistema potrebbe avere il bisogno di operare in un runlevel minore per effettuare delle operazioni di diagnosi, come risolvere delle corruzioni sul disco in runlevel 1.

Le caratteristiche di ogni runlevel determinano quale servizio è interrotto e quale viene avviato dal comando `init`. Per esempio, runlevel 1 (modalità utente singolo) interrompe qualunque servizio di rete, mentre il runlevel 3 avvia questi servizi. Assegnando specifici servizi per l'interruzione o l'avvio di un particolare runlevel, `init` è in grado di modificare la modalità del computer senza che l'utente debba interrompere o avviare i servizi manualmente.

I seguenti runlevel sono definiti per default in Red Hat Enterprise Linux:

- `0` — arresto
- `1` — modalità a utente singolo
- `2` — non utilizzato (definito dall'utente)
- `3` — modalità multiutente completa
- `4` — non utilizzato (definito dall'utente)
- `5` — modalità multiutente completa (con schermata di login basata su X)
- `6` — riavvio

In generale, gli utenti utilizzano Red Hat Enterprise Linux ad un runlevel 3 o runlevel 5 — entrambe con modalità multiutente. Gli utenti talvolta, personalizzano i runlevel 2 e 4 per soddisfare delle esigenze specifiche.

Il runlevel predefinito per il sistema è scritto nel file `/etc/inittab`. Per scoprire il runlevel di default per un sistema, cercate la riga simile a quella riportata all'inizio del file `/etc/inittab`:

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

Il runlevel predefinito nell'esempio di cui sopra, è cinque, come indicato dal numero dopo i primi due punti. Per cambiarlo, modifcate `/etc/inittab` come root.

Avvertenza

State attenti quando modificate il file `/etc/inittab`. Errori semplici possono causare l'impossibilità di riavvio del sistema. Se si verifica quanto detto, usate un dischetto di avvio, immettete la modalità utente singolo, o la madalità rescue e riparate il file.

Per ulteriori informazioni sulla modalità utente-singolo e sulla modalità rescue, consultate il capitolo intitolato *Ripristino di base del sistema* nella *Red Hat Enterprise Linux System Administration Guide*.

È possibile cambiare il runlevel di default durante l'avvio del sistema modificando semplicemente gli argomenti che sono passati dal boot loader al kernel. Per informazioni su come modificare il runlevel durante l'avvio, consultate la Sezione 2.8.

1.4.2. Utility dei Runlevel

Uno dei migliori modi per configurare il runlevel è di utilizzare *initscript utility*. Questi tool sono disegnati per semplificare la manutenzione dei file nella gerarchia delle directory SysV init e solleva gli amministratori di sistema dall'incombenza di manipolare i numerosi link simbolici nelle directory di `/etc/rc.d/`.

Red Hat Enterprise Linux fornisce tre di queste utility:

- `/sbin/chkconfig` — L'utility `/sbin/chkconfig` fornisce uno strumento semplice della linea di comando, per la manutenzione della gerarchia della directory `/etc/rc.d/init.d`.
- **/sbin/ntsysv** — l'utility basata su ncurses **/sbin/ntsysv** fornisce un'interfaccia basata su testo, che potrebbe essere più facile da usare di `chkconfig`.
- **Strumento di configurazione dei servizi** — Il programma grafico **Strumento di configurazione dei servizi** (`system-config-services`) è una utility flessibile per configurare i runlevel.

Per ulteriori informazioni su questi tool, consultate il capitolo *Controllo dell'accesso ai servizi* nella *Red Hat Enterprise Linux System Administration Guide*.

1.5. Arresto del sistema

Per arrestare Red Hat Enterprise Linux, l'utente root può emettere il comando `/sbin/shutdown`. La pagina man di `shutdown` offre un elenco completo delle opzioni, le due più diffuse sono:

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

Dopo aver eseguito l'arresto, l'opzione `-h` arresta la macchina, e l'opzione `-r` la riavvia.

Gli utenti della console PAM, possono usare i comandi `reboot` e `halt` per arrestare il sistema nel runlevel 1 a 5. Per maggiori informazioni sugli utenti della console PAM, consultate la Sezione 16.7.

Se il computer non si spegne da solo, attenti a non spegnerlo fino a quando non appare un messaggio indicando che il sistema è stato arrestato.

Se non aspettate la comparsa del messaggio, ne consegue che non tutte le partizioni del disco fisso vengono smontate, risultando in una corruzione del sistema.

Capitolo 2.

Il boot loader GRUB

Quando un computer con Red Hat Enterprise Linux viene alimentato, il sistema operativo viene caricato nella memoria da un programma speciale denominato *boot loader*. Un boot loader di solito è presente sul disco fisso primario del sistema o su un altro media, ed è responsabile del caricamento in memoria del kernel di Linux, dei file necessari o (in alcuni casi) di altri sistemi operativi.

2.1. Boot loader e architettura del sistema

Ogni architettura in grado di eseguire Red Hat Enterprise Linux utilizza un boot loader diverso. La seguente tabella elenca i boot loader disponibili per ogni architettura:

Architettura	Boot loader
AMD® AMD64	GRUB
IBM® eServer™ iSeries™	OS/400®
IBM® eServer™ pSeries™	YABOOT
IBM® S/390®	z/IPL
IBM® eServer™ zSeries®	z/IPL
Intel® Itanium™	ELILO
x86	GRUB

Tabella 2-1. Boot loader a seconda dell'architettura

Questo capitolo esamina i comandi e le opzioni di configurazione per ilboot loader GRUB disponibile con Red Hat Enterprise Linuxper l'architettura x86.

2.2. GRUB

GNU GRand Unified Bootloader (GRUB) è un programma che consente di selezionare quale sistema operativo o kernel è da caricare al momento dell'avvio del sistema. Consente inoltre di passare argomenti al kernel.

2.2.1. Processo di avvio di GRUB e x86

Questa sezione riporta in dettaglio il ruolo specifico di GRUB quando si effettua l'avvio di un sistema x86. Per rivedere il processo di avvio, consultare la Sezione 1.2.

Il processo di caricamento di GRUB avviene in diverse fasi:

1. *Caricamento del boot loader primario dal BIOS nell'MBR - Fase 1* [1].Il boot loader è posizionato nel piccolissimo spazio assegnato all'MBR, inferiore a 512byte ed è capace di caricare la fase 1.5 o 2 del boot loader.

1. Per ulteriori informazioni sul BIOS del sistema e sull'MBR, consultate la Sezione 1.2.1.

2. *Il boot loader della fase 1.5 è caricato in memoria da quello della fase 1, se necessario.* Alcuni elementi hardware richiedono una fase intermedia per giungere al boot loader della fase 2. Questo avviene quando la partizione `/boot/` è superiore ai 1024 cilindri della testina del disco fisso o quando si utilizza la modalità LBA. Il boot loader della fase intermedia è disponibile nella partizione `/boot/` o in una piccola sezione dell'MBR e della partizione `/boot/`.
3. *La fase 2 o boot loader secondario, viene caricata nella memoria.* Il boot loader secondario visualizza il menu di GRUB e l'ambiente dei comandi. Questa interfaccia vi consente di selezionare il sistema operativo o il kernel da avviare, il passaggio degli argomenti al kernel o di osservare i parametri del sistema.
4. *Il boot loader secondario oltre a leggere il sistema operativo o il kernel, è in grado di leggere i contenuti di `/boot/sysroot/` all'interno della memoria.* Dopo che GRUB ha determinato il sistema operativo o kernel da avviare, lo carica in memoria e cede il controllo della macchina al sistema operativo.

Il metodo utilizzato per avviare Red Hat Enterprise Linux è chiamato *caricamento diretto*, in quanto il boot loader carica direttamente il sistema operativo. Non esiste alcuna fase intermedia tra il boot loader ed il kernel.

Il processo d'avvio utilizzato da altri sistemi operativi può variare leggermente. Per esempio iI sistema operativo Microsoft® Windows®, oltre a numerosi altri sistemi operativi,vengono caricati mediante il metodo di *caricamento a catena*. Con questo metodo l'MBR fa semplicemente riferimento al primo settore della partizione contenente il sistema operativo, dove trova i file necessari per avviare il sistema.

GRUB supporta entrambi i metodi di avvio di caricamento, consentendovi di utilizzarli con qualsiasi sistema operativo.

Avvertenza

Durante l'installazione, il programma di installazione DOS e Windows di Microsoft, sovrascrive completamente l'MBR, eliminando qualsiasi boot loader esistente. Se create un sistema dual-boot, è preferibile installare prima il sistema operativo Microsoft.

2.2.2. Caratteristiche di GRUB

GRUB vanta una serie di caratteristiche che lo rendono preferibile ad altri boot loader disponibili per l'architettura x86. Ecco alcune delle peculiarità più importanti:

- *GRUB è in grado di fornire, su macchine x86, un ambiente pre-OS basato sui comandi.* In questo modo l'utente dispone della massima flessibilità nel caricamento dei sistemi operativi con determinate opzioni, o nella raccolta di informazioni riguardanti il sistema. Per anni, molte architetture non-x86, hanno utilizzato ambienti pre-OS che consentono l'avvio del sistema da una linea di comando.
- *GRUB supporta la modalità Logical Block Addressing (LBA).* La modalità LBA posiziona nel firmware dell'unità l'addressing conversion utilizzata per trovare i file nel firmware del disco fisso, ed è usato su molti IDE e su tutti i dispositivi fissi SCSI. Prima di LBA i boot loader potevano essere limitati dal cilindro 1024 e il BIOS non riusciva a individuare i file dopo quel punto. Il supporto LBA consente a GRUB di avviare i sistemi operativi dalle partizioni oltre il limite del cilindro 1024, se il BIOS supporta tale modalità LBA. La maggior parte dei BIOS la supporta.
- *GRUB può leggere le partizioni ext2.* GRUB può accedere al relativo file di configurazione `/boot/grub/grub.conf` a ogni avvio del sistema, evitandovi dunque di dover scrivere una nuova versione del boot loader primario nell'MBR tutte le volte che modificate le opzioni. L'unico

caso in cui potrebbe essere necessario reinstallare GRUB nell'MBR si verifica se il percorso fisico della partizione `/boot/` viene spostato sul disco. Per ulteriori informazioni sull'installazione di GRUB nell'MBR, consultate la Sezione 2.3.

2.3. Installazione di GRUB

Se non avete installato GRUB durante il processo di installazione, ecco il modo di farlo in seguito, e di renderlo così il vostro boot loader di default.

Prima di installare GRUB, dovete accertarvi di avere l'ultima versione disponibile di GRUB oppure potete utilizzare il pacchetto GRUB contenuto nel CDROM di installazione. Per istruzioni sull'installazione delle diverse versioni, consultate il capitolo *Gestione del pacchetto con RPM* nella *Red Hat Enterprise Linux System Administration Guide*.

Dopo avere installato il pacchetto GRUB, aprire un prompt della shell root ed eseguite il comando `/sbin/grub-install <posizione>`, dove `<posizione>` è, la posizione in cui deve essere installato il boot loader GRUB della fase 1. Per esempio, il seguente comando installa GRUB sull'MBR del dispositivo IDE master sul bus IDE primario:

```
/sbin/grub-install /dev/hda
```

Al successivo avvio del sistema dovreste visualizzare il menu del boot loader grafico GRUB prima del caricamento del kernel nella memoria.

Importante

Se GRUB viene installato su di un array RAID 1, il sistema potrebbe diventare non avviabile se si verifica un errore del disco. Viene fornito online un workaround non supportato sul seguente URL:

http://www.dur.ac.uk/a.d.stribblehill/mirrored_grub.html

2.4. Terminologia

Una delle cose più importanti da capire prima di usare GRUB è il modo in cui il programma fa riferimento a dispositivi come i dischi fissi o le partizioni. Questa informazione è fondamentale se desiderate configurare GRUB per l'avvio di più sistemi operativi.

2.4.1. Nomi dei dispositivi

Quando vi riferite ad un dispositivo particolare con GRUB, fatelo usando il seguente formato (notare che le parentesi e la virgola sono molto importanti):

`(<type-of-device><bios-device-number>,<partition-number>)`

`<type-of-device>` specifica il tipo di dispositivo dal quale GRUB stà eseguendo l'avvio. Le due opzioni più comuni sono `hd` per un disco fisso o `fd` per un dischetto da 3.5. È disponibile un tipo di dispositivo meno usato chiamato `nd` per un disco di rete. Le istruzioni su come configurare GRUB in modo da eseguire l'avvio attraverso la rete, sono disponibili su http://www.gnu.org/software/grub/manual/.

`<bios-device-number>` è il numero del dispositivo BIOS. Il disco fisso IDE primario viene numerato con `0` e il disco fisso IDE secondario, viene numerato `1`. La sintassi è simile a quella usata per i dispositivi dal kernel. Per esempio, `a` in `hda` per il kernel è analogo a `0` in `hd0` per GRUB, `b` in `hdb` è analogo a `1` in `hd1`, e così via.

Il <*numero-partizione*> indica il numero di una partizione specifica su di un dispositivo. Come per il <*bios-numero-dispositivo*>, la numerazione delle partizioni inizia da `0`. Tuttavia, le partizioni BSD sono invece rappresentate da lettere, con `a`corrispondente a `0`, `b` corrispondente a `1`, e così via.

Suggerimento

Il sistema di numerazione di GRUB parte da `0` e non da `1`. Questo è uno degli errori più comuni commessi dai nuovi utenti.

Per darvi un esempio, se un sistema possiede più di un disco fisso, GRUB si riferisce al primo disco fisso come `(hd0)` e il secondo come `(hd1)`. Lo stesso avviene per le partizioni, GRUB infatti si riferisce alla prima partizione sul disco fisso come `(hd0,0)`, e la terza partizione sul secondo disco fisso come `(hd1,2)`.

Per assegnare un nome a dispositivi e partizioni, GRUB utilizza le regole seguenti:

- Tutti i dischi fissi, non importa se sono IDE o SCSI, iniziano con `hd`. Le lettere `fd`.sono usate per specificare i dischetti 3.5.
- Per specificare un dispositivo intero, senza tener conto delle sue partizioni, occorre semplicemente tralasciare la virgola e il numero di partizione. Questo aspetto è importante quando GRUB deve configurare l'MBR per un disco in particolare. Per esempio `(hd0)` specifica l'MBR sul primo dispositivo e `(hd3)` indica il quarto.
- Se un sistema presenta dispositivi drive multipli, è importante alloraconoscere il loro ordine all'interno del BIOS. Tale compito non risulta essere molto complesso se il sistema presenta solo unità IDE o SCSI, se invece sono unità miste, è importante accedere prima il tipo di unità che presenta la partizione di avvio.

2.4.2. Nomi dei file ed elenchi dei blocchi

Quando digitate i comandi per GRUB i quali si riferiscono ad un file, come un elenco del menu, è necessario includere il file subito dopo aver specificato il dispositivo e la partizione.

Qui di seguito viene riportata la struttura di tale comando:

(<*device-type*><*device-number*>,<*partition-number*>)<*/path/to/file*>

In questo esempio, sostituire <*device-type*> con `hd`, `fd`, o `nd`. Sostituire <*device-number*> con il numero intero per il dispositivo. Sostituire <*/path/to/file*> con un percorso assoluto sulla parte superiore del dispositivo.

Potete inoltre indicare a GRUB i file che non compaiono nel filesystem, come per esempio un loader a catena (chain loader) contenuto nei primissimi blocchi di una partizione. Per caricare questi file, occorre fornire un *elenco dei blocchi*, che indichi a GRUB, blocco per blocco, la posizione del file nella partizione. Poiché un file può essere composto da molti insiemi di blocchi differenti, il suddetto elenco utilizza una sintassi speciale. Il blocco contenente il file, viene specificato da un numero di offset di blocchi, seguito dal numero di blocchi riferiti da quel punto specifico di offset. Gli offset dei blocchi sono elencati in un elenco e separati da virgole.

Considerate il seguente elenco di blocchi:

```
0+50,100+25,200+1
```

Questo esempio specifica un file che inizia sul primo blocco sulla partizione e utilizza i blocchi da 0 a 49, 99 a 124, e 199.

Quando si usa GRUB è utile sapere come scrivere gli elenchi dei blocchi in modo da caricare i sistemi operativi che utilizzano il caricamento a catena. Potete omettere il numero di blocchi se iniziate dal blocco 0. Per esempio, il file di caricamento a catena nella prima partizione del primo disco fisso avrà il seguente nome:

```
(hd0,0)+1
```

Potete inoltre utilizzare il comando `chainloader` con la stessa indicazione nella linea di comando di GRUB dopo aver impostato come root il dispositivo e la partizione corretti:

```
chainloader +1
```

2.4.3. Il file System root e GRUB

Alcuni utenti si confondono nell'utilizzare il termine *filesystem root* con GRUB. È importante ricordare che il filesystem root di GRUB non ha nulla a che fare con il filesystem root di Linux.

Il file system root di GRUB è il livello superiore del dispositivo specificato. Per esempio, il file immagine `(hd0,0)/grub/splash.xpm.gz` è posizionato all'interno della directory `/grub/` sul livello superiore (o root) della partizione `(hd0,0)` (la quale è la partizione `/boot/` per il sistema).

Successivamente, potete eseguire il comando `kernel` indicando come opzione la posizione del file del kernel. Una volta avviato il kernel di Linux, esso imposta il file system root conosciuto dagli utenti di Linux. Il file system root originale di GRUB ed i suoi mount vengono rimossi, il loro unico scopo è quello di caricare il file del kernel.

Per maggiori informazioni, consultate le note relative ai comandi `root` e `kernel` nella Sezione 2.6.

2.5. Interfacce di GRUB

GRUB dispone di tre potenti interfacce che forniscono diversi livelli di funzionalità. Ognuna di queste interfacce vi permette di avviare il kernel di Linux oppure un altro sistema operativo.

Le interfacce sono:

Note Bene

È possibile accedere alle seguenti interfacce di GRUB premendo, entro tre secondi, qualsiasi pulsante presente nella schermata di bypass del menu di GRUB.

Menu Interface

Questa è l'interfaccia di default mostrata quando GRUB viene configurato dal programma di installazione. Viene visualizzato un menu dei sistemi operativi o dei kernel preconfigurati, ordinati per nome. Potete utilizzare i tasti freccia per selezionare una opzione diversa da quella predefinita, e premere [Invio] per avviarla. In alternativa è possibile impostare un periodo di timeout, dopo il quale GRUB inizia a caricare l'opzione predefinita.

Dal menu a interfaccia potete inoltre digitare [e] per modificare i comandi della voce di menu evidenziata oppure [c] per visualizzare un'interfaccia a linea di comando.

Per ulteriori informazioni sulla configurazione di questa interfaccia, consultate la Sezione 2.7.

Interfaccia Editor per le entry del menu

Per passare a questa interfaccia è necessario premere il tasto [e] dal menu del boot loader. I comandi di GRUB per questa voce vengono visualizzati in questo ambito ed è possibile modificare queste linee di comando, prima di avviare il sistema operativo, aggiungendole ([o] inserisce la nuova linea dopo la riga corrente e [O] prima della riga corrente), modificandole ([e]) o cancellandole ([d]).

Dopo aver effettuato le modifiche, potete digitare [b] per applicare tali modifiche e avviare il sistema operativo. Il tasto [Esc] vi riporta all'interfaccia a menu standard senza applicare le modifiche. Invece digitando [c] potete visualizzare l'interfaccia della linea di comando.

Suggerimento

Per infomazioni su come modificare i runlevel con GRUB usando l'editor delle entry del menu, consultate la Sezione 2.8.

Interfaccia della linea di comando

Si tratta dell'interfaccia di base di GRUB, ma è anche quella che vi fornisce il maggior controllo. Infatti qui è possibile digitare tutti i comandi di GRUB e premere semplicemente [Invio] per eseguirli. Questa interfaccia dispone di caratteristiche avanzate simili a quelle della shell, tra cui la funzione di completamento automatico dei comandi, basata sul contesto, con il tasto [Tab] e le combinazioni di tasti [Ctrl] quando si digitano comandi come [Ctrl]-[a] per spostarsi all'inizio di una riga e [Ctrl]-[e] per spostarsi alla fine. Inoltre i tasti freccia, [Home], [Fine] e [Cancella] funzionano come nella shell `bash`.

Per un elenco di comandi comuni, consultate la Sezione 2.6.

2.5.1. Ordine di caricamento delle interfacce

Quando GRUB carica la seconda fase del boot loader, esso và alla ricerca dei propri file di configurazione. Quando trovati, la schermata di bypass dell'interfaccia del menu viene visualizzata. Se si preme un pulsante in meno di tre secondi, GRUB crea un elenco e visualizza l'interfaccia del menu. Se non si preme alcun pulsante, viene utilizzata nel menu di GRUB, la entry di default del kernel.

Se non è possibile individuare il file di configurazione oppure se questo non è leggibile, GRUB visualizza l'interfaccia a linea di comando per permettervi di digitare manualmente i comandi necessari all'avvio di un sistema operativo.

Se il file di configurazione non è valido, GRUB visualizza l'errore e richiede un input. Ciò può essere molto utile perché vi consente di vedere esattamente dove si è verificato il problema e di risolverlo nel file. Premendo un qualsiasi tasto tornerete al menu a interfaccia, dove potrete modificare l'opzione di menu e correggere il problema in base all'errore segnalato da GRUB. Se la correzione non ha buon esito, l'errore viene segnalato e potete ricominciare da capo.

2.6. Comandi

GRUB dispone di numerosi comandi nella propria interfaccia della linea di comando. Per alcuni di questi comandi è possibile digitare delle opzioni, dopo il nome, che vanno separate tramite spazi dal comando e da altre opzioni.

Qui di seguito viene riportato un elenco dei comandi più utili:

- `boot` — Consente di avviare il sistema operativo o il loader a catena (chainloader) specificato e caricato per ultimo.

- `chainloader </path/to/file>` — Permette di caricare il file specificato come un loader a catena. Se il file si trova nel primo settore della partizione indicata, utilizzate `+1`, invece del nome del file.

  Il seguente è un esempio del comando `chainloader`:
  ```
  chainloader +1
  ```

- `displaymem` — serve a visualizzare lo spazio di memoria disponibile in base alle informazioni fornite dal BIOS. Questo comando è utile per determinare la quantità di RAM di cui dispone il sistema prima di avviarlo.

- `initrd </path/to/initrd>` — Consente di indicare una RAM disk iniziale da utilizzare all'avvio. Un `initrd` è necessario quando il kernel richiede alcuni moduli per eseguire un avvio corretto, come nel caso in cui la partizione root viene formattata con il filesystem ext3.

  Il seguente è un esempio del comando `initrd`:
  ```
  initrd /initrd-2.6.8-1.523.img
  ```

- `install <stage-1> <install-disk> <stage-2> p <config-file>` — Serve a installare GRUB sull'MBR del sistema.

  - `<fase-1>` — che caratterizza il dispositivo, la partizione o il file contenenti l'immagine del boot loader primario, come `(hd0,0)/grub/stage1`.
  - `<disco-install>` — Specifica il disco dove il boot loader della prima fase dovrebbe essere installato, come ad esempio `(hd0)`.
  - `<stage-2>` — Invia la posizione del boot loader della fase 2 al boot loader della fase 1, come ad esempio `(hd0,0)/grub/stage2`.
  - `p <config-file>` — Indica al comando `install` che è stato specificato un file di configurazione del menu nella sezione `<config-file>`. come ad esempio `(hd0,0)/grub/grub.conf`.

  
  Avvertenza

  Il comando `install` sovrascrive qualsiasi informazione già posizionata sull'MBR.

- `kernel </path/to/kernel> <opzione-1> <opzione-N>` ... — Specifica il file del kernel da caricare quando si avvia il sistema operativo. Sostituire `</path/to/kernel>` con un percorso assoluto dalla partizione specificata dal comando root. Sostituire `<option-1>` con le opzioni per il kernel di Linux, come ad esempio `root=/dev/hda5` per specificare il dispositivo sul quale è situata la partizione root per il sistema. Opzioni multiple possono essere inviate al kernel in un elenco separato da uno spazio.

  Il seguente è un esempio del comando `kernel`:
  ```
  kernel /vmlinuz-2.4.21 root=/dev/hda5
  ```

  L'opzione nell'esempio precedente specifica che il file system root per Linux, è posizionato sulla partizione `hda5`.

- `root (<device-type>< device-number>,<partition>)` — Configura la partizione root per GRUB, come ad esempio `(hd0,0)`, ed esegue il montaggio della partizione.

  Il seguente è un esempio del comando `root`:
  ```
  root (hd0,0)
  ```

- `rootnoverify (<device-type><device-number>,<partition>)` — Configura la partizione root per GRUB, proprio come il comando `root`, ma non esegue il montaggio della partizione.

Sono disponibili anche altri comandi; digitare `help --all` per un elenco completo dei comandi. Per una descrizione di tutti i comandi di GRUB, consultare la documentazione disponibile online su http://www.gnu.org/software/grub/manual/.

2.7. File di configurazione del menu di GRUB

Il file di configurazione usato per creare l'elenco dei sistemi operativi da avviare nell'interfaccia a menu, consente all'utente di selezionare un gruppo di comandi preimpostati da eseguire. È possibile utilizzare i comandi indicati nella Sezione 2.6 nonché alcuni comandi speciali utilizzabili solo nel file di configurazione.

2.7.1. Struttura del file di configurazione

Il file di configurazione dell'interfaccia a menu di GRUB è `/boot/grub/grub.conf`. I comandi per impostare le preferenze generali dell'interfaccia a menu, si trovano all'inizio del file e sono seguiti da diverse voci per ognuno dei sistemi operativi o kernel elencati nei menu.

Ecco un esempio di file di configurazione di base del menu di GRUB, creato per l'avvio di Red Hat Enterprise Linux o di Microsoft Windows 2000:

```
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux AS (2.6.8-1.523)
        root (hd0,0)
        kernel /vmlinuz-2.6.8-1.523 ro root=/dev/VolGroup00/LogVol00 rhgb quiet
        initrd /initrd-2.6.8-1.523.img

# section to load Windows
title Windows
        rootnoverify (hd0,0)
        chainloader +1
```

Questo file indica a GRUB di creare un menu con Red Hat Enterprise Linux come sistema operativo di default che si avvia dopo 10 secondi. Vengono fornite due sezioni, una per ogni sistema operativo indicato, con comandi specifici per la tabella delle partizioni di questo sistema.

Note Bene

Notare che il default è specificato come numero intero. Esso si riferisce alla prima linea `title` nel file di configurazione di GRUB. Per la sezione `Windows` da impostare come default nell'esempio precedente, modificare `default=0` to `default=1`.

Tuttavia impostare il file di configurazione del menu di GRUB per l'avvio di più sistemi operativi esula dallo scopo di questo capitolo. Consultare la Sezione 2.9 per un elenco di risorse aggiuntive.

2.7.2. Direttive del file di configurazione

Le direttive seguenti sono generalmente utilizzate solo nel file di configurazione a menu di GRUB:

- `chainloader` *`</path/to/file>`* — Permette di caricare il file specificato come un loader a catena. Sostituire *`</path/to/file>`* con il percorso assoluto sul loader a catena. Se il file è posizionato sul primo settore della partizione specificata, usare l'elenco a blocco, `+1`.
- `color` *`<normal-color>`* *`<selected-color>`* — Consente di impostare determinati colori da utilizzare nel menu, uno per il primo piano e l'altro per lo sfondo. È sufficiente indicare i nomi dei colori, come `red/black`. Ecco un esempio:
  `color red/black green/blue`

- `default=<integer>` — Sostituire `<integer>` con il numero di 'title' della entry di default da caricare se l'interfaccia del menu va in time out.
- `=<integer>` — Sostituisce `<integer>` con il numero di 'title' della entry da provare se il primo tentativo fallisce.
- `hiddenmenu` — Impedisce la visualizzazione del menu a interfaccia di GRUB caricando la voce `default` al termine del periodo di `timeout`. L'utente può vedere il menu standard di GRUB premendo [Esc].
- `initrd </path/to/initrd>` — Consente di indicare un RAM disk iniziale da utilizzare all'avvio. Sostituire `</path/to/initrd>` con il percorso assoluto per il RAM disk iniziale.
- `kernel </path/to/kernel> <option-1> <option-N>` — Specifica il file del kernel da caricare quando si avvia il sistema operativo. Sostituire `</path/to/kernel>` con un percorso assoluto dalla partizione specificata dalla direttiva root. Opzioni multiple possono essere inviate al kernel una volta caricato.
- `password=<password>` — Impedisce agli utenti che non conoscono la password di modificare le voci di questa opzione del menu.

  Se lo desiderate, potete indicare un file di configurazione del menu alternativo dopo la direttiva `password=<password>`. In tal modo, GRUB riavvia il boot loader della seconda fase e usa il file di configurazione alternativo specificato, per creare il menu. Se il file di configurazione del menu alternativo non viene indicato dal comando, un utente che conosce la password può modificare il file di configurazione in uso al momento.

  Per maggiori informazioni su come rendere sicuro GRUB, consultare il capitolo intitolato *Sicurezza della workstation* nella *Red Hat Enterprise Linux Security Guide*.
- `root (<device-type><device-number>,<partition>)` — Configura la partizione root per GRUB, come ad esempio `(hd0,0)`, ed esegue il montaggio della partizione.
- `rootnoverify (<device-type><device-number>,<partition>)` — Configura la partizione root per GRUB, proprio come il comando `root`, ma non esegue il montaggio della partizione.
- `timeout =<integer>` — Specifica l'intervallo, in secondi, che GRUB attende prima di caricare la entry scelta nel comando `default`.
- `splashimage=<path-to-image>` — Specifica la posizione dell'immagine splash screen da utilizzare all'avvio di GRUB.
- `titolo group-title` — Imposta un nome da utilizzare con un particolare gruppo di comandi utilizzati per caricare un sistema operativo o un kernel.

Per aggiungere dei commenti leggibili da utenti al file di configurazione a menu, iniziare la riga con il carattere (`#`).

2.8. Modifica dei runlevel all'avvio

In Red Hat Enterprise Linux è possibile modificare il runlevel di default al momento dell'avvio.

Per modificare il runlevel di una singola sessione d'avvio, utilizzare le seguenti istruzioni:

- Quando al momento dell'avvio compare la schermata bypass del menu di GRUB, premete qualsiasi pulsante per poter accedere al menu di GRUB (per fare questo, non fate trascorrere un tempo superiore ai tre secondi).
- Premete [a] per aggiungere il comando `kernel`.

- Aggiungere <space><*runlevel*> alla fine della riga corrispondente alle opzioni d'avvio per il runlevel desiderato. Per esempio, la seguente entry inizierà un processo d'avvio all'interno del runlevel 3:

```
grub append> ro root=/dev/VolGroup00/LogVol00 rhgb quiet 3
```

2.9. Risorse aggiuntive

Questo capitolo è stato concepito solo come introduzione a GRUB. Per saperne di più sul suo funzionamento, consultate le risorse descritte qui di seguito.

2.9.1. Documentazione installata

- `/usr/share/doc/grub-`<*version-number*>`/` — Questa directory contiene informazioni utili relative all'utilizzo e alla configurazione di GRUB, dove <*version-number*> corrisponde alla versione del pacchetto GRUB installato.
- `info grub` — La pagina info di GRUB contiene un esercizion pratico, un manuale di riferimento per l'utente, un manuale di riferimento per il programmatore e un documento di tipo FAQ (con le domande più frequenti) su GRUB e il relativo utilizzo.

2.9.2. Siti Web utili

- http://www.gnu.org/software/grub/ — La home page del progetto GNU GRUB. Questo sito contiene le informazioni sull'andamento dello sviluppo di GRUB e una serie di FAQ.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Multiboot-with-GRUB.html — queste pagine Web indagano sui diversi usi di GRUB, tra cui la possibilità di avviare sistemi operativi diversi da Linux.
- http://www.linuxgazette.com/issue64/kohli.html — questa pagina Web contiene un articolo introduttivo alla configurazione di GRUB sul vostro sistema e comprende inoltre una panoramica delle opzioni della linea di comando.

2.9.3. Libri correlati

- *Red Hat Enterprise Linux Security Guide*; Red Hat, Inc. — Ll capitolo *Sicurezza della Workstation*, riporta in modo conciso come rendere sicurio i boot loader GRUB.

Capitolo 3.

Struttura del filesystem

3.1. Perché condividere una struttura comune?

La struttura del filesystem rappresenta, in un sistema operativo, il livello di base di una organizzazione. Quasi tutti i modi in cui un sistema operativo interagisce con gli utenti, le applicazioni e i modelli di sicurezza dipendono dal modo in cui il sistema memorizza i suoi file su un dispositivo di memorizzazione. Per svariate ragioni è importante che gli utenti, così come i programmi, possano fare riferimento a una linea guida comune per sapere dove leggere e scrivere i file.

I file system suddividono i file in due categorie logiche:

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

I file *condivisibili* sono file a cui vari host possono accedere in modo locale e remoto, mentre i file *non condivisibili* sono disponibili localmente. I file *variabili* come i documenti, possono cambiare in qualsiasi momento. I file *statici*, come i file binari, non cambiano senza un'azione dell'amministratore del sistema.

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

3.2. Panoramica sull'FHS (Filesystem Hierarchy Standard)

Red Hat Enterprise Linux usa la struttura del file system *Filesystem Hierarchy Standard* (*FHS*), che definisce i nomi, la posizione e i permessi per molti file e directory.

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

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

3.2.1. Organizzazione dell'FHS

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

Lo standard completo è disponibile online su http://www.pathname.com/fhs/.

3.2.1.1. La directory `/boot/`

La directory `/boot/` contiene file statici necessari per l'avvio del sistema, come ad esempio il kernel di Linux. Questi file sono essenziali per un avvio corretto del sistema.

Avvertenza

Non eliminate la directory `/boot/`, altrimenti non sarà più possibile avviare il sistema.

3.2.1.2. La directory `/dev/`

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

3.2.1.3. La directory `/etc/`

La directory `/etc/` è riservata ai file di configurazione locali presenti sulla vostra macchina. Nessun file binario deve essere inserito in `/etc/`. Tutti i file binari che sono stati precedentemente inseriti in `/etc/`, devono essere trasferiti in `/sbin/` oppure in `/bin/`.

Le directory `X11/` e `skel/` sono sottodirectory di `/etc/`:

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

La directory `/etc/X11/` viene designata per i file di configurazione del sistema X Window, come ad esempio `XF86Config`. La directory `/etc/skel/` viene designata per i file dell'utente "skeleton", cioè i file che servono per popolare una home directory quando viene creato un nuovo utente.

3.2.1.4. La directory `/lib/`

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

3.2.1.5. La directory `/media/`

La directory `/mnt/` contiene le sottodirectory utilizzate come mount point per quei media in grado di essere rimossi, come ad esempio i CD-ROM, Zip ed i dischetti floppy da 3.5.

3.2.1.6. La directory `/mnt/`

La directory `/mnt/` è riservata ai filesystem montati temporaneamente, come i mount del file system NFS. Per tutti i media in grado di essere rimossi, utilizzare la directory `/media/`

Nota Bene

Questa directory non deve essere installata dai programmi di installazione.

3.2.1.7. La directory `/opt/`

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

Un pacchetto che posiziona i file nella directory `/opt/`, crea una directory che presenta lo stesso nome del pacchetto. Questa directory, in ritorno, conserva i file che altrimenti verrebbero sparsi attraverso il file system, dando all'amministratore del sistema un modo semplice per determinare il ruolo di ogni file all'interno di un pacchetto particolare.

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

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

3.2.1.8. La directory `/proc/`

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

Data la svariata quantità di dati disponibili in `/proc/` ed i vari modi in cui questa directory può essere usata per comunicare con il kernel, è stato dedicato un intero capitolo all'argomento. Per maggiori informazioni, consultate Capitolo 5.

3.2.1.9. La directory `/sbin/`

La directory `/sbin/` contiene gli eseguibili utilizzati unicamente dall'utente root. Gli eseguibili in `/sbin/` servono solo al momento dell'avvio e per eseguire le operazioni di recupero del sistema.L'FHS dice:

> `/sbin` contiene normalmente i binari essenziali per l'avvio, il ripristino, il recupero e/o la riparazione del sistema oltre a quelli presenti in `/bin`. Qualunque altro programma eseguito dopo il montaggio della directory `/usr/` (quando non si verifica alcun problema) deve essere collocato in `/usr/sbin`. I Programmi di gestione del sistema installati in modo locale devono essere inseriti in `/usr/local/sbin`.

In `/sbin/` trovate, come minimo, i seguenti programmi:

```
arp, clock,halt,
init, fsck.*, grub,
ifconfig, mingetty, mkfs.*,
mkswap, reboot, route,
shutdown, swapoff, swapon
```

3.2.1.10. La directory `/srv/`

La directory `/srv/` contiene i dati specifici al sito forniti dal vostro sistema, che a sua volta stà eseguendo Red Hat Enterprise Linux. Questa directory fornisce agli utenti la posizione dei file data riguardanti un servizio particolare, come ad esempio FTP, WWW, o CVS. I dati che si riferiscono ad un utente in particolare, dovrebbero essere conservati all'interno della directory `/home/`.

Nota Bene

Tenete presente che i file data che si trovano attualmente in `/var/`, *potrebbero* essere spostate in `/srv/` in release future.

3.2.1.11. La directory `/sys/`

La directory `/sys/` utilizza il nuovo file system virtuale specifico al kernel 2.6. Grazie al maggior supporto per dispositivi hardware hot plug con il kernel 2.6, la directory `/sys/` contiene le stesse informazioni contenute in `/proc/`, ma in grado di visualizzare una panoramica gerarchica di informazioni specifiche riguardanti i dispositivi hot plug.

Per verificare il montaggio effettivo dei dispositivi USB e FireWire, consultate le pagine man di `/sbin/hotplug` e `/sbin/udev`

3.2.1.12. La directory `/usr/`

La directory `/usr/` contiene tutti i file che possono essere condivisi attraverso macchine multiple. La directory `/usr/` è solitamente nella propria partizione, ed è montata come sola lettura. Le seguenti directory dovrebbero rappresentare le sottodirectory di `/usr/`:

```
/usr
  |- bin/
  |- etc/
  |- games/
  |- include/
  |- kerberos/
  |- lib/
  |- libexec/
  |- local/
  |- sbin/
  |- share/
  |- src/
  |- tmp -> ../var/tmp/
  |- X11R6/
```

Sotto la directory `/usr/`, la sottodirectory `bin/` contiene gli eseguibili, `etc` contiene i file di configurazione del sistema, `games` quelli per i giochi, `include/` contiene i file header di C, `kerberos/` contiene i binari e molte altre cose relative a Kerberos, e `lib/` contiene i file object e le librerie che non sono stati concepiti per essere usati direttamente dagli utenti o dagli script della shell. La directory `libexec/` contiene piccoli programmi d'aiuto richiamati da altri programmi, `sbin/` è per i binari di amministrazione del sistema (quelli che non appartengono alla directory `/sbin/`), `share/` contiene i file non specifici per l'architettura, `src/` contiene i codici sorgente e `X11R6/` è destinato al Sistema X Window (XFree86/ su Red Hat Enterprise Linux).

3.2.1.13. La directory `/usr/local/`

L'FHS afferma che:

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

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

```
/usr/local
       |- bin/
       |- etc/
       |- games/
       |- include/
       |- lib/
       |- libexec/
       |- sbin/
       |- share/
       |- src/
```

In Red Hat Enterprise Linux, l'uso desiderato della directory `/usr/local/` è leggermente diverso da quello specificato dall'FHS. L'FHS afferma che `/usr/local/` si dovrebbe trovare nel posto in cui è memorizato il software che non deve subire aggiornamenti del sistema. Poiché gli aggiornamenti del software vengono effettuati in modo sicuro con *RPM Package Manager* (*RPM*), non è necessario proteggere i file mettendoli in `/usr/local/`. Invece, vi raccomandiamo di usare `/usr/local/` per il software locale della vostra macchina.

Per esempio, se la directory `/usr/` viene montata come sola condivisione NFS da un host remoto, è ancora possibile installare un pacchetto o un programma sotto la directory `/usr/local/`.

3.2.1.14. La directory `/var/`

Poiché con FHS dovete essere in grado di montare `/usr/` in sola lettura, tutti i programmi che scrivono il file log o necessitano delle directory `spool/` o `lock/` dovrebbero scriverli nella directory `/var/`. L'FHS afferma che `/var/` è per:

> ...file di dati variabili. Questa directory contiene le directory e i file di spool, dati di loggin e di amministrazione, file temporanei e transitori.

Le seguenti directory si trovano all'interno della directory `/var/`:

```
/var
  |- account/
  |- arpwatch/
  |- cache/
  |- crash/
  |- db/
  |- empty/
  |- ftp/
  |- gdm/
  |- kerberos/
  |- lib/
  |- local/
  |- lock/
```

```
|- log/
|- mail -> spool/mail/
|- mailman/
|- named/
|- nis/
|- opt/
|- preserve/
|- run/
+- spool/
     |- at/
     |- clientmqueue/
     |- cron/
     |- cups/
     |- exim/
     |- lpd/
     |- mail/
     |- mailman/
     |- mqueue/
     |- news/
     |- postfix/
     |- repackage/
     |- rwho/
     |- samba/
     |- squid/
     |- squirrelmail/
     |- up2date/
     |- uucp
     |- uucppublic/
     |- vbox/
|- tmp/
|- tux/
|- www/
|- yp/
```

I file log del sistema, come `messages/` e `lastlog/`, si trovano in `/var/log/`. La directory `/var/lib/rpm/` contiene anche i database del sistema RPM. I file lock si trovano nella directory `/var/lock/`, solitamente in directory particolari per il programma che usa in modo specifico il file. La directory `/var/spool/` possiede le sottodirectory per i programmi nei quali vengono conservati i file data.

3.3. Posizione dei file speciali sotto Red Hat Enterprise Linux

Red Hat Enterprise Linux ha esteso leggermente la struttura FHS per adattarsi ad alcuni file speciali.

Molti dei file che riguardano RPM sono conservati nella directory `/var/lib/rpm/`. Per maggiori informazioni in merito agli RPM, cosultate il capitolo intitolato *Gestione di pacchetti con RPM* nella *Red Hat Enterprise Linux System Administration Guide*.

La directory `/var/spool/up2date/` contiene i file utilizzati dal **Red Hat Update Agent**, contenente le informazioni relative agli header RPM per il sistema. Questa posizione può anche essere utilizzata per memorizzare temporaneamente gli RPM scaricati durante l'aggiornamento del sistema. Per maggiori informazioni relative a Red Hat Network, consultate il sito relativo all'indirizzo https://rhn.redhat.com/.

Un'altra posizione specifica di Red Hat Enterprise Linux è la directory `/etc/sysconfig/`, dove vengono conservate le informazioni relative alla configurazione. Molti script eseguiti durante l'avvio

usano i file contenuti in questa directory. Per maggiori infromazioni sul contenuto di questa directory e sul ruolo che questi file svolgono nell'ambito del processo di avvio, consultate Capitolo 4.

Infine, un'altra directory degna di nota è `/initrd/`. Si tratta di una directory vuota, ma viene utilizzata come mount point cruciale durante il processo di avvio.

Avvertenza

Non eliminate per nessuna ragione la directory `/initrd/`, altrimenti non sarà più possibile avviare il sistema e comparirà un messaggio di errore panic relativo al kernel.

Capitolo 4.

La directory `sysconfig`

La directory `/etc/sysconfig/` contiene un certo numero di file di configurazione per Red Hat Enterprise Linux.

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

4.1. File contenuti in `/etc/sysconfig/`

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

- `amd`
- `apmd`
- `arpwatch`
- `authconfig`
- `autofs`
- `clock`
- `desktop`
- `devlabel`
- `dhcpd`
- `exim`
- `firstboot`
- `gpm`
- `harddisks`
- `hwconf`
- `i18n`
- `init`
- `ip6tables-config`
- `iptables-config`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`
- `named`
- `netdump`
- `network`
- `ntpd`

- pcmcia
- radvd
- rawdevices
- samba
- sendmail
- selinux
- spamassassin
- squid
- system-config-securitylevel
- system-config-users
- system-logviewer
- tux
- vncservers
- xinetd

Nota bene

Se alcuni dei file di seguito elencati non sono presenti nella directory /etc/sysconfig/, il programma corrispondente potrebbe non essere installato.

Quanto segue rappresenta una descrizione di questi file. I file non riportati e le opzioni aggiuntive per i file setssi, sono disponibili nel file /usr/share/doc/initscripts-<*version-number*>/sysconfig.txt (sostituire <*version-number*> con la versione del pacchetto initscripts). Alternativamente, può risultare utile consultare gli initscript nella directory /etc/rc.d/.

4.1.1. /etc/sysconfig/amd

Il file /etc/sysconfig/amd contiene diversi parametri utilizzati da amd, e che consentono di montare e smontare automaticamente i file system.

4.1.2. /etc/sysconfig/apmd

Il file /etc/sysconfig/apmd viene utilizzato da apmd per configurare le impostazioni di potenza da avviare/terminare/modificare in caso di presenza di una sospensione o di un ripristino. Questo file influenza il modo di funzionamento di apmd durante l'avvio, a seconda se il vostro hardware supporti l'*Advanced Power Management* (*APM*) oppure se l'utente abbia configurato il sistema in modo da utilizzarlo. Il demone apm è un programma di controllo che utilizza il codice di gestione della potenza all'interno del kernel di Linux. Se usate un portabile esso è in grado di segnalarvi lo stato della batteria e di altre impostazione relative alla potenza.

4.1.3. /etc/sysconfig/arpwatch

Il file /etc/sysconfig/arpwatch serve ad inviare argomenti al demone arpwatch durante l'avvio del sistema. Il demone arpwatch mantiene una tabella di indirizzi Ethernet MAC e dei corrispondenti indirizzi IP. Per default, questo file imposta come proprietario del processo arpwatch l'utente pcap, inviando altresì qualsiasi messaggio alla coda di posta root. Per ulteriori informazioni sui parametri utilizzati in questo file, consultate la pagina man di arpwatch.

4.1.4. /etc/sysconfig/authconfig

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

- USEMD5=<*value*>, dove <*valore*> può essere sostituito con uno dei seguenti valori:
  - yes — MD5 se volete utilizzare MD5 per l'autenticazione.
  - no — se non volete utilizzare MD5 per l'autenticazione.

- USEKERBEROS=<*valore*>, dove <*value*> può essere sostituito con uno dei seguenti valori:
  - yes — se volete utilizzare Kerberos per l'autenticazione.
  - no — se non volete utilizzare Kerberos per l'autenticazione.

- USELDAPAUTH=<*valore*>, dove <*valore*> può essere sostituito con uno dei seguenti valori:
  - yes — se volete utilizzare LDAP per l'autenticazione.
  - no — se non volete utilizzare LDAP per l'autenticazione.

4.1.5. /etc/sysconfig/autofs

Il file /etc/sysconfig/autofs definisce le opzioni personali per il montaggio automatico dei dispositivi. Questo file controlla la funzione dei demoni automount, i quali sono in grado di eseguire il montaggio automatico dei file system durante il loro utilizzo, oppure un processo di unmount dopo un certo periodo di inattività dei file system stessi. I file system possono includere i file system di rete, i CD-ROM, i dischetti e altri tipi di media.

Il file /etc/sysconfig/autofs può contenere quanto segue:

- LOCALOPTIONS="<*value*>", dove "<*value*>" specifica le regole di automount specifiche della macchina. Il valore di default risulta essere una riga vuota ("").
- DAEMONOPTIONS="<*value*>", dove "<*value*>" risulta essere il periodo di automount espresso in secondi, prima dello smontaggio del dispositivo. Il valore di default è di 60 secondi ("--timeout=60").
- UNDERSCORETODOT=<*value*>, dove <*value*> risulta essere il valore binario che decide se convertire i trattini presenti nei file name in puntini. Per esempio, auto_home in auto.home e auto_mnt in auto.mnt. Il valore di default è 1 (vero).
- DISABLE_DIRECT=<*value*>, dove <*value*> è un valore binario in grado di decidere se abilitare o meno il supporto per il montaggio diretto, in quanto l'implementazione di Linux non è conforme all'automounter di Sun Microsystems. Il valore di default è 1 (vero), e permette di avere una certa compatibilità con la sintassi di specificazione delle opzioni automounter di Sun.

4.1.6. /etc/sysconfig/clock

Il file /etc/sysconfig/clock controlla l'interpretazione dei valori letti dall'orologio del sistema.

I valori corretti sono i seguenti:

- UTC=<*valore*>, dove <*valore*> può essere sostituito con uno dei seguenti valori boolean:
  - true o yes — indica che l'orologio è impoostato secondo l'ora Universale.
  - false o no — indica che l'orologio è impostato secondo l'ora locale.

- ARC=<*valore*>, dove <*valore*> può essere sostituito con uno dei seguenti valori:
  - true o yes — Èattivo il time offset di 42 anni della console ARC. Questa impostazione è solo valida sui sistemi ARC o Alpha basati su AlphaBIOS).
  - false o no — Questo valore indica che viene utilizzato il metodo normale del periodo di UNIX.
- SRM=<*valore*>, dove <*valore*> può essere sostituito con uno dei seguenti valori:
  - true o yes — Indica che è in attivo l'epoca 1900 della console SRM. Questa impostazione è solo valida sui sistemi Alpha basati su SRM.
  - false o no — Questo valore indica che viene utilizzato il metodo normale del periodo di UNIX.
- ZONE=<*nome del file*> — Indica il file del fuso orario sotto /usr/share/zoneinfo dove /etc/localtime ne rappresenta una copia. Il file contiene informazioni come ad esempio: ZONE="America/New York"

Le precedenti versioni di Red Hat Enterprise Linux usavano i seguenti valori (le quali sono sconsigliate):

- CLOCKMODE=<*valore*>, dove <*valore*> può essere sostituito con uno dei seguenti valori:
  - GMT — indica che l'orologio è impostato secondo l'ora Universale (Ora del meridiano di Greenwich).
  - ARC — indica che il time offset di 42 anni è attivo (solo per sistemi basati su Alpha).

4.1.7. /etc/sysconfig/desktop

Il file /etc/sysconfig/desktop specifica il desktop per i nuovi utenti, e quale display manager da eseguire una volta entrati nel runlevel 5.

I valori corretti sono i seguenti:

- DESKTOP="<*valore*>", dove "<*valore*>" può essere uno dei seguenti valori:
  - GNOME — Seleziona l'ambiente del desktop GNOME.
  - KDE — Seleziona l'ambiente del desktop KDE.

- DISPLAYMANAGER="<*value*>", dove "<*value*>" può essere uno dei seguenti valori:
  - GNOME — Seleziona il GNOME Display Manager.
  - KDE — Seleziona il KDE Display Manager.
  - XDM — Seleziona X Display Manager.

Per maggiori infomazioni consultate Capitolo 7.

4.1.8. `/etc/sysconfig/devlabel`

`/etc/sysconfig/devlabel` è il file di configurazione di `devlabel`. Non deve essere modificato manualmente, ma configurato usando il comando `/sbin/devlabel`.

Per informazioni sull'uso del comando `devlabel`, consultare il capitolo *Nomi del dispositivo definiti dall'utente* nella *Red Hat Enterprise Linux System Administration Guide*.

4.1.9. `/etc/sysconfig/dhcpd`

Il file `/etc/sysconfig/dhcpd` serve ad inviare argomenti al demone `dhcpd` durante l'avvio. Il demone `dhcpd` implementa i protocolli (DHCP) Dynamic Host Configuration Protocol e (BOOTP) il protocollo Internet Bootstrap. DHCP e BOOTP assegnano i nomi host alle macchine presenti in rete. Per maggiori informazioni su quali parametri potete utilizzare in questo file, consultate la pagina man `dhcpd`.

4.1.10. `/etc/sysconfig/exim`

Il file `/etc/sysconfig/exim` consente di inviare messaggi a uno o più client, indirizzando il messaggio sulla rete necessaria. Il file imposta i valori di default per eseguire exim. I valori di default vengono impostati in modo da essere eseguiti come un demone in background e ne controllano la coda di attesa ogni ora, nel caso in cui qualche messaggio sia stato ritornato.

I valori includono:

- `DAEMON=`<*value*>, dove <*value*> è uno dei seguenti:
  - `yes` — exim può essere configurato per l'ascolto della mail in arrivo sulla porta 25. `yes` implica l'uso delle opzioni `-bd` di Exim.
  - `no` — exim non dovrebbe essere configurato per l'ascolto delle mail in arrivo sulla porta 25.

- `QUEUE=1h` viene trasmesso a exim come `-q$QUEUE`. L'opzione `-q` non viene trasmessa a exim se esiste `/etc/sysconfig/exim`, e `QUEUE` risulta essere vuota o non definita.

4.1.11. `/etc/sysconfig/firstboot`

Al primo avvio del sistema, il programma `/sbin/init` chiama lo script `etc/rc.d/init.d/firstboot` che a sua volta lancia l'applicazione **Agent Setup**. Questa applicazione consente all'utente di installare gli ultimi aggiornamenti e ulteriori applicazioni e documentazioni.

Il file `/etc/sysconfig/firstboot` indica all'applicazione **Agent Setup** di non effettuare successivi riavvii. Per eseguirla la volta successiva che il sistema si riavvia rimuovete semplicemente `/etc/sysconfig/firstboot` ed eseguite `chkconfig --level 5 firstboot on`.

4.1.12. /etc/sysconfig/gpm

Il file /etc/sysconfig/gpm serve ad inviare gli argomenti al demone gpm durante l'avvio. Il demone gpm è il mouse server che permette l'accelerazione del mouse e la pressione del tasto centrale. Per maggiori informazioni su quali parametri potete utilizzare in questo file, consultate la pagina man digpm. Per default, la direttiva DEVICE, viene impostata su /dev/input/mice.

4.1.13. /etc/sysconfig/harddisks

Il file /etc/sysconfig/harddisks vi consente di regolare il disco fisso. L'amministratore può anche utilizzare il file /etc/sysconfig/hardiskhd[a-h] per impostare i parametri per driver specifici.

Avvertenza

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

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

- USE_DMA=1, impostando il valore 1 viene abilitato il DMA. Tuttavia, con alcuni chipset e combinazioni del disco fisso, il DMA può provocare il danneggiamento dei dati. *Prima di abilitare questa opzione, controllate la documentazione del disco fisso oppure con il rivenditore.* Per default, questa entry non è commentata, e quindi risulta essere disabilitata.
- Multiple_IO=16: se impostato su 16 abilita diversi settori per ogni interruzione di I/O. Se abilitata, questa caratteristica riduce del 30-50% l'overhead del sistema operativo. *Utilizzare con cautela.* Per default, questa entry non è commentata, e quindi non risulta essere abilitata.
- EIDE_32BIT=3: abilita il supporto (E)IDE 32-bit I/O per una scheda dell'interfaccia. Per default, questa entry non è commentata, e quindi risulta essere disabilitata.
- LOOKAHEAD=1 abilita il read-lookahead sull'unità. Per default questa entry non è commentata, e quindi risulta essere disabilitata.
- EXTRA_PARAMS=specifica dove si possono aggiungere altri parametri. Per default non risultano esserevi altri parametri.

4.1.14. /etc/sysconfig/hwconf

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

4.1.15. /etc/sysconfig/i18n

Il file /etc/sysconfig/i18n imposta la lingua di default, qualunque lingua supportata, e il font predefinito del sistema. Per esempio:

```
LANG="en_US.UTF-8"
SUPPORTED="en_US.UTF-8:en_US:en"
SYSFONT="latarcyrheb-sun16"
```

4.1.16. `/etc/sysconfig/init`

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

Possono essere utilizzati i valori seguenti:

- `BOOTUP=<valore>`, dove `<valore>`può essere sostituito con uno dei seguenti valori:
  - `color` — Richiama una schermata standard di avvio a colori, in cui il successo o il fallimento dei dispositivi e dei servizi è visualizzato con colori diversi.
  - `verbose` — Richiama una schermata con stile antiquato, che visualizza soprattutto informazioni piuttosto che messaggi di successo o fallimento.
  - Qualsiasi altro elemento richiama una schermata nuova, ma senza formattazione ANSI.

- `RES_COL=<valore>`, dove `<valore>` è il numero di colonne della schermata dove vengono avviati i label riguardanti lo stato. Il default è 60.
- `MOVE_TO_COL=<valore>`, dove `<valore>` muove il cursore alla riga `RES_COL`. Per default vengono utilizzate le sequenze ANSI visualizzate tramite il comando `echo -en`.
- `SETCOLOR_SUCCESS=<valore>`, dove `<valore>` determina il colore per la visualizzazione di una operazione che abbia avuto successo tramite il comando `echo -en`. Il colore impostato è il verde.
- `SETCOLOR_FAILURE=<valore>`, dove `<valore>` determina il colore per la visualizzazione di una operazione che abbia avuto esito negativo,tramite il comando `echo -en`. Il colore impostato è il giallo.
- `SETCOLOR_WARNING=<valore>`, dove `<valore>` determina il colore per la visualizzazione di un avvertimento tramite il comando `echo -en`. Il colore impostato è il giallo.
- `SETCOLOR_NORMAL=<valore>`, dove `<valore>` imposta il colore al valore "normale" tramite il comando `echo -en`.
- `LOGLEVEL=<valore>`, dove `<valore>` indica il livello di registrazione per il kernel della console iniziale. Il livello di default è 3; mentre 8 significa tutto (incluso il debugging), mentre 1 significa solo kernel panic. Il demone `syslogd` sovrascrive questa impostazione una volta avviato.
- `PROMPT=<valore>`, dove `<valore>` può essere sostituito con uno dei seguenti valori boolean:
  - `yes` — abilita il controllo della chiave per la modalità interattiva.
  - `no` — disabilita il controllo della chiave per la modalità interattiva.

4.1.17. `/etc/sysconfig/ip6tables-config`

Il file `/etc/sysconfig/ip6tables-config` contiene informazioni speciali utilizzate dal kernel, per impostare il filtraggio del pacchetto IPv6 in fase di avvio, o ogni qualvolta che il servizio `ip6tables` viene avviato.

Non modificate questo file manualmente se non sapete come creare le regole `ip6tables`. Se desiderate, potete creare manualmente le regole mediante `/sbin/ip6tables`. Una volta create, aggiungere le regole al file `/etc/sysconfig/ip6tables`, digitando il seguente comando:

```
/sbin/service ip6tables save
```

Una volta creato questo file, tutte le regole dei firewall salvate in questo contesto continueranno a esistere dopo il riavvio del sistema.

Per ulteriori informazioni su ip6tables consultate Capitolo 18.

4.1.18. /etc/sysconfig/iptables-config

Il file /etc/sysconfig/iptables-config contiene le informazioni utilizzate dal kernel per impostare i servizi di filtraggio dei pacchetti al momento dell'avvio, oppure ogni qualvolta il servizio viene avviato.

Non modificare questo file manualmente se non siete avvezzi all'uso di metodologie per creare le regole di iptables. Il modo più semplice per aggiungere delle regole, è quello di utilizzare l'applicazione **Strumento di configurazione del livello di sicurezza** (system-config-securitylevel), per creare un firewall. Mediante queste applicazioni il file verrà automaticamente modificato alla fine del processo.

Se lo desiderate, potete creare manualmente delle regole mediante /sbin/iptables. Una volta create, aggiungere le regole al file /etc/sysconfig/iptables, digitando il seguente comando:

```
/sbin/service iptables save
```

Una volta creato questo file, tutte le regole dei firewall salvate in questo contesto continueranno a esistere dopo il riavvio del sistema.

Per ulteriori informazioni su iptables consultate Capitolo 18.

4.1.19. /etc/sysconfig/irda

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

Possono essere utilizzati i valori seguenti:

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

- DEVICE=<*valore*>, dove <*valore*> è il dispositivo (di solito una porta seriale), che gestisce le connessioni a infrarossi. Un esempio di dispositivo seriale potrebbe essere /dev/ttyS2.
- DONGLE=<*valore*>, dove <*valore*> specifica il tipo di dongle utilizzato per la comunicazione a infrarossi. Questa impostazione esiste per le persone che utilizzano dongle seriali piuttosto che vere porte a infrarossi. Un dongle è un dispositivo che, collegato a una porta seriale tradizionale, permette di comunicare tramite infrarossi. Questa riga è commentata per default, perché i portatili con porte a infrarossi, sono molto più diffusi di quelli con dongle aggiunti. Un esempio di entry dongle potrebbe essere actisys+.
- DISCOVERY=<*valore*>, dove <*valore*> può essere sostituito con uno dei seguenti valori:
  - yes — Avvia irattach nella modalità discovery, ciò significa che vengono controllati altri dispositivi a infrarossi. È necessario attivare questo comando per cercare un collegamento a infrarossi (altrimenti non viene inizializzata la connessione).
  - no — non avvia irattach nella modalità Discovery.

4.1.20. /etc/sysconfig/keyboard

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

- KEYBOARDTYPE="sun|pc", dove sun indica che una tastiera Sun è collegata a /dev/kbd, o pc indica che una tastiera PS/2 è collegata ad una porta PS/2.
- KEYTABLE="<*file*>", dove <*file*> rappresenta il nome di un file keytable.

  Per esempio, KEYTABLE="us". I file che possono essere utilizzati come keytable partono da /usr/lib/kbd/keymaps/i386 e da qui si suddividono in differenti layout della tastiera, tutti etichettati come <*file*>.kmap.gz. Viene usato il primo file individuato in /usr/lib/kbd/keymaps/i386 che coincide con le impostazioni di KEYTABLE.

4.1.21. /etc/sysconfig/kudzu

Il file /etc/sysconfig/kuzdu consente all'avvio un controllo sicuro del vostro hardware tramite kudzu. Per "controllo sicuro" si intende un controllo in grado di disattivare il controllo della porta seriale.

- SAFE=<*valore*>, dove <*valore*> può essere sostituito con uno dei seguenti valori:
  - yes — kuzdu esegue un controllo sicuro.
  - no — kuzdu esegue un controllo normale.

4.1.22. /etc/sysconfig/mouse

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

- FULLNAME="<*valore*>", dove "<*valore*>" si riferisce al nome completo del tipo di mouse utilizzato.
- MOUSETYPE="<*valore*>", dove "<*valore*>" può avere uno dei seguenti valori:
  - imps2 — Un mouse a ruota USB generico.
  - microsoft — un mounse Microsoft™.
  - mouseman — un mouse MouseMan™.
  - mousesystems — un mouse Mouse Systems™.
  - ps/2 — un mouse PS/2.
  - msbm — un mouse bus Microsoft™.
  - logibm — un mouse bus Logitech™.
  - atibm — un mouse bus ATI™.
  - logitech — un mouse Logitech™.
  - mmseries — un mouse MouseMan™ datato.
  - mmhittab — un mouse mmhittab.

- XEMU3="<*valore*>", dove "<*valore*>" può essere uno dei seguenti valori boolean:
  - yes — Il mouse ha solo due pulsanti, ma il terzo viene emulato.
  - no — Il mouse ha già tre pulsanti.
- XMOUSETYPE="<*valore*>", dove "<*valore*>" indica il tipo di mouse utilizzato quando X è in esecuzione. Le opzioni sono le stesse di MOUSETYPE nello stesso file.
- DEVICE=<*valore*>, dove <*valore*> è il dispositivo mouse.

  Un esempio di valore, /dev/input/mice, risulta essere un link simbolico che indica il dispositivo mouse in uso.

4.1.23. /etc/sysconfig/named

Il file /etc/sysconfig/named serve ad inviare argomenti al demone named durante l'avvio. Il demone named è un server *Domain Name System* (*DNS*) che implementa la distribuzione *Berkeley Internet Name Domain* (*BIND*) versione 9. Il server presenta una tabella i cui nomi host sono associati a indirizzi IP sulla rete.

Al momento, si possono usare solo i valori seguenti:

- ROOTDIR="<*/some/where*>", dove <*/some/where*> si riferisce al percorso completo della directory di un ambiente chroot configurato sotto il quale named verrà eseguito. Tale ambiente chroot deve prima essere configurato. Digitate info chroot per sapere come farlo.
- OPTIONS="<*valore*>", dove <*valore*> è qualsiasi opzione elencata nella pagina man di named, eccetto **-t**. Al posto di **-t**, utilizzate la linea ROOTDIR.

Per maggiori informazioni sui parametri che potete utilizzare per questo file, consultate la pagina man di named. Per informazioni più dettagliate su come configurare un server BIND DNS, consultate Capitolo 12. Per default, questo file non contiene alcun parametro.

4.1.24. /etc/sysconfig/netdump

/etc/sysconfig/netdump è il file di configurazione per il servizio /etc/init.d/netdump. Il servizio netdump invia dati oops e dump di memoria attraverso la rete. In generale, netdump non è indispensabile, dunque, a meno che non sia strettamente necessario, non dovreste utilizzarlo. Per maggiori informazioni su quali parametri potete usare nel file, consultate la pagina man netdump.

4.1.25. /etc/sysconfig/network

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

- NETWORKING=<*valore*>, dove <*valore*> può essere sostituito con uno dei seguenti valori:
  - yes — la rete deve essere configurata.
  - no — la rete non deve essere configurata.
- HOSTNAME=<*valore*>, dove <*valore*> dovrebbe essere sostituito dall'*FQDN* (*Fully Qualified Domain Name*), per esempio hostname.domain.com, ma può anche essere un nome host di vostra scelta.

Nota bene

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

- `GATEWAY=`<*valore*>, dove <*valore*> rappresenta l'indirizzo IP del gateway della rete.
- `GATEWAYDEV=`<*valore*>, dove <*valore*> rappresenta il dispositivo per accedere al gateway, per esempio `eth0`.
- `NISDOMAIN=`<*valore*>, dove <*valore*> rappresenta il nome del dominio NIS.

4.1.26. `/etc/sysconfig/ntpd`

Il file `/etc/sysconfig/ntpd` serve ad inviare argomenti al demone `ntpd` durante l'avvio. Il demone `ntpd` imposta e gestisce l'orologio di sistema in modo da essere sincronizzato con un time server standard di Internet. Implementa la versione 4 del protocollo (NTP) Network Time Protocol. Per maggiori informazioni su quali parametri potete utilizzare in questo file, utilizzate un Web browser per visualizzare il seguente file: `/usr/share/doc/ntp-`<*version*>`/ntpd.htm` (dove <*version*> è il numero della versione di `ntpd`). Per default, questo file imposta il proprietario del processo `ntpd` come utente `ntp`.

4.1.27. `/etc/sysconfig/pcmcia`

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

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

- `PCIC=`<*valore*>, dove <*valore*> può essere sostituito con uno dei seguenti valori:
  - `i82365` — il computer ha un chipset socket PCMCIA di tipo i82365.
  - `tcic` — Il computer ha un chipset socket PCMCIA di tipo tcic.

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

4.1.28. `/etc/sysconfig/radvd`

Il file `/etc/sysconfig/radvd` serve per inviare argomenti al demone `radvd` durante l'avvio. Il demone `radvd` resta in ascolto per le richieste del router, inviando gli avvisi del router stesso sotto forma di versione 6 del protocollo IP. Questo servizio consente agli host di una rete di cambiare in modo dinamico i propri router predefiniti sulla base di tali messaggi. Per maggiori informazioni su

quali parametri potete utilizzare in questo file, consultate la pagina man diradvd. Per default, questo file imposta il proprietario del processo radvd per l'utente radvd.

4.1.29. /etc/sysconfig/rawdevices

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

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

4.1.30. /etc/sysconfig/samba

Il file /etc/sysconfig/samba serve per inviare argomenti ai demoni smbd e nmbd durante l'avvio. Il demone smbd fornisce una connettività per il file sharing ai client Windows presenti nella rete. Il demone nmbd fornisce NetBIOS tramite servizi di denominazione IP. Per maggiori informazioni su quali parametri potete utilizzare in questo file, consultate la pagina man smbd. Per default, questo file imposta smbd e nmbd in modo da poter essere eseguiti in modalità daemon.

4.1.31. /etc/sysconfig/selinux

Il file /etc/sysconfig/selinux contiene le opzioni di configurazione di base per SELinux. Il suddetto file risulta essere un link simbolico per /etc/selinux/config. Per maggiori informazioni su SELinux, consultate Capitolo 21.

4.1.32. /etc/sysconfig/sendmail

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

I valori includono:

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

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

4.1.33. /etc/sysconfig/spamassassin

Il file /etc/sysconfig/spamassassin serve per inviare argomenti al demone spamd (una versione demone di Spamassassin) al momento dell'avvio. Spamassassin è un'applicazione email per il filtro dello spam. Per un elenco delle opzioni disponibili consultate la pagina man di spamd. Per default, questo file configura spamd in modo da essere eseguito in modalità demone, crea preferenze per utenti e crea automaticamente gli elenchi whitelists (vengono abilitati numerosi mittenti).

Per maggiori infomazioni su Spamassassin, consultate la Sezione 11.4.2.6.

4.1.34. /etc/sysconfig/squid

Il file /etc/sysconfig/squid serve per inviare argomenti al demone squid durante l'avvio. Il demone è un server proxy per applicazioni Web client. Per maggiori informazioni su come configurare un server proxy squid, utilizzate un browser Web per aprire la directory /usr/share/doc/squid-<*versione*>/ (dove <*versione*> va sostituito con il numero di versione di squid installato sul sistema). Per default, questo file imposta squid in modo che si avvii in modalità daemon e stabilisce la quantità di tempo che trascorre prima che esso si arresti.

4.1.35. /etc/sysconfig/system-config-securitylevel

Il file /etc/sysconfig/system-config-securitylevel contiene tutte le opzioni scelte dall'utente l'ultima volta che lo**Strumento di configurazione del livello di sicurezza**(system-config-securitylevel) è stato eseguito. Gli utenti non dovrebbero modificare questo file manualmente. Per maggiori infomazioni su **Strumento di configurazione del livello di sicurezza**, consultate il capitolo inititolato *Configurazione di Base del Firewall* nella *Red Hat Enterprise Linux System Administration Guide*.

4.1.36. /etc/sysconfig/system-config-users

/etc/sysconfig/system-config-users è il file di configurazione dell'applicazione grafica, **Utente Manager**. Questo file viene usato solo per filtrare gli utenti del sistema come root, daemon, o lp. Questo file può essere modificato tramite il menu a tendina **Preferenze => Filtra utenti e gruppi di sistema** nell'applicazione **Utente Manager**, e non deve essere modificato manualmente. Per maggiori informazioni su come utilizzare tale applicazione, consultate il capitolo intitolato *Configurazione di utenti e gruppi* all'interno della *Red Hat Enterprise Linux System Administration Guide*.

4.1.37. /etc/sysconfig/system-logviewer

/etc/sysconfig/system-logviewer è il file di configurazione per l'applicazione grafica di visualizzazione dei log interattivi **Log Viewer**. Questo file può essere modificato tramite il menu a tendina **Modifca => Preferenze** dell'applicazione **Log Viewer** e non deve essere modificato manualmente. Per ulteriori informazioni sull'utilizzo di questa applicazione, consultate il capitolo *Log Files* nella *Red Hat Enterprise Linux System Administration Guide*.

4.1.38. /etc/sysconfig/tux

/etc/sysconfig/tux è il file di configurazione per il Web server Red Hat Content Accelerator basato sul kernel (in precedenza noto come TUX). Per maggiori informazioni su come configurare il Red Hat Content Accelerator, utilizzate un Web browser per aprire /usr/share/doc/tux-<*versione*>/tux/index.html (sostituire <*versione*> con il numero di versione di TUX installato sul sistema). I parametri disponibili per questo file sono elencati in /usr/share/doc/tux-<*versione*>/tux/parameters.html.

4.1.39. /etc/sysconfig/vncservers

Il file /etc/sysconfig/vncservers configura l'avvio del server *VNC* (*Virtual Network Computing*).

VNC è un sistema di visualizzazione remoto che consente di mostrare un ambiente desktop non solo sull'elaboratore dove è in esecuzione ma anche su reti diverse (da una LAN a Internet), utilizzando una vasta gamma di architetture.

Potrebbe contenere:

- VNCSERVERS=<*valore*>, dove <*valore*> è impostato come "1:fred", per indicare che un server VNC deve essere avviato dall'utente fred per il display :1. L'utente fred deve aver impostato una password VNC utilizzando il comando vncpasswd prima di collegarsi al server VNC remoto.

Quando utilizzate un server VNC, le comunicazioni non sono criptate e perciò il server VNC non deve essere utilizzato su di una rete non sicura. Per istruzioni particolari riguardanti l'uso di SSH per rendere le comunicazioni VNC sicure, consultate le informazioni all'indirizzo http://www.uk.research.att.com/archive/vnc/sshvnc.html.Per saperne di più su SSH, consultare Capitolo 20 nella *Red Hat Enterprise Linux System Administration Guide*.

4.1.40. /etc/sysconfig/xinetd

Il file /etc/sysconfig/xinetd serve per inviare argomenti al demone xinetd al momento dell'avvio. Il demone xinetd avvia programmi che forniscono servizi Internet quando viene ricevuta una richiesta sulla porta per quel servizio. Per maggiori informazioni su quali parametri potete utilizzare in questo file consultate la pagina man di xinetd. Per informazioni sul servizio xinetd, consultate la Sezione 17.3.

4.2. Directory presenti all'interno della directory /etc/sysconfig/

Le seguenti directory si trovano normalmente in /etc/sysconfig/.

- apm-scripts — Questa directory contiene lo script di sospensione/ripristino APM. Non modificate questo file direttamente. Se avete esigenza di personalizzarlo, create semplicemente un file denominato /etc/sysconfig/apm-scripts/apmcontinue e verrà richiamato in fondo allo script. Potete anche controllare lo script modificando /etc/sysconfig/apmd.
- cbq — Questa directory contiene i file di configurazione necessari per effettuare il *Class Based Queuing* per la gestione della larghezza di banda sulle interfacce di rete. CBQ divide il traffico dell'utente in una gerarchia di diverse classi basate su qualsiasi combinazione di indirizzi IP, protocolli, e di tipi di applicazione.
- networking/ — Questa directory è utilizzata dallo **Strumento di amministrazione di rete** (system-config-network), e non è consigliabile modificare i suoi contenuti manualmente. Per sapere come configurare le interfacce di rete tramite lo **Strumento di amministrazione di rete**, consultate il capitolo intitolato *Configurazione della rete* nella *Red Hat Enterprise Linux System Administration Guide*.
- network-scripts — contiene i seguenti file di configurazione relativi alla rete:
  - File di configurazione della rete per ogni interfaccia di rete configurata (per esempio il file ifcfg-eth0 per l'interfaccia Ethernet eth0.
  - Script utilizzati per attivare e disattivare le interfacce di rete, come ifup e ifdown.
  - Script utilizzati per attivare e disattivare le interfacce ISDN, come ifup-isdn e ifdown-isdn
  - Vari script condivisi di funzione di rete che non devono essere modificati manualmente.

  Per maggiori informazioni sulla directory network-scripts, consultate il Capitolo 8.
- rhn/ — Contiene i file di configurazione e le chiavi GPG per Red Hat Network. Nessuno dei file contenuti in questa directory deve essere modificato manualmente. Per maggiori informazioni su Red Hat Network, consultate il relativo sito web di Red Hat Network all'indirizzo https://rhn.redhat.com/.

4.3. Risorse Addizionali

Questo capitolo è solo inteso come una introduzione ai file nella directory `/etc/sysconfig/`. Per informazioni più complete consultate quanto segue.

4.3.1. Documentazione Installata

- `/usr/share/doc/initscripts-<numero-versione>/sysconfig.txt` — Questo file contiene un elenco più autorevole dei file trovati nella directory `/etc/sysconfig/` e le opzioni a loro disponibili. Il *<numero-versione>* nel percorso per questo file corrisponde alla versione del pacchetto `initscripts` installato.

Capitolo 5.

Il filesystem `proc`

Il kernel di Linux ha due funzioni principali: controllare l'accesso ai dispositivi fisici e stabilire quando e come i vari processi interagiscono con tali dispositivi. La directory `/proc/` — anche chiamata file system `proc` —contiene una gerarchia di file speciali che rappresentano lo stato corrente del kernel — consentendo alle applicazioni e agli utenti di esplorare il sistema attraverso il punto di vista del kernel.

All'interno della directory `/proc` potete trovare numerose informazioni sull'hardware e su qualsiasi processo attualmente in esecuzione. Inoltre alcuni file all'interno dell'albero delladirectory `/proc` possono essere manipolati dagli utenti e dalle applicazioni per comunicare al kernel eventuali modifiche di configurazione.

5.1. Un filesystem virtuale

In Linux tutto viene memorizzato sotto forma di file. La maggior parte degli utenti hanno familiarità con i due principali tipi di file, ovvero i file di testo e binari. La directory `/proc/`, tuttavia, contiene un altro tipo di file denominato *file virtuale*. Per questo motivo `/proc/` è spesso indicato come *filesystem virtuale*.

Questi file virtuali hanno qualità univoche e la maggior parte di essi ha dimensioni pari a zero byte, ma quando visualizzati, possono contenere una grande quantità di informazioni. Inoltre gran parte delle impostazioni dell'ora e della data dei file virtuali riflette la data e l'ora correnti, per indicare il continuo mutamento.

I file virtuali come `/proc/interrupts`, `/proc/meminfo`, `/proc/mounts` e `/proc/partitions` forniscono una visualizzazione corrente dell'hardware del sistema. Altri, come il file `/proc/filesystems` e la directory `/proc/sys/` forniscono informazioni sulla configurazione del sistema e le interfacce.

A scopo organizzativo i file contenenti informazioni relative a un argomento simile sono raggruppati in directory virtuali e in sottodirectory. Per esempio, `/proc/ide/` contiene informazioni per tutti i dispositivi fisici IDE. In modo simile le directory dei processi contengono informazioni su ciascun processo in esecuzione nel sistema.

5.1.1. Visualizzazione di file virtuali

Combinando i comandi `cat`, `more` o `less` sui file presenti all'interno della directory `/proc/`, utenti possono accedere immediatamente a una enorme quantità di informazioni inerenti al sistema. Per esempio, per visualizzare quale tipo di CPU è presente su di un computer, digitate `cat /proc/cpuinfo` per ricevere un output simile a quanto segue:

```
processor : 0
vendor_id : AuthenticAMD
cpu family : 5
model  : 9
model name : AMD-K6(tm) 3D+ Processor
stepping : 1
cpu MHz  : 400.919
cache size : 256 KB
fdiv_bug : no
hlt_bug  : no
f00f_bug : no
```

```
coma_bug : no
fpu  : yes
fpu_exception : yes
cpuid level : 1
wp  : yes
flags  : fpu vme de pse tsc msr mce cx8 pge mmx syscall 3dnow k6_mtrr
bogomips : 799.53
```

Quando visualizzate diversi file virtuali all'interno del filesystem `/proc`, noterete che alcune informazioni risultano immediatamente comprensibili mentre altre parti non sono leggibili. Questo è in parte il motivo per cui esistono utility specifiche, come per esempio `lspci`, `apm`, `free` e `top`, che permettono di estrarre i dati dai file virtuali e visualizzarli in modo comprensibile.

Nota Bene

Alcuni dei file virtuali contenuti nella directory `/proc` sono impostati per risultare leggibili solo all'utente root.

5.1.2. Come cambiare i file virtuali

In generale, la maggior parte dei file virtuali all'interno della directory `/proc/` sono di sola lettura. Tuttavia, è possibile utilizzare alcuni di essi operando qualche modifica nelle impostazioni del kernel. Questo vale soprattutto per i file contenuti nella sottodirectory `/proc/sys/`.

Per cambiare il valore di un file virtuale, utilizzate il comando `echo` con un simbolo (>), per ridirezionare il nuovo valore al file. Per esempio, per cambiare il vostro hostname potete digitare:

```
echo www.example.com > /proc/sys/kernel/hostname
```

Altri file si comportano come switch binari o booleani. Per esempio, digitando `cat /proc/sys/net/ipv4/ip_forward`, otterrete `0` oppure `1`. Uno `0` indica che il kernel non stà inoltrando pacchetti di rete. Utilizzando il comando `echo` per cambiare il valore del file `ip_forward` in `1`, potete abilitare immediatamente l'inoltro dei pacchetti.

Suggerimento

Un altro comando utilizzato per modificare le impostazioni della subdirectory `/proc/sys/` è `/sbin/sysctl`. Per ulteriori informazioni su questo comando, consultate la Sezione 5.4

Per un elenco di alcuni dei file di configurazione del kernel disponibili all'interno della sottodirectory `/proc/sys/`, consultate la Sezione 5.3.9.

5.2. File di livello superiore all'interno del filesystem proc

L'elenco seguente riporta alcuni dei file virtuali di livello superiore più utili contenuti nella directory `/proc/`.

Nota Bene

Nella maggior parte dei casi, il contenuto dei file elencati in questa sezione non sarà lo stesso di quelli installati sulla vostra macchina. Questo perché gran parte delle informazioni è specifica dell'hardware su cui Red Hat Enterprise Linux è in esecuzione.

5.2.1. `/proc/apm`

Questo file fornisce informazioni sullo stato del sistema*Advanced Power Management (APM)*, tali informazioni vengono poi utilizzate dal comando `apm`. Se a un alimentatore CA è collegato un sistema non alimentato a batteria, il file virtuale ha più o meno questo aspetto:

```
1.16 1.2 0x07 0x01 0xff 0x80 -1% -1 ?
```

L'esecuzione del comando `apm -v` in tale sistema dà un output simile al seguente:

```
APM BIOS 1.2 (kernel driver 1.16ac)
AC on-line, no system battery
```

Per i sistemi non alimentati a batteria, `apm` può svolgere altre operazioni oltre a quella di mettere la macchina in modalità di standby. Il comando `apm` è molto più utile per i laptop. Per esempio, l'output riportato di seguito deriva dal comando `cat /proc/apm` di un portatile collegato a una presa di corrente:

```
1.16 1.2 0x03 0x01 0x03 0x09 100% -1 ?
```

Quando lo stesso portatile non è più collegato all'alimentazione, il contenuto del file `apm` cambia in modo seguente:

```
1.16 1.2 0x03 0x00 0x00 0x01 99% 1792 min
```

Il comando `apm -v` produce informazioni più utili come quelli riportati di seguito:

```
APM BIOS 1.2 (kernel driver 1.16)
AC off-line, battery status high: 99% (1 day, 5:52)
```

5.2.2. `/proc/buddyinfo`

Questo file viene usato principalmente per diagnosticare le problematiche dovute alla frammentazione della memoria. Usando l'algoritmo buddy, ogni colonna rappresenta il numero di pagine di un certo ordine (e di una certa misura), disponibili in ogni istante. Per esempio, per la zona DMA (direct memory access), sono disponibili 90 blocchi di memoria 2^(0*PAGE_SIZE). In modo del tutto analogo, sono disponibili 6 blocchi di 2^(1*PAGE_SIZE) e 2 di 2^(2*PAGE_SIZE).

La riga `DMA` si riferisce ai primi 16 MB presenti su di un sistema, la riga `HighMem` invece si riferisce alla memoria con un valore maggiore di 4GB presente sul sistema, mentre `Normal` si riferisce alla memoria con un valore intermedio rispetto ai due precedentemente descritti.

Il seguente è un esempio di un output tipico di `/proc/buddyinfo`:

```
Node 0, zone      DMA     90      6      2      1      1      ...
Node 0, zone   Normal   1650    310      5      0      0      ...
Node 0, zone  HighMem      2      0      0      1      1      ...
```

5.2.3. /proc/cmdline

Questo file mostra i parametri trasmessi al kernel al momento dell'avvio. Un esempiodel file /proc/cmdline ha il seguente aspetto:

```
ro root=/dev/VolGroup00/LogVol00 rhgb quiet 3
```

Ciò sta ad indicare che il kernel è stato montato in modalità di sola lettura ((ro)), posizionato sul primo volume logico (LogVol00) del primo gruppo di volume (/dev/VolGroup00). LogVol00 è l'equivalente di una partizione del disco presente in un sistema non-LVM (Logical Volume Management), proprio come /dev/VolGroup00 risulta essere simile nel concetto a /dev/hda1, ma più flessibile.

Per maggiori informazioni sull'LVM utilizzato con Red Hat Enterprise Linux, consultate http://www.tldp.org/HOWTO/LVM-HOWTO/index.html.

rhgb indica l'installazione del pacchetto rhgb, e che l'avvio grafico è supportato, assumendo però che /etc/inittab sia in grado di visualizzare il runlevel di default impostato su id:5:initdefault:.

Per finire, quiet indica la soppressione di tutti i messaggi verbose del kernel al momento dell'avvio.

5.2.4. /proc/cpuinfo

Il file virtuale identifica il tipo di processore presente sul vostro sistema. Quello riportato di seguito è un esempio di output tipico derivante da /proc/cpuinfo:

```
processor : 0
vendor_id : GenuineIntel
cpu family : 15
model  : 2
model name : Intel(R) Xeon(TM) CPU 2.40GHz
stepping : 7
cpu MHz  : 2392.371
cache size : 512 KB
physical id : 0
siblings : 2
runqueue : 0
fdiv_bug : no
hlt_bug  : no
f00f_bug : no
coma_bug : no
fpu  : yes
fpu_exception : yes
cpuid level : 2
wp  : yes
flags  : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm
bogomips : 4771.02
```

- processor — Attribuisce un numero identificativo a ciascun processore. Sui sistemi che hanno un unico processore, viene visualizzato soltanto 0.
- cpu family — È in grado di identificare il tipo di processore presente nel sistema. Se si tratta di un sistema basato su un processore Intel, per determinare il valore è sufficiente anteporre il numero a "86". Questa operazione è particolarmente utile nel caso si vogliano delle informazioni sull'architettura di un vecchio sistema, come 586, 486 o 386. Poichè per determinate architetture

a volte vengono compilati alcuni pacchetti RPM, questo valore vi consente di determinare quale pacchetto installare sul sistema.

- `model name` — mostra il nome comune del processore, compreso il nome del suo progetto.
- `cpu MHz` — Mostra l'esatta velocità in megahertz di quel particolare processore nell'ordine delle migliaia.
- `cache size` — mostra la quantità di memoria della cache di livello 2 disponibile per il processore.
- `siblings` — Visualizza il numero di CPU sibling sullo stesso CPU fisico, per architetture che usano hyper-threading.
- `flags` — definisce svariate caratteristiche del processore, per esempio la presenza di una FPU (unità in virgola mobile) e la capacità di elaborare istruzioni MMX.

5.2.5. `/proc/crypto`

Questo file elenca tutte le informazioni installate riguardanti la cifratura e utilizzate dal kernel di Linux, incluso ogni singola informazione. Di seguito viene riportato un esempio di file `/proc/crypto`:

```
name         : sha1
module       : kernel
type         : digest
blocksize    : 64
digestsize   : 20

name         : md5
module       : md5
type         : digest
blocksize    : 64
digestsize   : 16
```

5.2.6. `/proc/devices`

Questo file visualizza i diversi caratteri e dispositivi a blocchi attualmente configurati (non include i dispositivi i cui moduli non sono stati caricati). Ecco riportato un esempio di output:

```
Character devices:
  1 mem
  4 /dev/vc/0
  4 tty
  4 ttyS
  5 /dev/tty
  5 /dev/console
  5 /dev/ptmx
  7 vcs
 10 misc
 13 input
 29 fb
 36 netlink
128 ptm
136 pts
180 usb

Block devices:
  1 ramdisk
  3 ide0
```

```
  9 md
 22 ide1
253 device-mapper
254 mdp
```

L'output del file `/proc/devices` comprende il numero maggiore e il nome del dispositivo ed è suddiviso in due sezioni principali: `Character devices` e `Block devices`.

I *dispositivi a carattere* sono simili ai *dispositivi a blocchi*, a eccezione di due differenze sostanziali:

1. I dispositivi a carattere non richiedono l'operazione di buffering.Mentre i dispositivi a blocco dispongono di un buffer grazie al quale possono ordinare tali richieste prima di elaborarle. Ciò si rivela alquanto utile nel caso dei dispositivi creati per immagazzinare informazioni — per esempio i dischi fissi —, poichè l'abilità di ordinare l'informazione prima che venga scritta sul dispositivo è permette poi di ordinarla in modo più efficiente.
2. I dispositivi a carattere non inviano i dati in base a una dimensione predefinita. In secondo luogo, i dispositivi a blocchi possono inviare e ricevere informazioni in blocchi di una certa dimensione, configurati a seconda del dispositivo.

Per maggiori informazioni sui dispositivi, consultate la seguente documentazione:

`/usr/share/doc/kernel-doc-<version>/Documentation/devices.txt`

5.2.7. /proc/dma

Questo file contiene un elenco dei canali DMA per il canale ISA in uso. Un esempio di file `/proc/dma` ha il seguente aspetto:

```
 4: cascade
```

5.2.8. /proc/execdomains

Il file elenca quali sono i *formati di eseguibili* attualmente supportati dal kernel di Linux e la gamma di "personalità" che essi supportano.

```
0-0   Linux            [kernel]
```

Pensate ai domini degli eseguibili, come la "personalità" di un determinato sistema operativo. Poichè altri formati binari, quali Solaris, UnixWare e FreeBSD, possono essere utilizzati con Linux, i programmatori possono modificare il modo in cui il sistema operativo gestisce le chiamate del sistema da questi binari,cambiando la personalità del compito. A eccezione del dominio eseguibile `PER_LINUX`, personalità diverse possono essere implementate come moduli caricabili dinamicamente.

5.2.9. /proc/fb

Questo file contiene un elenco di dispositivi del frame buffer, con il numero del dispositivo del frame buffer e l'unità che lo controlla. Un tipico esempio di output di `/proc/fb` per sistemi che contengono dispositivi frame buffer ha il seguente aspetto:

```
0 VESA VGA
```

5.2.10. `/proc/filesystems`

Il file visualizza un elenco dei tipi di filesystem attualmente supportati dal kernel. Un esempio di output da un file `/proc/filesystems` generico, è simile a quanto segue:

```
nodev   sysfs
nodev   rootfs
nodev   bdev
nodev   proc
nodev   sockfs
nodev   binfmt_misc
nodev   usbfs
nodev   usbdevfs
nodev   futexfs
nodev   tmpfs
nodev   pipefs
nodev   eventpollfs
nodev   devpts
        ext2
nodev   ramfs
nodev   hugetlbfs
        iso9660
nodev   mqueue
        ext3
nodev   rpc_pipefs
nodev   autofs
```

La prima colonna indica se il filesystem è stato montato su un dispositivo a blocchi; quelli che iniziano con `nodev` non sono montati su un dispositivo a blocchi. Nella seconda colonna sono elencati i nomi dei filesystem supportati.

Il comando `mount` scorre attraverso i filesystem qui riportati,quando non ne viene specificato uno come argomento.

5.2.11. `/proc/interrupts`

Questo file registra il numero di interrupt per (IRQ) su di una architettura x86. Un file standard `/proc/interrupts` ha solitamente questo aspetto:

```
           CPU0
  0:   80448940          XT-PIC  timer
  1:     174412          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          1          XT-PIC  rtc
 10:     410964          XT-PIC  eth0
 12:      60330          XT-PIC  PS/2 Mouse
 14:    1314121          XT-PIC  ide0
 15:    5195422          XT-PIC  ide1
NMI:          0
ERR:          0
```

Nel caso di macchine multiprocessore, questo file può avere un aspetto leggermente diverso:

```
           CPU0       CPU1
  0: 1366814704          0          XT-PIC  timer
  1:        128        340    IO-APIC-edge  keyboard
  2:          0          0          XT-PIC  cascade
  8:          0          1    IO-APIC-edge  rtc
```

```
 12:       5323       5793    IO-APIC-edge  PS/2 Mouse
 13:          1          0          XT-PIC  fpu
 16:   11184294   15940594   IO-APIC-level  Intel EtherExpress Pro 10/100 Ethernet
 20:    8450043   11120093   IO-APIC-level  megaraid
 30:      10432      10722   IO-APIC-level  aic7xxx
 31:         23         22   IO-APIC-level  aic7xxx
NMI:          0
ERR:          0
```

La prima colonna si riferisce al numero di IRQ. Ogni CPU presente nel sistema ha la propria colonna e il proprio numero di interrupt (IRQ). La colonna successiva indica il tipo di interrupt e l'ultima colonna contiene il nome del dispositivo interessato.

Ogni tipo di interrupt presente in questo file, i quali sono specifici a seconda dell'architettura, ha un significato leggermente diverso. Per le macchine x86, sono comuni i seguenti valori:

- `XT-PIC` — gli interrupt del vecchio computer AT.
- `IO-APIC-edge` — il segnale di voltaggio su questo interrupt è in transizione dal basso verso l'alto, creando così un *margine* dove si verifica l'interrupt, ed è segnalato una sola volta. Questo tipo di interrupt, così come l'interrupt `IO-APIC-level`, è possibile solo su sistemi con processori della famiglia 586 e successivi.
- `IO-APIC-level` — Genera degli interrupt con l'aumentare del suo segnale di voltaggio, fino a quando lo stesso segnale non diminuisce il suo valore.

5.2.12. `/proc/iomem`

Il file mostra la mappa corrente della memoria del sistema per i vari dispositivi:

```
00000000-0009fbff : System RAM
0009fc00-0009ffff : reserved
000a0000-000bffff : Video RAM area
000c0000-000c7fff : Video ROM
000f0000-000fffff : System ROM
00100000-07ffffff : System RAM
  00100000-00291ba8 : Kernel code
  00291ba9-002e09cb : Kernel data
e0000000-e3ffffff : VIA Technologies, Inc. VT82C597 [Apollo VP3]
e4000000-e7ffffff : PCI Bus #01
  e4000000-e4003fff : Matrox Graphics, Inc. MGA G200 AGP
  e5000000-e57fffff : Matrox Graphics, Inc. MGA G200 AGP
e8000000-e8ffffff : PCI Bus #01
  e8000000-e8ffffff : Matrox Graphics, Inc. MGA G200 AGP
ea000000-ea00007f : Digital Equipment Corporation DECchip 21140 [FasterNet]
  ea000000-ea00007f : tulip
ffff0000-ffffffff : reserved
```

Nella prima colonna sono visualizzati i registri di memoria usati da ogni tipo di memoria. La seconda colonna indica il tipo di memoria presente all'interno di tali registri e visualizza persino quali registri di memoria sono usati dal kernel all'interno della RAM del sistema o, se il network interface card possiede porte Ethernet multiple, e i registri di memoria assegnati per ogni porta.

5.2.13. `/proc/ioports`

L'output di `/proc/ioports` fornisce un elenco della porta registrata che viene utilizzata per comunicazioni in ingresso o in uscita con un dispositivo. Questo file può essere piuttosto lungo. Il seguente risulta essere un elenco parziale:

```
0000-001f : dma1
0020-003f : pic1
0040-005f : timer
0060-006f : keyboard
0070-007f : rtc
0080-008f : dma page reg
00a0-00bf : pic2
00c0-00df : dma2
00f0-00ff : fpu
0170-0177 : ide1
01f0-01f7 : ide0
02f8-02ff : serial(auto)
0376-0376 : ide1
03c0-03df : vga+
03f6-03f6 : ide0
03f8-03ff : serial(auto)
0cf8-0cff : PCI conf1
d000-dfff : PCI Bus #01
e000-e00f : VIA Technologies, Inc. Bus Master IDE
  e000-e007 : ide0
  e008-e00f : ide1
e800-e87f : Digital Equipment Corporation DECchip 21140 [FasterNet]
  e800-e87f : tulip
```

La prima colonna indica l'effettiva gamma dell'indirizzo della porta I/O riservato al dispositivo presente nell'elenco della seconda colonna.

5.2.14. `/proc/kcore`

Il file rappresenta la memoria fisica del sistema ed è memorizzato in formato file core. A differenza di molti file `/proc/`, `kcore` visualizza la dimensione. Questo valore viene fornito in byte ed equivale alla dimensione della memoria fisica (RAM) usata più 4 KB.

Il contenuto di questo file è progettato per essere esaminato da un debbuger, come `gdb` e non è leggibile.

Attenzione

Non cercate di visualizzare il file virtuale `/proc/kcore`. I contenuti del file altereranno l'output di testo sul terminale. Se vi dovesse capitare per errore di visualizzare il file, premete [Ctrl]-[C] per arrestare il processo e digitate poi `reset` per tornare a visualizzare il prompt della linea di comando.

5.2.15. `/proc/kmsg`

Il file è utilizzato per contenere messaggi generati dal kernel. Tali messaggi vengono poi raccolti da altri programmi, come per esempio `/sbin/klogd` o `/bin/dmesg`.

5.2.16. /proc/loadavg

Questo file permette di dare uno sguardo al carico medio del processore riguardante la CPU e IO nel tempo, e fornisce altresì dati aggiuntivi utilizzati da uptime e da altri comandi. Un esempio di file /proc/loadavg sarà simile al seguente:

```
0.20 0.18 0.12 1/80 11206
```

Le prime tre colonne misurano il grado di utilizzo della CPU e IO nei periodi da uno, cinque e 10 minuti. La quarta colonna mostra il numero di processi attualmente in esecuzione e il numero totale dei processi. L'ultima colonna visualizza l'ultimo ID usato.

5.2.17. /proc/locks

Questo file visualizza i file attualmente bloccati dal kernel. I contenuti di questo file presentano dati interni di debugging del kernel, e possono variare sensibilmente a seconda dell'uso del sistema. Un file tipico /proc/locks di un sistema con carico al minimo ha questo aspetto:

```
1: POSIX  ADVISORY  WRITE 3568 fd:00:2531452 0 EOF
2: FLOCK  ADVISORY  WRITE 3517 fd:00:2531448 0 EOF
3: POSIX  ADVISORY  WRITE 3452 fd:00:2531442 0 EOF
4: POSIX  ADVISORY  WRITE 3443 fd:00:2531440 0 EOF
5: POSIX  ADVISORY  WRITE 3326 fd:00:2531430 0 EOF
6: POSIX  ADVISORY  WRITE 3175 fd:00:2531425 0 EOF
7: POSIX  ADVISORY  WRITE 3056 fd:00:2548663 0 EOF
```

A ciascun blocco viene attribuito un numero, posto all'inizio di ogni linea. La seconda colonna si riferisce alla classe di blocco utilizzata: FLOCK indica che il file è stato bloccato, secondo il vecchio stile UNIX, da una chiamata di sistema flock, mentre POSIX rappresenta il nuovo sistema di bloccaggio POSIX, che si serve della chiamata di sistema lockf.

La terza colonna può avere due valori: ADVISORY o MANDATORY. ADVISORYindica che il blocco non impedisce ad altre persone di accedere ai dati; si limita ad impedire altri tentativi di bloccare gli stessi. MANDATORY segnala che non sono permessi altri accessi ai dati mentre il blocco è attivo. La quarta colonna indica se il blocco concede o meno al proprietario (holder) l'accesso READ o WRITE al file. La quinta colonna mostra l'ID del processo che detiene il blocco. La sesta colonna mostra l'ID del file che viene bloccato nel seguente formato: *MAJOR-DEVICE*: *MINOR-DEVICE*:*INODE-NUMBER*. La settima e l'ottava colonna indicano dove inizia e finisce l'area del file bloccato.

5.2.18. /proc/mdstat

Questo file contiene l'informazione corrente per la configurazioni di dischi multipli (RAID). Se il sistema non dispone di tale configurazione, allora /proc/mdstat avrà il seguente aspetto:

```
Personalities :
read_ahead not set
unused devices: <none>
```

Il file rimane nella stessa condizione come visto precedente finché non esiste un RAID software o un dispositivo md. In tal caso, potete usare /proc/mdstat per farvi un'idea dell'attuale situazione dei vostri dispositivi RAID md*X*.

Il file /proc/mdstat mostra un sistema che presenta md0 configurato come dispositivo RAID 1. Al momento sta risincronizzando i dischi:

```
Personalities : [linear] [raid1]
read_ahead 1024 sectors
```

```
md0: active raid1 sda2[1] sdb2[0] 9940 blocks [2/2] [UU] resync=1% finish=12.3min
algorithm 2 [3/3] [UUU]
unused devices: <none>
```

5.2.19. `/proc/meminfo`

Questo è uno dei file nella directory `/proc` più comunemente usati: riporta, infatti, una grande quantità di informazioni preziose in merito all'attuale utilizzo della RAM nel sistema.

Un sistema con 256 MB di RAM e 512 MB di spazio swap potrebbe presentare un file `/proc/meminfo` simile a questo:

```
MemTotal:       255908 kB
MemFree:         69936 kB
Buffers:         15812 kB
Cached:         115124 kB
SwapCached:          0 kB
Active:          92700 kB
Inactive:        63792 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       255908 kB
LowFree:         69936 kB
SwapTotal:      524280 kB
SwapFree:       524280 kB
Dirty:               4 kB
Writeback:           0 kB
Mapped:          42236 kB
Slab:            25912 kB
Committed_AS:   118680 kB
PageTables:       1236 kB
VmallocTotal:  3874808 kB
VmallocUsed:      1416 kB
VmallocChunk:  3872908 kB
HugePages_Total:     0
HugePages_Free:      0
Hugepagesize:     4096 kB
```

Molte delle informazioni qui riportate sono utilizzate dai comandi `free`, `top` e `ps`. A dire il vero, l'output del comando `free` ha un aspetto simile ai contenuti e alla struttura di `/proc/meminfo`. Guardando direttamente `/proc/meminfo`, si possono osservare ulteriori dettagli:

- `MemTotal` — quantità totale di RAM fisica, misurata in kilobyte.
- `MemFree` — quantità di RAM fisica, misurata in kilobyte, ancora inutilizzata dal sistema.
- `Buffers` — quantità di RAM fisica, misurata in kilobyte, utilizzata per i buffer dei file.
- `Cached` — quantità di RAM fisica, misurata in kilobyte, utilizzata come memoria cache.
- `SwapCached` — La quantità di swap misurata in kilobyte, utilizzata come memoria cache.
- `Active` — Risulta essere la quantità totale di memoria cache buffer o della pagina, misurata in kilobyte ed impiegata attivamente. Esso rappresenta la quantità di memoria utilizzata recentemente, e non impiegata per altri scopi.
- `Inactive` — Risulta essere la quantità totale di memoria cache buffer o della pagina, misurata in kilobyte e disponibile all'uso. Esso rappresenta la quantità di memoria non recentemente utilizzata, ed in grado di essere impiegata per altri scopi.

- `HighTotal` e `HighFree` — quantità di memoria totale e rimanente, in kilobyte, che non è mappata direttamente allo spazio del kernel. Il valore `HighTotal` può variare a seconda del tipo di kernel utilizzato.
- `LowTotal` e `LowFree` — quantità di memoria totale e rimanente, in kilobyte, mappata direttamente allo spazio del kernel. Il valore `LowTotal` può variare a seconda del tipo di kernel utilizzato.
- `SwapTotal` — quantità totale di spazio di swap disponibile, misurata in kilobyte.
- `SwapFree` — quantità totale di spazio di swap rimanente, misurata in kilobyte.
- `Dirty` — La quantità totale di memoria misurata in kilobyte, in attesa di essere riscritta su disco.
- `Writeback` — La quantità totale di memoria misurata in kilobyte, riscritta attivamente sul disco.
- `Writeback` — La quantità totale di memoria misurata in kilobyte, impiegata per mappare i dispositivi, i file o le librerie utilizzando il comando `mmap`.
- `Slab` — La quantità di memoria misurata in kilobyte, utilizzata dal kernel, per conservare i dati sulla struttura riguardanti il proprio utilizzo.
- `Committed_AS` — La quantità totale di memoria misurata in kilobyte, stimata per completare il carico di lavoro. Questo valore rappresenta l'ipotesi peggiore, ed include il valore della memoria di swap.
- `PageTables` — La quantità totale di memoria misurata in kilobyte, dedicata al livello più basso della tabella della pagina.
- `VMallocTotal` — La quantità totale di memoria misurata in kilobyte, per lo spazio totale allocato all'indirizzo virtuale.
- `VMallocUsed` — La quantità totale di memoria misurata in kilobyte, riguardante lo spazio usato dell'indirizzo virtuale.
- `VMallocChunk` — Il blocco di memoria adiacente più grande, misurato in kilobyte, dello spazio disponibile dell'indirizzo virtuale.
- `HugePages_Total` — Il numero totale di hugepage per il sistema. Il numero è ottenuto dividendo `Hugepagesize` per i megabyte impostati separatamente per le hugepage specificate in `/proc/sys/vm/hugetlb_pool`. *Questa statistica appare solo sulle architetture x86, Itanium, e AMD64.*
- `HugePages_Free` — Il numero totale di hugepage disponibili per il sistema. *Questa statistica appare solo sulle architetture x86, Itanium, e AMD64.*
- `Hugepagesize` — La misura per ogni unità hugepage in kilobyte. Per default, il valore è 4096 KB su kernel di tipo uniprocessor per architetture a 32 bit. Per SMP e kernel hugemem e AMD64, il default è 2048 KB. Per architetture Itanium il default è 262144 KB. *Questa statistica appare solo sulle architetture x86, Itanium, e AMD64.*

5.2.20. `/proc/misc`

Il file elenca driver misti registrati sul dispositivo principale, il cui numero è 10:

```
 63 device-mapper
175 agpgart
135 rtc
134 apm_bios
```

La prima colonna indica il numero minore di ciascun dispositivo, mentre la seconda colonna mostra il driver in uso.

5.2.21. `/proc/modules`

Questo file mostra un elenco di tutti i moduli che sono stati caricati nel kernel. Il suoi contenuti variano a seconda della configurazione e dell'uso del vostro sistema, ma dovrebbe essere organizzato in modo analogo all'output delfile `/proc/modules` di questo esempio:

Nota Bene

Questo esempio è stato riformattato in un formato leggibile. La maggior parte di queste informazioni possono essere visualizzate tramite il comando `/sbin/lsmod`.

```
nfs      170109  0 -          Live 0x129b0000
lockd    51593   1 nfs,       Live 0x128b0000
nls_utf8 1729    0 -          Live 0x12830000
vfat     12097   0 -          Live 0x12823000
fat      38881   1 vfat,      Live 0x1287b000
autofs4  20293   2 -          Live 0x1284f000
sunrpc   140453  3 nfs,lockd, Live 0x12954000
3c59x    33257   0 -          Live 0x12871000
uhci_hcd 28377   0 -          Live 0x12869000
md5      3777    1 -          Live 0x1282c000
ipv6     211845 16 -          Live 0x128de000
ext3     92585   2 -          Live 0x12886000
jbd      65625   1 ext3,      Live 0x12857000
dm_mod   46677   3 -          Live 0x12833000
```

La prima colonna contiene il nome del modulo.

La seconda colonna si riferisce alla dimensione della memoria del modulo espressa in byte.

La terza colonna elenca gli esempi del modulo precedentemente caricati. Il valore zero rappresenta un modulo che è stato scaricato.

La quarta colonna indica se il modulo dipende dalla presenza di un altro modulo per poter funzionare, elencando i moduli in questione.

La quinta colonna indica lo stato di caricamento nel quale si trova il modulo: `Live`, `Loading`, o `Unloading`, rappresentano i soli valori possibili.

La sesta colonna indica l'offset attuale della memoria del kernel, per il modulo caricato. Questa informazione potrebbe essere utile per il debugging, o per tool come `oprofile`.

5.2.22. `/proc/mounts`

Questo file fornisce un elenco di tutti i mount utilizzati dal sistema:

```
rootfs / rootfs rw 0 0
/proc /proc proc rw,nodiratime 0 0
none /dev ramfs rw 0 0
/dev/mapper/VolGroup00-LogVol00 / ext3 rw 0 0
none /dev ramfs rw 0 0
/proc /proc proc rw,nodiratime 0 0
/sys /sys sysfs rw 0 0
none /dev/pts devpts rw 0 0
usbdevfs /proc/bus/usb usbdevfs rw 0 0
/dev/hda1 /boot ext3 rw 0 0
none /dev/shm tmpfs rw 0 0
```

```
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
sunrpc /var/lib/nfs/rpc_pipefs rpc_pipefs rw 0 0
```

L'output qui di seguito è simile ai contenuti di `/etc/mtab`, con la differenza che `/proc/mount` potrebbe risultare più aggiornato.

La prima colonna specifica il dispositivo montato e la seconda indica il mountpoint, e la terza colonna indica il tipo di filesystem, mentre la quarta specifica se è montato in modalità di sola lettura (`ro`) oppure lettura-scrittura (`rw`). La quinta e la sesta colonna riportano dei valori fittizi creati in modo da corrispondere al formato in uso in `/etc/mtab`.

5.2.23. /proc/mtrr

Il file si riferisce all'attuale MTRR (Memory Type Range Registers) in uso con il sistema. Se l'architettura del sistema supporta gli MTRR, allora il file `/proc/mtrr` avrà all'incirca questo aspetto:

```
reg00: base=0x00000000 (   0MB), size= 256MB: write-back, count=1
reg01: base=0xe8000000 (3712MB), size=  32MB: write-combining, count=1
```

Gli MTRR vengono utilizzati con i processori Intel della famiglia P6 (Pentium II e successivi) per controllare l'accesso del processore nella gamma della memoria. Usando una scheda video su bus PCI o AGP, un file `/proc/mtrr` configurato correttamente, può aumentare le prestazioni più del 150%.

Il più delle volte, questo valore è configurato per default. Per maggiori informazioni sulla configurazione manuale di questo file consultate quanto segue:

```
/usr/share/doc/kernel-doc-<version>/Documentation/mtrr.txt
```

5.2.24. /proc/partitions

Questo file contiene le informazioni per l'allocazione del blocco della partizione. Un esempio di questo file è simile al seguente:

```
major minor  #blocks  name

   3     0   19531250 hda
   3     1     104391 hda1
   3     2   19422585 hda2
 253     0   22708224 dm-0
 253     1     524288 dm-1
```

Molte delle informazioni qui riportate sono poco importanti per gran parte degli utenti, a eccezione delle linee che seguono:

- `major` — Il numero maggiore del dispositivo con questa partizione. Il numero maggiore in `/proc/partitions`, (`3`), corrisponde al dispositivo a blocco `ide0` presente in `/proc/devices`.
- `minor` — il numero minore del dispositivo con questa partizione. Serve a separare le partizioni in dispositivi fisici differenti e si riferisce al numero posto alla fine del nome della partizione.
- `#blocks` — elenca il numero dei blocchi fisici del disco contenuti in una determinata partizione.
- `name` — nome della partizione.

5.2.25. /proc/pci

Questo file contiene un elenco completo di tutti i dispositivi PCI presenti sul sistema. A seconda del numero dei dispositivi PCI, /proc/pci può raggiungere una discreta lunghezza. Ecco qui un esempio dell'aspetto di questo file su un sistema di base:

```
Bus  0, device   0, function  0:
  Host bridge: Intel Corporation 440BX/ZX - 82443BX/ZX Host bridge (rev 3).
    Master Capable.  Latency=64.
    Prefetchable 32 bit memory at 0xe4000000 [0xe7ffffff].
Bus  0, device   1, function  0:
  PCI bridge: Intel Corporation 440BX/ZX - 82443BX/ZX AGP bridge (rev 3).
    Master Capable.  Latency=64.  Min Gnt=128.
Bus  0, device   4, function  0:
  ISA bridge: Intel Corporation 82371AB PIIX4 ISA (rev 2).
Bus  0, device   4, function  1:
  IDE interface: Intel Corporation 82371AB PIIX4 IDE (rev 1).
    Master Capable.  Latency=32.
    I/O at 0xd800 [0xd80f].
Bus  0, device   4, function  2:
  USB Controller: Intel Corporation 82371AB PIIX4 USB (rev 1).
    IRQ 5.
    Master Capable.  Latency=32.
    I/O at 0xd400 [0xd41f].
Bus  0, device   4, function  3:
  Bridge: Intel Corporation 82371AB PIIX4 ACPI (rev 2).
    IRQ 9.
Bus  0, device   9, function  0:
  Ethernet controller: Lite-On Communications Inc LNE100TX (rev 33).
    IRQ 5.
    Master Capable.  Latency=32.
    I/O at 0xd000 [0xd0ff].
    Non-prefetchable 32 bit memory at 0xe3000000 [0xe30000ff].
Bus  0, device  12, function  0:
  VGA compatible controller: S3 Inc. ViRGE/DX or /GX (rev 1).
    IRQ 11.
    Master Capable.  Latency=32.  Min Gnt=4.Max Lat=255.
    Non-prefetchable 32 bit memory at 0xdc000000 [0xdfffffff].
```

L'output mostra un elenco di tutti i dispositivi PCI nell'ordine bus, dispositivo e funzione. Oltre a riportare il nome e la versione del dispositivo questo elenco fornisce anche informazioni dettagliate sull'IRQ in modo che l'amministratore può andare rapidamente alla ricerca di conflitti.

Suggerimento

Per ottenere una versione più leggibile di queste informazioni, digitate:

```
/sbin/lspci -vb
```

5.2.26. /proc/slabinfo

Questo file fornisce informazioni sull'uso della memoria a livello dello *slab*. I kernel di Linux di versione superiore a 2.2 utilizzano i *gruppi di slab*, per gestire la memoria oltre il livello di pagina. Gli oggetti comunemente utilizzati dispongono di gruppi di slab propri.

Invece di eseguire manualmente il parsing di un file molto dettagliato del tipo `/proc/slabinfo`, il programma `/usr/bin/slabtop` visualizza le informazioni slab cache del kernel in tempo reale. Questo programma permette di eseguire configurazioni personalizzate, incluso il refresh della schermata e l'operazione di riordino delle colonne.

Qui di seguito viene riportato un esempio di `/usr/bin/slabtop`:

```
Active / Total Objects (% used)    : 133629 / 147300 (90.7%)
Active / Total Slabs (% used)      : 11492 / 11493 (100.0%)
Active / Total Caches (% used)     : 77 / 121 (63.6%)
Active / Total Size (% used)       : 41739.83K / 44081.89K (94.7%)
Minimum / Average / Maximum Object : 0.01K / 0.30K / 128.00K

  OBJS ACTIVE  USE OBJ SIZE  SLABS OBJ/SLAB CACHE SIZE NAME
44814  43159  96%    0.62K   7469        6     29876K ext3_inode_cache
36900  34614  93%    0.05K    492       75      1968K buffer_head
35213  33124  94%    0.16K   1531       23      6124K dentry_cache
 7364   6463  87%    0.27K    526       14      2104K radix_tree_node
 2585   1781  68%    0.08K     55       47       220K vm_area_struct
 2263   2116  93%    0.12K     73       31       292K size-128
 1904   1125  59%    0.03K     16      119        64K size-32
 1666    768  46%    0.03K     14      119        56K anon_vma
 1512   1482  98%    0.44K    168        9       672K inode_cache
 1464   1040  71%    0.06K     24       61        96K size-64
 1320    820  62%    0.19K     66       20       264K filp
  678    587  86%    0.02K      3      226        12K dm_io
  678    587  86%    0.02K      3      226        12K dm_tio
  576    574  99%    0.47K     72        8       288K proc_inode_cache
  528    514  97%    0.50K     66        8       264K size-512
  492    372  75%    0.09K     12       41        48K bio
  465    314  67%    0.25K     31       15       124K size-256
  452    331  73%    0.02K      2      226         8K biovec-1
  420    420 100%    0.19K     21       20        84K skbuff_head_cache
  305    256  83%    0.06K      5       61        20K biovec-4
  290      4   1%    0.01K      1      290         4K revoke_table
  264    264 100%    4.00K    264        1      1056K size-4096
  260    256  98%    0.19K     13       20        52K biovec-16
  260    256  98%    0.75K     52        5       208K biovec-64
```

Alcune delle statistiche più comunemente usate in `/proc/slabinfo` e incluse in `/usr/bin/slabtop` includono:

- `OBJS` — Il numero totale di oggetti (blocchi di memoria), incluso quelli in uso (allocati), e quelli di riserva non in uso.
- `ACTIVE` — Il numero di oggetti (blocchi di memoria) in uso (allocati).
- `USE` — Percentuale degli oggetti attivi. ((ACTIVE/OBJS)(100))
- `OBJ SIZE` — Misura degli oggetti.
- `SLABS` — Il numero totale di slab.
- `OBJ/SLAB` — Il numero degli oggetti in grado di essere conservati all'interno di uno slab.
- `CACHE SIZE` — La misura della cache dello slab.

- `NAME` — Il nome dello slab.

Per maggiori informazioni sul programma `/usr/bin/slabtop`, consultate la pagina man di `slabtop`.

5.2.27. `/proc/stat`

Questo file tiene traccia di svariate statistiche relative al sistema dal momento dell'ultimo riavvio. I contenuti di `/proc/stat`, i quali possono raggiungere una discreta lunghezza, iniziano generalmente in questo modo:

```
cpu  259246 7001 60190 34250993 137517 772 0
cpu0 259246 7001 60190 34250993 137517 772 0
intr 354133732 347209999 2272 0 4 4 0 0 3 1 1249247 0 0 80143 0 422626 5169433
ctxt 12547729
btime 1093631447
processes 130523
procs_running 1
procs_blocked 0
preempt 5651840

cpu  209841 1554 21720 118519346 72939 154 27168
cpu0 42536 798 4841 14790880 14778 124 3117
cpu1 24184 569 3875 14794524 30209 29 3130
cpu2 28616 11 2182 14818198 4020 1 3493
cpu3 35350 6 2942 14811519 3045 0 3659
cpu4 18209 135 2263 14820076 12465 0 3373
cpu5 20795 35 1866 14825701 4508 0 3615
cpu6 21607 0 2201 14827053 2325 0 3334
cpu7 18544 0 1550 14831395 1589 0 3447
intr 15239682 14857833 6 0 6 6 0 5 0 1 0 0 0 29 0 2 0 0 0 0 0 0 0 94982 0 286812
ctxt 4209609
btime 1078711415
processes 21905
procs_running 1
procs_blocked 0
```

Alcune delle statistiche più comunemente usate includono:

- `cpu` — Misura il numero di *jiffies* (1/100 di secondo per i sistemi x86) rispettivamente in modalità utente, in modalità utente con priorità bassa (nice), system mode, compiti idle, attesa I/O, IRQ (hardirq), e softirq. IRQ (hardirq) rappresenta la risposta più diretta ad un evento hardware. IRQ implica un lavoro minimo per ordinare il lavoro "pesante" in modo da poter eseguire softirq. Softirq viene eseguito con una priorità più bassa rispetto a IRQ, e quindi può essere interrotto più frequentemente. Il totale per tutte le CPU viene riportato nella parte superiore, mentre ogni singola CPU viene elencata nella parte bassa insieme con le proprie statistiche. Il seguente esempio riporta una configurazione del tipo 4-way Intel Pentium Xeon, con il multi-threading abilitato, quindi in grado di mostrare quattro processori fisici e quattro processori virtuali per un totale di otto processori.
- `page` — numero di pagine di memoria che il sistema ha utilizzato all'interno e all'esterno del disco.
- `swap` — numero di pagine di swap raccolte e liberate dal sistema.
- `intr` — numero degli interrupt verificatisi nel sistema.
- `btime` — tempo di avvio, misurato in numero di secondi, a partire dal 1 gennaio 1970 (noto anche come *epoca*).

5.2.28. /proc/swaps

Questo file misura lo spazio di swap e il suo utilizzo. Per sistemi che hanno un'unica partizione di swap, l'output del file /proc/swap ha all'incirca questo aspetto:

```
Filename                        Type        Size    Used    Priority
/dev/mapper/VolGroup00-LogVol01 partition   524280  0       -1
```

Anche se queste informazioni si possono trovare in altri file disponibili nella directory /proc/, /proc/swap fornisce una rapida rappresentazione del nome di ogni file di swap, del tipo di spazio di swap e delle dimensioni totali usate (in kilobyte). La colonna della priorità è utile quando vengono utilizzati file di swap multipli. Quanto più bassa è la priorità, tanto maggiore è la probabilità che il file di swap venga utilizzato.

5.2.29. /proc/sysrq-trigger

Usando il comando echo, un utente root remoto può eseguire i comandi System Request Key in modo remoto, come se fosse in un terminal locale. Per eseguire echo e quindi per inserire i valori in questo file, /proc/sys/kernel/sysrq deve essere impostato su di un valore diverso da 0. Per maggiori informazioni sul System Request Key, consultate la Sezione 5.3.9.3.

Anche se è possibile scrivere su questo file, non è possibile effettuare la lettura, anche da parte di utente root.

5.2.30. /proc/uptime

Il file indica da quanto tempo il computer è acceso dal momento dell'ultimo riavvio. L'output di /proc/uptime è piuttosto ridotto:

```
350735.47 234388.90
```

Il primo numero indica il numero totale dei secondi trascorsi dall'accensione del sistema, mentre l'altro indica quanti di quei secondi la macchina ha trascorso in idle, in secondi.

5.2.31. /proc/version

Questo file indica la versione del kernel di Linux, del gcc in uso, e della versione di Red Hat Enterprise Linux installata sul sistema:

```
Linux version 2.6.8-1.523 (user@foo.redhat.com) (gcc version 3.4.1 20040714 \
 (Red Hat Enterprise Linux 3.4.1-7)) #1 Mon Aug 16 13:27:03 EDT 2004
```

Queste informazioni servono per diversi scopi, tra cui quello di fornire i dati relativi alla versione al prompt di login.

5.3. Directory all'interno di /proc

Gruppi comuni di informazioni relative al kernel vengono raccolti in directory e sottodirectory all'interno di /proc.

5.3.1. Directory del processo

Ciascuna directory di `/proc` contiene un numero di directory identificate con un numero. Un elenco di queste directory sarà simile al seguente:

```
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 1
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 1010
dr-xr-xr-x    3 xfs      xfs             0 Feb 13 01:28 1087
dr-xr-xr-x    3 daemon   daemon          0 Feb 13 01:28 1123
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 11307
dr-xr-xr-x    3 apache   apache          0 Feb 13 01:28 13660
dr-xr-xr-x    3 rpc      rpc             0 Feb 13 01:28 637
dr-xr-xr-x    3 rpcuser  rpcuser         0 Feb 13 01:28 666
```

Queste directory vengono chiamate *directory del processo*, poiché si riferiscono all'ID di un processo e contengono informazioni specifiche relative a quel processo. Il proprietario e il gruppo di ciascuna di queste directory è impostato per l'utente che sta eseguendo quel dato processo. Una volta terminato, la sua directory `/proc` scompare.

Ciascuna directory del processo contiene i file seguenti:

- `cmdline` — contiene gli argomenti della linea di comando che hanno dato inizio al processo.
- `cwd` — collegamento simbolico con la directory attualmente in funzione per il processo.
- `environ` — Fornisce un elenco delle variabili di ambiente per il processo. La variabile di ambiente viene data in caratteri maiuscoli e il valore in caratteri minuscoli.
- `exe` — collegamento simbolico all'eseguibile di questo processo.
- `fd` — directory contenente tutti i descrittori dei file per un particolare processo. Vengono forniti sotto forma di collegamenti numerati:
  ```
  total 0
  lrwx------    1 root     root           64 May  8 11:31 0 -> /dev/null
  lrwx------    1 root     root           64 May  8 11:31 1 -> /dev/null
  lrwx------    1 root     root           64 May  8 11:31 2 -> /dev/null
  lrwx------    1 root     root           64 May  8 11:31 3 -> /dev/ptmx
  lrwx------    1 root     root           64 May  8 11:31 4 -> socket:[7774817]
  lrwx------    1 root     root           64 May  8 11:31 5 -> /dev/ptmx
  lrwx------    1 root     root           64 May  8 11:31 6 -> socket:[7774829]
  lrwx------    1 root     root           64 May  8 11:31 7 -> /dev/ptmx
  ```
- `maps` — Contiene un elenco delle mappe di memoria per i vari eseguibili e per i file di libreria associati a questo processo. Questo file può essere piuttosto lungo, a seconda della complessità del processo, in ogni caso un esempio di output tratto dal processo `sshd` inizia nel modo seguente:
  ```
  08048000-08086000 r-xp 00000000 03:03 391479     /usr/sbin/sshd
  08086000-08088000 rw-p 0003e000 03:03 391479     /usr/sbin/sshd
  08088000-08095000 rwxp 00000000 00:00 0
  40000000-40013000 r-xp 00000000 03:03 293205     /lib/ld-2.2.5.so
  40013000-40014000 rw-p 00013000 03:03 293205     /lib/ld-2.2.5.so
  40031000-40038000 r-xp 00000000 03:03 293282     /lib/libpam.so.0.75
  40038000-40039000 rw-p 00006000 03:03 293282     /lib/libpam.so.0.75
  40039000-4003a000 rw-p 00000000 00:00 0
  4003a000-4003c000 r-xp 00000000 03:03 293218     /lib/libdl-2.2.5.so
  4003c000-4003d000 rw-p 00001000 03:03 293218     /lib/libdl-2.2.5.so
  ```
- `mem` — memoria occupata dal processo. Questo file non può essere letto dall'utente.
- `root` — collegamento con la directory root del processo.
- `stat` — stato del processo.
- `statm` — stato della memoria utilizzata dal processo. I file `statm` hanno all'incirca questo aspetto:

```
263 210 210 5 0 205 0
```

Le sette colonne si riferiscono alle statistiche della memoria per il processo. Nell'ordine in cui sono disposte, da sinistra a destra, riportano diversi aspetti della memoria utilizzata:

1. Dimensione totale del programma, in kilobyte.
2. Dimensione delle porzioni di memoria, in kilobyte.
3. Numero di pagine condivise.
4. Numero di pagine che contengono programmi di codifica.
5. Numero di pagine di dati/stack.
6. Numero di pagine di libreria.
7. Numero di pagine marcate dirty.

- `status` — Fornisce lo stato del processo in forma molto più leggibile rispetto a `stat` o `statm`. L'output per `sshd` ha un aspetto simile al seguente:

```
Name: sshd
State: S (sleeping)
Tgid: 797
Pid: 797
PPid: 1
TracerPid: 0
Uid: 0 0 0 0
Gid: 0 0 0 0
FDSize: 32
Groups:
VmSize:     3072 kB
VmLck:         0 kB
VmRSS:       840 kB
VmData:      104 kB
VmStk:        12 kB
VmExe:       300 kB
VmLib:      2528 kB
SigPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 8000000000001000
SigCgt: 0000000000014005
CapInh: 0000000000000000
CapPrm: 00000000fffffeff
CapEff: 00000000fffffeff
```

L'informazione in questo output include il nome del processo e l'ID, lo stato, come per esempio `S (sleeping)` o `R(running)`, e l'ID dell'utente/gruppo che sta eseguendo il processo, e dati dettagliati relativi all'utilizzo della memoria.

5.3.1.1. `/proc/self/`

La directory `/proc/self` è un collegamento al processo attualmente in esecuzione. Consente al processo di autoesaminarsi senza dover conoscere il proprio ID.

All'interno di un ambiente shell, un elenco della directory `/proc/self` produce lo stesso contenuto di un elenco della directory per quel processo.

5.3.2. `/proc/bus/`

Questa directory contiene informazioni specifiche per i vari bus disponibili sul sistema. Per esempio, su di un sistema standard contenente bus PCI e USB, i dati correnti su ciascuno di questi bus sono disponibili all'interno della subdirectory sotto `/proc/bus/` tramite lo stesso nome, come ad esempio `/proc/bus/pci/`.

Le subdirectory e i file disponibili all'interno di `/proc/bus/` variano a seconda dei dispositivi collegati al sistema. Tuttavia, ogni tipo di bus possiede almeno una directory. All'interno di queste directory del bus, vi è normalmente almeno una subdirectory identificata da un numero, come ad esempio `001`, la quale contiene file binari.

Per esempio, la subdirectory `/proc/bus/usb` contiene dei file che registrano i vari dispositivi su qualunque bus USB e i driver necessari per utilizzarli. Quanto segue rappresenta un esempio di elenco di una directory `/proc/bus/usb/`:

```
total 0
dr-xr-xr-x    1 root     root            0 May  3 16:25 001
-r--r--r--    1 root     root            0 May  3 16:25 devices
-r--r--r--    1 root     root            0 May  3 16:25 drivers
```

La directory `/proc/bus/usb/001/` contiene tutti i dispositivi sul primo bus USB e il file `devices` identifica un USB root hub sulla scheda madre.

Il seguente è un esempio di un file `/proc/bus/usb/devices`:

```
T:  Bus=01 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#=  1 Spd=12  MxCh= 2
B:  Alloc=  0/900 us ( 0%), #Int=  0, #Iso=  0
D:  Ver= 1.00 Cls=09(hub  ) Sub=00 Prot=00 MxPS= 8 #Cfgs=  1
P:  Vendor=0000 ProdID=0000 Rev= 0.00
S:  Product=USB UHCI Root Hub
S:  SerialNumber=d400
C:* #Ifs= 1 Cfg#= 1 Atr=40 MxPwr=  0mA
I:  If#= 0 Alt= 0 #EPs= 1 Cls=09(hub  ) Sub=00 Prot=00 Driver=hub
E:  Ad=81(I) Atr=03(Int.) MxPS=   8 Ivl=255ms
```

5.3.3. `/proc/driver/`

Questa directory contiene le informazioni per driver specifici usati dal kernel.

Un file comune qui trovato, è `rtc`, il quale fornisce l'output del driver per il *Real Time Clock (RTC)* del sistema, il dispositivo che segna il tempo quando il sistema è spento. L'output prodotto da `/proc/driver/rtc` ha un aspetto simile al seguente:

```
rtc_time        : 16:21:00
rtc_date        : 2004-08-31
rtc_epoch       : 1900
alarm           : 21:16:27
DST_enable      : no
BCD             : yes
24hr            : yes
square_wave     : no
alarm_IRQ       : no
update_IRQ      : no
periodic_IRQ    : no
periodic_freq   : 1024
batt_status     : okay
```

Per maggiori informazioni sull'RTC, consultate la seguente documentazione:

`/usr/share/doc/kernel-doc-<version>/Documentation/rtc.txt`.

5.3.4. /proc/fs

Questa directory indica quali filesystem vengono esportati. Se si esegue un server NFS, potete digitare `cat /proc/fs/nfs/exports` per visualizzare i filesystem condivisi ed i permessi concessi a tali filesystem. Per ulteriori informazioni sulla condivisione dei filesystem con NFS, consultate Capitolo 9.

5.3.5. /proc/ide/

Questa directory contiene informazioni sui dispositivi IDE presenti sul sistema. Ogni canale IDE viene rappresentato come una directory separata, per esempio `/proc/ide/ide0` e `/proc/ide/ide1`. È inoltre disponibile un file `drivers`, che fornisce il numero della versione dei vari driver utilizzati sui canali IDE:

```
ide-floppy version 0.99.newide
ide-cdrom version 4.61
ide-disk version 1.18
```

Molti chipset forniscono anche un file in questa directory, in grado di riportare dati aggiuntivi sulle unità collegate attraverso i vari canali. Per esempio un chipset generico Intel PIIX4 Ultra 33 produce il file `/proc/ide/piix` che indicherà se i protocolli DMA o UDMA sono attivati per i dispositivi sui canali IDE:

```
                            Intel PIIX4 Ultra 33 Chipset.
------------- Primary Channel ---------------- Secondary Channel -------------
                enabled                          enabled
------------- drive0 --------- drive1 -------- drive0 ---------- drive1 ------
DMA enabled:    yes              no              yes               no
UDMA enabled:   yes              no              no                no
UDMA enabled:   2                X               X                 X
UDMA
DMA
PIO
```

Esplorando la directory in cerca di un canale IDE, come `ide0`, si possono ottenere informazioni aggiuntive. Il file `channel` fornisce il numero del canale, mentre `model` indica il tipo di bus per il canale (per esempio `pci`).

5.3.5.1. Directory del dispositivo

Nella directory del canale IDE è presente una directory dei dispositivi, il cui nome corrisponde alla lettera dell'unità nella directory `/dev`. Per esempio, la prima unità IDE su `ide0` sarà `hda`.

Nota Bene

È presente un link simbolico per ogni directory presente all'interno di `/proc/ide/`.

Ciascuna directory dei dispositivi contiene una serie di informazioni e statistiche. Il contenuto delle directory varia a seconda del tipo di dispositivo collegato. Tra i file più utili comuni a diversi dispositivi si trovano:

- `cache` — La cache del dispositivo.
- `capacity` — capacità del dispositivo, in blocchi di 512 byte.
- `driver` — L'unità e la versione usate per controllare il dispositivo.
- `geometry` — geometria fisica e logica del dispositivo.
- `media` — tipo di dispositivo, per esempio `disk`.
- `model` — numero o nome del modello del dispositivo.
- `settings` — Una raccolta dei parametri correnti del dispositivo. Di norma questo file contiene una discreta quantità di informazioni tecniche piuttosto utili. Un esempio di file `settings` per un disco fisso IDE standard potrebbe avere un aspetto simile al seguente:

```
name                    value           min             max             mode
----                    -----           ---             ---             ----
acoustic                0               0               254             rw
address                 0               0               2               rw
bios_cyl                38752           0               65535           rw
bios_head               16              0               255             rw
bios_sect               63              0               63              rw
bswap                   0               0               1               r
current_speed           68              0               70              rw
failures                0               0               65535           rw
init_speed              68              0               70              rw
io_32bit                0               0               3               rw
keepsettings            0               0               1               rw
lun                     0               0               7               rw
max_failures            1               0               65535           rw
multcount               16              0               16              rw
nice1                   1               0               1               rw
nowerr                  0               0               1               rw
number                  0               0               3               rw
pio_mode                write-only      0               255             w
unmaskirq               0               0               1               rw
using_dma               1               0               1               rw
wcache                  1               0               1               rw
```

5.3.6. `/proc/irq/`

La directory è utilizzata per impostare l'affinità tra IRQ e CPU, che consente al sistema di connettere un particolare IRQ a un'unica CPU. Oppure è possibile escludere una CPU dalla gestione degli IRQ.

Ciascun IRQ ha la propria directory, il che gli consente di essere configurato in modo diverso da tutti gli altri. Il file `/proc/irq/prof_cpu_mask` è un bitmask contenente i valori di default per il file `smp_affinity` all'interno della directory IRQ. I valori contenuti in `smp_affinity` specificano quali CPU gestiscono quel particolare IRQ.

Per maggiori informazioni sulla directory `/proc/irq/`, consultate la seguente documentazione:

/usr/share/doc/kernel-doc-<*version*>/Documentation/filesystems/proc.txt

5.3.7. /proc/net/

Questa directory permette di osservare in modo completo i vari parametri e le varie statistiche della rete. Ogni directory e file virtuale all'interno di questa directory, descrive gli aspetti della configurazione di rete del sistema. Di seguito viene riportato un elenco parziale della directory /proc/net/:

- arp — Contiene la tabella ARP del kernel. Questo file è particolarmente utile per collegare l'indirizzo hardware a un indirizzo IP su di un sistema.
- atm — I file all'interno di questa directory contengono le impostazioni *ATM (Asynchronous Transfer Mode, modalità di trasferimento asincrona)* e delle statistiche. Questa directory è usata soprattutto con il networking ATM e le schede ADSL.
- dev — Elenca i vari dispositivi di rete configurati sul sistema, completi di statistiche di trasmissione e ricezione. Questo file indica il numero di byte inviati e ricevuti da ciascuna interfaccia, il numero di pacchetti in entrata ed in uscita, il numero di errori rilevati, il numero dei pacchetti persi e molto altro ancora.
- dev_mcast — Elenca i vari gruppi multicast Layer2 su cui ogni dispositivo è in ascolto.
- igmp — elenca gli indirizzi IP multicast a cui è collegato il sistema.
- ip_conntrack — Elenca i collegamenti di rete tracciati, per macchine che effettuano l'inoltro dei collegamenti IP.
- ip_tables_names — Elenca i tipi di iptables in uso. Questo file è solo presente se iptables è attivo sul sistema e contiene uno o più valori di seguito riportati: filter, mangle, o nat.
- ip_mr_cache — elenca la cache del routing multicast.
- ip_mr_vif — elenca le interfacce virtuali del protocollo multicast.
- netstat — contiene una raccolta molto dettagliata di statistiche di networking, insieme ai servizi di temporizzazione TCP, ai SYN cookie inviati e ricevuti e molto altro.
- psched — elenca i parametri dello schedulatore di pacchetti.
- raw — elenco di statistiche del dispositivo a carattere.
- route — Elenca la tabella di routing del kernel.
- rt_cache — contiene la cache di routing corrente.
- snmp — elenco di dati relativi al protocollo SNMP (Simple Network Management Protocol) per i vari protocolli di networking in uso.
- sockstat — fornisce statistiche per il socket.
- tcp — contiene informazioni dettagliate riguardo al socket TCP.
- tr_rif — tabella di routing per il RIF token ring.
- udp — contiene informazioni dettagliate riguardo al socket UDP.
- unix — elenca i socket di dominio UNIX attualmente in uso.
- wireless — elenca i dati relativi all'interfaccia wireless.

5.3.8. `/proc/scsi/`

Questa directory è analoga alla directory `/proc/ide/`, ma serve per i dispositivi SCSI collegati.

Il file principale contenuto in questa directory è `/proc/scsi/scsi` che contiene un elenco di tutti i dispositivi SCSI riconosciuti. In questo elenco è disponibile il tipo di dispositivo, il nome del modello, il fornitore, il canale SCSI e i dati ID.

Per esempio, se un sistema contiene un CD-ROM SCSI, una unità a nastro, un disco fisso e un controller RAID, questo file sarà simile al seguente:

```
Attached devices:
Host: scsi1 Channel: 00 Id: 05 Lun: 00
  Vendor: NEC      Model: CD-ROM DRIVE:466 Rev: 1.06
  Type:   CD-ROM                           ANSI SCSI revision: 02
Host: scsi1 Channel: 00 Id: 06 Lun: 00
  Vendor: ARCHIVE  Model: Python 04106-XXX Rev: 7350
  Type:   Sequential-Access                ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 06 Lun: 00
  Vendor: DELL     Model: 1x6 U2W SCSI BP  Rev: 5.35
  Type:   Processor                        ANSI SCSI revision: 02
Host: scsi2 Channel: 02 Id: 00 Lun: 00
  Vendor: MegaRAID Model: LD0 RAID5 34556R Rev: 1.01
  Type:   Direct-Access                    ANSI SCSI revision: 02
```

Ciascun dispositivo SCSI utilizzato dal sistema, ha la propria directory all'interno di `/proc/scsi/`, il quale contiene i file specifici di ogni controller SCSI che utilizza quel driver. Dunque, dall'esempio precedente, sono presenti le directory `aic7xxx/` e `megaraid/` poichè vengono utilizzati i due driver. I file di ciascuna delle directory contengono, di norma, la gamma dell'indirizzo I/O, le informazioni IRQ e le statistiche relative al controller SCSI che utilizza quel driver. Ogni controller può riportare un diverso tipo e una diversa quantità di informazioni. Il file dell'adattatore per host Adaptec AIC-7880 Ultra SCSI per il sistema preso come esempio produce il seguente output:

```
Adaptec AIC7xxx driver version: 5.1.20/3.2.4
Compile Options:
  TCQ Enabled By Default : Disabled
  AIC7XXX_PROC_STATS     : Enabled
  AIC7XXX_RESET_DELAY    : 5

Adapter Configuration:
           SCSI Adapter: Adaptec AIC-7880 Ultra SCSI host adapter
                         Ultra Narrow Controller
    PCI MMAPed I/O Base: 0xfcffe000
 Adapter SEEPROM Config: SEEPROM found and used.
      Adaptec SCSI BIOS: Enabled
                    IRQ: 30
                   SCBs: Active 0, Max Active 1,
                         Allocated 15, HW 16, Page 255
             Interrupts: 33726
      BIOS Control Word: 0x18a6
   Adapter Control Word: 0x1c5f
   Extended Translation: Enabled
Disconnect Enable Flags: 0x00ff
     Ultra Enable Flags: 0x0020
 Tag Queue Enable Flags: 0x0000
Ordered Queue Tag Flags: 0x0000
Default Tag Queue Depth: 8
    Tagged Queue By Device array for aic7xxx host instance 1:
      {255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255}
```

```
    Actual queue depth per device for aic7xxx host instance 1:
      {1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1}

Statistics:


(scsi1:0:5:0)
  Device using Narrow/Sync transfers at 20.0 MByte/sec, offset 15
  Transinfo settings: current(12/15/0/0), goal(12/15/0/0), user(12/15/0/0)
  Total transfers 0 (0 reads and 0 writes)
             < 2K      2K+     4K+     8K+    16K+    32K+    64K+   128K+
   Reads:       0        0       0       0       0       0       0       0
  Writes:       0        0       0       0       0       0       0       0


(scsi1:0:6:0)
  Device using Narrow/Sync transfers at 10.0 MByte/sec, offset 15
  Transinfo settings: current(25/15/0/0), goal(12/15/0/0), user(12/15/0/0)
  Total transfers 132 (0 reads and 132 writes)
             < 2K      2K+     4K+     8K+    16K+    32K+    64K+   128K+
   Reads:       0        0       0       0       0       0       0       0
  Writes:       0        0       0       1     131       0       0       0
```

Questo output rivela la velocità di trasferimento ai vari dispositivi SCSI collegati al controller sulla base del canale ID, oltre a delle statistiche dettagliate inerenti alla quantità e alle dimensioni dei file letti o scritti da quel dispositivo. Per esempio, questo controller sta comunicando con il CD-ROM a 20 megabyte al secondo, mentre l'unità a nastro sta comunicando a soli 10 megabyte al secondo.

5.3.9. `/proc/sys/`

La directory `/proc/sys/` è una directory speciale, diversa dalle altre directory presenti in `/proc/`. Infatti, non solo fornisce numerose informazioni relative al sistema, ma consente anche di modificare la configurazione di un kernel. Ciò consente all'amministratore della macchina di abilitare e disabilitare immediatamente le caratteristiche del kernel.

Attenzione

Fate attenzione quando modificate le impostazioni di un sistema di produzione utilizzando i vari file contenuti nella directory `/proc/sys/`. In seguito alla modifica di un'impostazione errata il kernel può diventare instabile e può dunque essere necessario riavviare il sistema.

Per questa ragione, prima di tentare di cambiare un valore nella directory `/proc/sys`, assicuratevi di conoscere le opzioni corrette per quel file.

Un buon modo per determinare se un particolare file può essere configurato oppure se è stato concepito solo per fornire informazioni, è quello di estrarne un elenco con il flag **`-l/`** nel terminale. Se il file può essere scritto, è possibile utilizzarlo per configurare il kernel. Per esempio, un elenco parziale del file `/proc/sys/fs` ha il seguente aspetto:

```
-r--r--r--    1 root     root            0 May 10 16:14 dentry-state
-rw-r--r--    1 root     root            0 May 10 16:14 dir-notify-enable
-r--r--r--    1 root     root            0 May 10 16:14 dquot-nr
-rw-r--r--    1 root     root            0 May 10 16:14 file-max
-r--r--r--    1 root     root            0 May 10 16:14 file-nr
```

In questo elenco i file `dir-notify-enable` e `file-max` possono essere scritti e pertanto è possibile utilizzarli per configurare il kernel. Gli altri file forniscono solamente un feedback in relazione alle attuali impostazioni.

La modifica di un valore all'interno di un file `/proc/sys` viene effettuata ripetendo il nuovo valore nel file. Per esempio, per abilitare il tasto SysRq su un kernel in funzione, digitate il comando:

```
echo 1 > /proc/sys/kernel/sysrq
```

In questo modo il valore del file `sysrq` passerà da `0` (off) a `1` (on).

Alcuni file di configurazione `/proc/sys/` contengono più di un valore. Per inviare a questi file nuovi valori in modo corretto, inserite uno spazio tra ogni valore trasmesso con il comando `echo`, come mostrato in questo esempio:

```
echo 4 2 45 > /proc/sys/kernel/acct
```

Nota Bene

Qualsiasi modifica di configurazione effettuata tramite il comando `echo`, scomparirà nel momento in cui il sistema verrà riavviato. Per sapere come rendere effettive le modifiche dopo il riavvio del sistema, consultate la Sezione 5.4.

La directory `/proc/sys` contiene svariate sottodirectory che controllano aspetti diversi di un kernel in funzione.

5.3.9.1. `/proc/sys/dev/`

Questa directory fornisce parametri per dispositivi particolari presenti sul sistema. Molti sistemi hanno almeno due directory, `cdrom/` e `raid`. I kernel personalizzati possono avere altre directory, come `parport/`, che fornisce la capacità di condividere una porta parallela tra i driver multipli dei dispositivi.

La directory `cdrom/` contiene un file chiamato `info`, in grado di mostrare una serie di parametri importanti del CD-ROM:

```
CD-ROM information, Id: cdrom.c 3.20 2003/12/17

drive name:             hdc
drive speed:            48
drive # of slots:       1
Can close tray:         1
Can open tray:          1
Can lock tray:          1
Can change speed:       1
Can select disk:        0
Can read multisession:  1
Can read MCN:           1
Reports media changed:  1
Can play audio:         1
Can write CD-R:         0
Can write CD-RW:        0
Can read DVD:           0
Can write DVD-R:        0
Can write DVD-RAM:      0
```

```
Can read MRW:           0
Can write MRW:          0
Can write RAM:          0
```

Esaminando rapidamente questo file è possibile scoprire le caratteristiche di un CD-ROM ignoto. Se si dispone di più CD-ROM su uno stesso sistema, ciascun dispositivo avrà la propria colonna di informazioni.

Svariati file contenuti in `/proc/sys/dev/cdrom`, come `autoclose` e `checkmedia`, possono essere utilizzati per controllare il CD-ROM del sistema. Utilizzate il comando `echo` per abilitare o disabilitare queste caratteristiche.

Se nel kernel è stato compilato il supporto RAID, sarà disponibile la directory `/proc/sys/dev/raid`, che conterra almeno due file: `speed_limit_min` e `speed_limit_max`. Queste impostazioni determinano in quale misura va aumentata la velocità con cui viene utilizzato il dispositivo RAID per task di I/O particolarmente intensivi, come la risincronizzazione dei dischi.

5.3.9.2. `/proc/sys/fs/`

Questa directory contiene una serie di opzioni e informazioni relative a vari aspetti del filesystem, tra cui informazioni su quota, file handle, inode e dentry.

La directory `binfmt_misc` viene utilizzata per fornire al kernel il supporto per formati con binari misti.

I file più importanti di `/proc/sys/fs/` comprendono:

- `dentry-state` — Fornisce lo stato della directory della cache. L'aspetto del file è simile al seguente:
  ```
  57411 52939 45 0 0 0
  ```
  Il primo numero mostra il numero totale delle voci presenti nella directory della cache, mentre il secondo visualizza il numero delle voci non utilizzate. Il terzo numero indica i secondi che trascorrono tra il momento in cui una directory viene liberata e il momento in cui è possibile "reclamarla", mentre il quarto misura le pagine richieste attualmente dal sistema. Gli ultimi due numeri non sono in uso e visualizzano solo il numero 0.
- `dquot-nr` — Elenca il numero massimo delle entry di quota disco memorizzato nella cache.
- `file-max` — Elenca il numero massimo di file handle che il kernel può allocare. Aumentando il valore di questo file si possono risolvere eventuali errori derivanti da una carenza di file handle disponibili.
- `file-nr` — Elenca il numero di file handle allocati, il numero di file handle utilizzati e il numero massimo di file handle.
- `overflowgid` e `overflowuid` — definiscono rispettivamente l'ID di gruppo e l'ID utente da utilizzare con filesystem che supportano solo ID utente e di gruppo a 16 bit.
- `super-max` — controlla il numero massimo di superblocchi disponibili.
- `super-nr` — visualizza il numero di superblocchi attualmente in uso.

5.3.9.3. `/proc/sys/kernel/`

Questa directory contiene una serie di file di configurazione che interessano direttamente l'operato del kernel. Tra i file più importanti trovate:

- `acct` — Controlla la sospensione della contabilità relativa a un processo sulla base della percentuale di spazio libero disponibile sul filesystem contenente il log. Per default, il file ha un aspetto simile al seguente:

  ```
  4 2 30
  ```

  Il primo valore definisce la soglia percentuale di spazio libero necessario per ristabilire il logging, mentre il secondo valore stabilisce il limite della percentuale di spazio disponibile quando il logging è sospeso. Il terzo valore definisce l'intervallo in secondi, in cui il kernel interroga il filesystem per vedere se il logging deve essere sospeso o ripreso.

- `cap-bound` — controlla le impostazioni del *limite di capacità*. Fornisce un elenco delle azioni che qualsiasi processo sul sistema è in grado di compiere. Se un'azione non è presente in questo elenco, allora nessun processo è in grado di compierla, a prescindere dalla quantità di privilegi di cui dispone. L'idea di fondo, in questo caso, è quella di rendere più sicuro il sistema facendo in modo che determinate situazioni non si verifichino durante il processo di avvio, per lo meno a partire da un determinato momento.

  Per un elenco di valori valido per questo file virtuale, consultare la seguente documentazione:

  `/lib/modules/<kernel-version>/build/include/linux/capability.h`.

- `ctrl-alt-del` — Controlla se [Ctrl]-[Alt]-[Delete] riavvia il computer in modo corretto tramite `init` (`0`) o se provocherà, piuttosto, un riavvio repentino senza sincronizzare i dirty buffer 'modificati' con il disco (`1`).

- `domainname` — Configura il nome di dominio del sistema, come `example.com`.

- `exec-shield` — Configura il contenuto Exec Shield del kernel. Exec Shield fornisce protezione contro certi tipi di attacchi di sovrannumero del buffer.

  Sono disponibili due valori per il file virtuale:

  - `0` — Disabilita Exec Shield.
  - `1` — Abilita Exec Shield. Questo è il valore di default.

  

  Importante

  Se il sistema stà eseguendo delle applicazioni che riguardano la sicurezza, le quali sono state avviate mentre Exec Shield non era abilitato, le suddette applicazioni devono essere riavviate quando Exec Shield viene abilitato.

- `exec-shield-randomize` — Abilita la randomizzazione della posizione di diversi oggetti all'interno della memoria. Ciò viene usato come deterrente per potenziali aggressori in cerca di programmi e demoni all'interno della memoria. Ogni qualvolta un programma o un demone viene avviato, esso viene posizionato all'interno della memoria in un luogo differente, e mai in un indirizzo della memoria assoluto o statico.

  Sono disponibili due valori per il file virtuale:

  - `0` — Disabilita la randomizzazione di Exec Shield. Ciò può risultare utile per il debugging delle applicazioni.
  - `1` — Abilita la randomizzazione di Exec Shield. Questo è il valore di default. Nota bene: Il file `exec-shield`deve essere impostato su `1` per rendere `exec-shield-randomize` effettivo.

- `hostname` — Configura il nome host del sistema, per esempio `www.example.com`.

- `hotplug` — Configura l'utility da utilizzare quando il sistema rileva una modifica nella configurazione. Viene utilizzato principalmente con USB e Cardbus PCI. Si consiglia di non modificare il

valore di default di /sbin/hotplug, a meno che non si stia provando un nuovo programma che svolga questo ruolo.

- modprobe — Imposta la posizione del programma da utilizzare per caricare i moduli del kernel. Il valore di default di /sbin/modprobe indica che kmod lo chiamerà proprio per caricare il modulo quando un kernel thread richiama kmod.
- msgmax — Imposta la dimensione massima dei messaggi inviati da un processo all'altro, impostata su 8192 byte per default. Si consiglia di evitare di aumentare questo valore, poichè i messaggi in coda tra i vari processi vengono immagazzinati nella memoria non-intercambiabile del kernel. Qualsiasi aumento in msgmax comporterebbe un aumento della quantità di RAM necessaria per il sistema.
- msgmnb — stabilisce il numero massimo di byte consentiti per una singola coda di messaggi. Il numero predefinito è 16384.
- msgmni — definisce il numero massimo di identificatori consentiti per una coda di messaggi. Il valore predefinito è 16.
- osrelease — elenca il numero di release del kernel di Linux. Questo file può essere modificato solo cambiando il sorgente del kernel e ricompilando.
- ostype — visualizza il tipo di sistema operativo. Per default, questo file è impostato su Linux e questo valore può essere modificato solo cambiando la sorgente del kernel e ricompilando.
- overflowgid e overflowuid — definiscono rispettivamente l'ID di gruppo e l'ID utente da utilizzare con le chiamate di sistema su architetture che supportano soltanto ID utente e di gruppo a 16 bit.
- panic — Determina il numero di secondi utilizzati dal kernel per posticipare il riavvio del sistema qualora si verificasse un panic del kernel. Per default, il valore è impostato su 0, il quale disattiva il riavvio automatico in seguito a una crisi.
- printk — questo file controlla una serie di impostazioni relative alla stampa o alla registrazione di messaggi di errore. Ciascun messaggio di errore riportato dal kernel è associato a un *livello di log* che determina l'importanza del messaggio stesso. I valori del livello di log si articolano come segue:
  - 0 — emergenza kernel: il sistema è inutilizzabile.
  - 1 — allarme kernel: è necessario un intervento immediato.
  - 2 — il kernel è in condizioni critiche.
  - 3 — errore generale del kernel.
  - 4 — avvertimento sulle condizioni generali del kernel.
  - 5 — condizioni del kernel normali ma significative.
  - 6 — messaggio informativo riguardo al kernel.
  - 7 — messaggi a livello di debug riguardanti il kernel.

  Nel file printk sono presenti quattro valori:

  ```
  6     4     1     7
  ```

  Ciascuno di questi valori definisce una regola distinta per la gestione dei messaggi di errore. Il primo valore, chiamato *livello di log della console*, indica la priorità più bassa dei messaggi che verranno visualizzati sulla console (più è bassa la priorità, più è alto il numero del livello di log). Il secondo valore definisce il livello di log di default per i messaggi ai quali non è associato un livello di log specificato. Il terzo valore indica la configurazione più bassa per il livello di log della console. Infine, l'ultimo numero indica il valore predefinito per il livello di log della console.
- La directory random — Elenca numerosi valori relativi alla generazione di numeri casuali per il kernel.

- `rtsig-max` — Configura il numero massimo di segnali POSIX realtime che il sistema può tenere in coda contemporaneamente. Il valore di default è `1024`.
- `rtsig-nr` — Elenca il numero attuale di segnali POSIX realtime tenuti in coda dal kernel.
- `sem` — Configura le impostazioni del *semaforo* all'interno del kernel. Per semaforo si intende un oggetto IPC di System V utilizzato per controllare l'uso di un particolare processo.
- `shmall` — stabilisce la quantità totale di memoria condivisa (misurata in byte) che può essere utilizzata sul sistema ogni singola volta. Il valore predefinito è `2097152`.
- `shmmax` — stabilisce la dimensione massima (misurata in byte) del segmento di memoria condivisa consentita dal kernel. Il valore predefinito è `33554432`, ma il kernel può supportare valori molto più alti di questo.
- `shmmni` — stabilisce il numero massimo di segmenti di memoria condivisa per l'intero sistema, in byte. Il valore predefinito è `4096`.
- `sysrq` — Attiva il System Request Key, se questo valore è impostato su un numero diverso dal default cioè zero (`0`).

  Il System Request Key abilita un input immediato al kernel, digitando una semplice combinazione di tasti. Per esempio il System Request Key può essere usato per spegnere o riavviare un sistema immediatamente, e per la sincronizzazione di tutti i filesystem montati o lo scaricamento di informazioni importanti sulla vostra console. Per iniziare un System Request Key, digitare [Alt]-[SysRq]-[*<system request code>*]. Sostituire *<system request code>* con uno dei seguenti codici:

  - `r` — Disabilita la modalità raw per la tastiera, e la imposta su XLATE (una modalità della tastiera limitata che non riconosce i modificatori come ad esempio [Alt], [Ctrl], o [Shift]).
  - `k` — Interrompe tutti i processi attivi in una console virtuale. Chiamato anche *Secure Access Key* (*SAK*), viene usato spesso per verificare che il prompt di login sia generato da `init`, e non da una copia trojan creata per catturare il nome utente e la password.
  - `b` — Esegue un riavvio del kernel senza smontare i file system o sincronizzando i dischi collegati al sistema.
  - `c` — Interrompe il sistema senza smontare i file system o sincronizzando i dischi collegati al sistema.
  - `o` — Disabilita completamente il sistema.
  - `s` — Cerca di sincronizzare i dischi collegati al sistema.
  - `u` — Cerca di eseguire un unmount e di rimontare tutti i file system di sola lettura.
  - `p` — Esegue un output di tutte le flag ed effettua una registrazione sulla console.
  - `t` — Esegue un output di un elenco dei processi sulla console.
  - `m` — Esegue un output delle statistiche della memoria sulla console.
  - `0` fino a `9` — Imposta il livello di log per la console.
  - `e` — Interrompe tutti i processi ad eccezione di `init`, usando SIGTERM.
  - `i` — Interrompe tutti i processi ad eccezione di `init`, usando SIGKILL.
  - `l` — Interrompe tutti i processi usando SIGKILL (incluso `init`). *Il sistema non può essere usato dopo aver emesso il codice System Request Key.*
  - `h` — Visualizza il testo d'aiuto.

  Questa caratteristica è molto utile quando si usa un kernel di sviluppo o quando si verifica un arresto (freeze) del sistema.

Attenzione

Il System Request Key viene considerato pericoloso per la sicurezza, in quanto una console senza alcuna supervisione, permette ad un aggressore di guadagnare accesso al sistema. Per questa ragione, per default non è selezionato.

Per maggiori informazioni sul System Request Key, consultate `/usr/share/doc/kernel-doc-<version>/Documentation/sysrq.txt`.

- `sysrq-key` — Definisce il codice della chiave per il System Request Key (`84` è il default).
- `sysrq-sticky` — Definisce se System Request Key è una combinazione di tasti idonea. I valori accettati sono i seguenti:
  - `0` — [Alt]-[SysRq] e il codice di richiesta del sistema, devono essere premuti simultaneamente. Questo è il valore di default.
  - `1` — [Alt]-[SysRq] devono essere premuti simultaneamente, ma il codice di richiesta del sistema può essere premuto indipendentemente, prima del numero di secondi specificato in `/proc/sys/kernel/sysrq-timer`.
- `sysrq-timer` — Specifica il numero di secondi che devono trascorrere prima che il codice di richiesta del sistema venga premuto. Il valore di default è `10`.
- `tainted` — Indica se un modulo non-GPL è stato caricato.
  - `0` — Nessun modulo non-GPL è stato caricato.
  - `1` — Almeno un modulo senza una licenza GPL (inclusi i moduli senza licenza) è stato caricato.
  - `2` — Almeno un modulo è stato forzato al caricamento con il comando `insmod -f`.
- `threads-max` — stabilisce il numero massimo di thread che il kernel può utilizzare, con un valore di default pari a `2048`.
- `version` — visualizza la data e l'ora dell'ultima compilazione del kernel. Il primo campo di questo file, che può essere per esempio `#3`, si riferisce al numero di volte in cui il kernel è stato costruito dalla base sorgente.

5.3.9.4. `/proc/sys/net/`

Questa directory contiene delle sottodirectory inerenti vari aspetti del networking. Molte configurazioni, durante la compilazione del kernel, rendono disponibili diverse directory, come `appletalk`, `ethernet`, `ipv4`, `ipx` e `ipv6`. Modificando questi file all'interno di queste directory,gli amministratori di sistema sono in grado di sistemare le configurazione della rete su di un sistema in esecuzione.

Data l'ampia gamma di possibili opzioni di networking disponibile con Linux, verranno presentate solo le directory `/proc/sys/net` più comuni.

La directory `/proc/sys/net/core` contiene una serie di impostazioni che controllano l'interazione tra il kernel e i livelli di networking. I file più importanti sono i seguenti:

- `message_burst` — Imposta la quantità di tempo, in decimi di secondo, necessaria per scrivere un messaggio di avvertimento. Questa impostazione viene utilizzata per alleviare gli attacchi del tipo *Denial of Service* (*Dos*). L'impostazione di default è `50`.
- `message_cost` — Determina un costo su ogni messaggio di avvertimento. Più alto è il valore di questo file (il default è impostato su `5`), maggiore è la probabilità che il messaggio venga ignorato. Questa impostazione viene usata per mitigare gli attacchi DoS.

Un hacker potrebbe infatti bombardare il sistema di richieste che generano errori e riempiono le partizioni del disco di log o richiedono a tutte le risorse del sistema di gestire logging di errore. Le impostazioni in `message_burst` e `message_cost` possono essere modificate in funzione del fattore di rischio accettabile per il sistema contro la necessità di un logging di vasta portata.

- `netdev_max_backlog` — stabilisce il numero massimo di pacchetti che possono restare in coda quando la velocità con cui una particolare interfaccia riceve i pacchetti è superiore a quella con cui il kernel è in grado di elaborarli. Il valore predefinito per questo file è `300`.
- `optmem_max` — configura la dimensione massima del buffer ausiliario consentito per ogni socket.
- `rmem_default` — stabilisce la dimensione predefinita (misurata in byte) del buffer del socket per la ricezione.
- `rmem_max` — stabilisce la dimensione massima (misurata in byte) del buffer del socket per la ricezione.
- `wmem_default` — stabilisce la dimensione predefinita (misurata in byte) del buffer del socket per la trasmissione.
- `wmem_max` — stabilisce la dimensione massima (misurata in byte) del socket per la trasmissione.

La directory `/proc/sys/net/ipv4` contiene impostazioni di networking aggiuntive. Molte di queste impostazioni, usate tra di loro, sono utili per impedire attacchi al sistema o utilizzare il sistema in modo che funga da router.

Attenzione

L'errata modifica di questi file può avere ripercussioni sulla connettività remota al vostro sistema.

Qui di seguito viene riportato un elenco di alcuni dei file più importanti contenuti nella directory `/proc/sys/net/ipv4/`:

- `icmp_destunreach_rate`, `icmp_echoreply_rate`, `icmp_paramprob_rate` e `icmp_timeexeed_rate` — Impostano la velocità massima, in centesimi di secondo, di invio dei pacchetti ICMP agli host sotto diverse condizioni. Una impostazione `0` rimuove tutti i ritardi e non è quindi consigliabile.
- `icmp_echo_ignore_all` e `icmp_echo_ignore_broadcasts` — consentono, rispettivamente, al kernel di ignorare i pacchetti ICMP ECHO provenienti da qualsiasi host o solo quelli provenienti da indirizzi broadcast e multicast. Se è impostato il valore `0` il kernel risponderà positivamente, mentre con valore `1` i pacchetti saranno ignorati.
- `ip_default_ttl` — imposta il *TTL (Time To Live)* predefinito, ossia il valore che limita il numero di salti che un pacchetto può compiere prima di arrivare a destinazione. Aumentare questo valore può portare a una riduzione nelle prestazioni del sistema.
- `ip_forward` — consente alle interfacce del sistema di inoltrarsi pacchetti a vicenda. Il valore predefinito di questo file è `0` e ciò significa che la funzione di inoltro non è abilitata. Per attivarla occorre impostare il file su `1`.
- `ip_local_port_range` — Specifica il range di porte che TCP o UDP devono utilizzare quando è necessaria una porta locale. Il primo numero rappresenta la porta più bassa da utilizzare, mentre il secondo numero indica quella più alta. Per i sistemi su cui si prevede di dover utilizzare un numero più elevato di porte rispetto a quello di default 1024 a 4999, dovreste usare un range che và da 32768 a 61000.
- `tcp_syn_retries` — Permette di impostare un limite al numero di tentativi da parte del sistema di trasmettere un pacchetto SYN quando si sta cercando di effettuare una connessione.

- tcp_retries1 — imposta il numero di tentativi di trasmissione consentiti quando si sta cercando di rispondere a una connessione in ingresso. Il numero predefinito è 3.
- tcp_retries2 — imposta il numero di tentativi consentiti di trasmissione dei pacchetti TCP. Il valore predefinito è 15.

Se desiderate un elenco completo dei file e delle opzioni disponibili nella directory /proc/sys/net/ipv4/, consultate il file /usr/share/doc/kernel-doc-<*version*>/Documentation/networking/ip-sysctl.txt.

All'interno della directory /proc/sys/net/ipv4/ esistono altre directory, le quali affrontano un asspetto diverso dello stack di rete. La directory /proc/sys/net/ipv4/conf/ consente di configurare ciascuna delle interfacce del sistema in modo diverso, incluso l'uso delle impostazioni di default per i dispositivi non configurati (nella subdirectory /proc/sys/net/ipv4/conf/default/) e impostazioni che annullano qualsiasi configurazione speciale (nella subdirectory /proc/sys/net/ipv4/conf/all/).

La directory /proc/sys/net/ipv4/neigh/ contiene delle regole per communicare con altri sistemi (o host) direttamente collegati al vostro sistema (denominato network neighbour) e inoltre contiene delle regole diverse per sistemi più distanti più di un hop.

Il routing IPV4 ha la propria directory (/proc/sys/net/ipv4/route/). A differenza di conf/ e neigh, la directory /proc/sys/net/ipv4/route/ contiene delle specifiche applicate al routing di tutte le interfacce presenti sul sistema. Molte di queste impostazioni, tra cui max_size, max_delay e min_delay, riguardano il controllo delle dimensioni della cache di routing. Per vuotare la cache di routing scrivete qualsiasi valore sul file flush.

Informazioni aggiuntive su queste directory e i valori possibili per i loro file di configurazione, possono essere trovati in:

/usr/share/doc/kernel-doc-<*version*>/Documentation/filesystems/proc.txt

5.3.9.5. /proc/sys/vm/

Questa directory facilita la configurazione del sottosistema (VM) virtual memory del kernel di Linux. Il kernel fa un uso estensivo ed efficiente della memoria virtuale, comunemente nota come spazio di swap.

I seguenti file si trovano normalmente nella directory /proc/sys/vm:

- block_dump — Quando abilitato, configura il debugging I/O del blocco. Tutte le operazioni di lettura e scrittura vengono conseguentemente registrate. Ciò può risultare utile se si diagnostica la fase di spin up e spin down del disco per la conservazione della batteria del laptop. Quando block_dump è abilitato, tutti gli output possono essere recuperati tramite dmesg. Il valore di default è 0.

Suggerimento

Se block_dump viene abilitato nello stesso istante del debugging del kernel, è prudente arrestare il demone klogd, in quanto esso potrebbe generare attività non corrette, causate da block_dump.

- dirty_background_ratio — Avvia, tramite un demone pdflush, la riscrittura di dati marcati dirty 'sporchi' nel background su questa percentuale di memoria totale. Il valore di default è 10.
- dirty_expire_centisecs — Definisce quando i dati marcati dirty presenti in memoria, sono abbastanza vecchi da poterli accantonare. I dati marcati dirty presenti in memoria per un periodo maggiore di questo intervallo, vengono accantonati con l'entrata in funzione del demone pdflush. Il valore di default è 3000, ed è espresso in centinaia di secondi.

- `dirty_ratio` — Attiva una riscrittura attivo di dati marcati dirty a questa percentuale di memoria totale, per il generatore dei suddetti dati tramite pdflush. Il valore di default è `10`.
- `dirty_writeback_centisecs` — Definisce l'intervallo tra i risvegli del demone pdflush, il quale elimina dal disco i dati marcati dirty presenti in memoria. Il valore di default è `500`, ed è espresso in centinaia di secondi.
- `laptop_mode` — Minimizza il numero delle volte che un disco fisso ha bisogno di eseguire uno spin up, mantenendo il più a lungo possibile lo spin down, in modo da conservare la potenza della batteria presente sui laptop. Ciò aumeta l'efficienza combinando tutti i processi I/O futuri, riducendo la frequenza di spin up. Il valore di default è `0`, ma viene abilitato automaticamente nel caso in cui viene usata una batteria.

  Questo valore viene controllato automaticamente dal demone acpid una volta notificato all'utente che la potenza della batteria è stata abilitata. Nessuna modifica da parte dell'utente o nessuna interazione risulta essere necessaria, se il laptop supporta la specificazione ACPI (Advanced Configuration and Power Interface)

  Per maggiori informazioni, consultate la seguente documentazione:

  `/usr/share/doc/kernel-doc-<version>/Documentation/laptop-mode.txt`
- `lower_zone_protection` — Determina l'aggressività del kernel nella difesa delle zone di allocazione della memoria più bassa. Ciò può risultare efficace se utilizzato con macchine che presentano uno spazio della memoria `highmem` abilitato. Il valore di default è `0`, nessuna protezione. Tutti gli altri valori interi sono in megabyte, e la memoria `lowmem` è così protetta dall'essere allocata degli utenti.

  Per maggiori informazioni, consultate la seguente documentazione:

  `/usr/share/doc/kernel-doc-<version>/Documentation/filesystems/proc.txt`
- `max_map_count` — configura il numero massimo di zone di memoria map di cui può disporre un processo. Di norma, il valore predefinito `65536` risulta appropriato.
- `min_free_kbytes` — Forza la VM (virtual memory manager) di Linux a mantenere disponibili un numero minimo di kilobytes. La VM utilizza questo numero per elaborare un valore `pages_min` per ogni zona `lowmem` presente nel sistema. Il valore di default risulta essere conforme alla memoria totale della macchina.
- `nr_hugepages` — Indica il numero corrente di pagine `hugetlb` configurate presenti nel kernel.

  Per maggiori informazioni, consultate la seguente documentazione:

  `/usr/share/doc/kernel-doc-<version>/Documentation/vm/hugetlbpage.txt`
- `nr_pdflush_threads` — Indica il numero di demoni pdflush attualmente in esecuzione. Questo file è di sola lettura, e non deve essere modificato da parte dell'utente. Sotto carichi I/O significativi, il valore di default viene aumentato dal kernel.
- `overcommit_memory` — Configura le condizioni sotto le quali una richiesta di memoria molto grande può essere accettata o rifiutata. Sono disponibili le seguenti modalità:
  - `0` — Il kernel esegue una gestione di tipo 'heuristic memory overcommit', calcolando la quantità di memoria disponibile, interrompendo le richieste chiaramente non valide. Sfortunatamente, poichè la memoria è allocata mediante un algoritmo euristico invece di un algoritmo preciso, il sistema può risultare sovraccarico. Ciò rappresenta l'impostazione di default.
  - `1` — Il kernel non esegue alcuna gestione di tipo memory overcommit . Con questa impostazione, viene aumentato il potenziale di sovraccarico del sistema, così come le prestazioni per attività che richiedono molta memoria (come quelle utilizzate da alcune applicazioni scientifiche).
  - `2` — Il kernel non accetta le richieste per la memoria che si aggiungono allo swap più la percentuale della RAM fisica specificata in `/proc/sys/vm/overcommit_ratio`. Questa impostazione è idonea per coloro che desiderano avere un rischio minore di sfruttamento della memoria.

Nota Bene

Questa impostazione è consigliata per i sistemi che presentano aree di swap maggiori della memoria fisica.

- `overcommit_ratio` — Specifica la percentuale della RAM fisica considerata quando `/proc/sys/vm/overcommit_memory` viene impostato su `2`. Il valore di default è `50`.
- `page-cluster` — Stabilisce il numero di pagine lette in una volta. Il valore di default `3`, che di fatto si riferisce a 16 pagine, risulta adeguato per la maggior parte dei sistemi.
- `swappiness` — Determina il numero massimo di swap di una macchina. Più alto è il valore, maggiore saranno gli eventi di swap. Il valore di default, in percentuale, è impostato su `60`.

Tutta la documentazione basata sul kernel è disponibile su:

`/usr/share/doc/kernel-doc-<version>/Documentation/`, il quale contiene informazioni aggiuntive.

5.3.10. `/proc/sysvipc/`

La directory contiene informazioni sulle risorse di System V IPC. I file contenuti in questa directory riguardano le chiamate di System V IPC per i messaggi (`msg`), i semafori (`sem`) e la memoria condivisa (`shm`).

5.3.11. `/proc/tty/`

La directory contiene informazioni circa i *dispositivi tty* disponibili e attualmente in uso sul sistema. I terminali a carattere, che in origine si chiamavano *dispositivi teletype* (telescriventi), vengono ora chiamati dispositivi tty.

In Linux esistono tre diversi tipi di dispositivi tty. I *dispositivi seriali* vengono utilizzati con le connessioni seriali per esempio tramite un modem o un cavo seriale. I *terminal virtuali* creano la connessione comune della console per esempio le console virtuali disponibili quando viene digitata la combinazione di tasti [Alt]-[<F-key>] nella console di sistema. Gli *pseudo terminali* creano una comunicazione bidirezionale (two-way) usata da alcune applicazioni di alto livello per esempio XFree86. Il file `drivers` è, un elenco dei dispositivi tty attualmente in uso come riportato nel seguente esempio:

```
serial               /dev/cua        5  64-127 serial:callout
serial               /dev/ttyS       4  64-127 serial
pty_slave            /dev/pts      136   0-255 pty:slave
pty_master           /dev/ptm      128   0-255 pty:master
pty_slave            /dev/ttyp       3   0-255 pty:slave
pty_master           /dev/pty        2   0-255 pty:master
/dev/vc/0            /dev/vc/0       4       0 system:vtmaster
/dev/ptmx            /dev/ptmx       5       2 system
/dev/console         /dev/console    5       1 system:console
/dev/tty             /dev/tty        5       0 system:/dev/tty
unknown              /dev/vc/%d      4    1-63 console
```

Il file `/proc/tty/driver/serial` elenca le statistiche di utilizzo e lo stato di ciascuna delle linee tty seriali.

Per poter utilizzare i dispositivi tty in modo analogo ai dispositivi di rete, il kernel di Linux applica al dispositivo una *line discipline*. Questo consente al driver di inserire un tipo di intestazione in ogni

blocco dati trasmesso tramite il dispositivo, permettendo così, all'estremo della connessione, di vedere un blocco dati come singola parte di un flusso dati. SLIP e PPP sonoline discipline comuni di linea, utilizzate per connettere tra loro vari sistemi mediante collegamento seriale.

Le line discipline registrate sono memorizzate nel file `ldiscs` e informazioni dettagliate sono disponibili all'interno della directory `ldisc`.

5.4. Usando il comando `sysctl`

Il `/sbin/sysctl` è utilizzato per visualizzare, impostare e automatizzare parametri speciali del kernel nella directory `/proc/sys/`.

Se desiderate una rapida panoramica di tutte le impostazioni configurabili nella directory `/proc/sys/`, digitate il comando `/sbin/sysctl-a` come utente root. Questo rende possibile ottenere un elenco molto dettagliato, una piccola parte di tale elenco ha all'incirca il seguente aspetto:

```
net.ipv4.route.min_delay = 2
kernel.sysrq = 0
kernel.sem = 250     32000     32     128
```

In questo modo si ottengono le stesse informazioni fornite dalla visualizzazione di un singolo file per volta. L'unica differenza è data dalla posizione del file. Per esempio, il file `/proc/sys/net/ipv4/route/min_delay` è elencato come `net.ipv4.route.min_delay`: gli slash della directory sono sostituiti da punti e la parte `proc.sys` sottointesa.

Il comando `sysctl` può essere utilizzato al posto di `echo` per assegnare dei valori ai file scrivibili nella directory `/proc/sys/`. Per esempio, invece di utilizzare questo comando

```
echo 1 > /proc/sys/kernel/sysrq
```

usare il comando `sysctl` equivalente in modo seguente:

```
sysctl -w kernel.sysrq="1"
kernel.sysrq = 1
```

L'impostazione rapida di singoli valori come questo all'interno di `/proc/sys` risulta utile quando si sta effettuando una prova, ma non dà risultati altrettanto positivi su un sistema di produzione, in quanto le impostazioni speciali presenti in `/proc/sys` vanno perdute al riavvio della macchina. Per conservare le impostazioni personali, aggiungetele al file `/etc/sysctl.conf`.

A ogni riavvio del sistema, il programma `init` esegue lo script `/etc/rc.d/rc.sysinit`. Questo script contiene un comando per l'esecuzione di `sysctl`, utilizzando `/etc/sysctl.conf` per stabilire i valori passati al kernel. I valori aggiunti a `/etc/sysctl.conf` avranno effetto subito dopo l'avvio del sistema.

5.5. Risorse aggiuntive

Di seguito è riportato un elenco di fonti aggiuntive relative al filesystem `/proc/`.

5.5.1. Documentazione installata

Alcune delle migliori documentazioni inerenti al filesystem `proc`,sono installate per default, sul sistema.

- /usr/share/doc/kernel-doc-<*version*>/Documentation/filesystems/proc.txt — Contiene alcune informazioni limitate di varia natura, relative a tutti gli aspetti della directory /proc/.
- /usr/share/doc/kernel-doc-<*version*>/Documentation/sysrq.txt — Panoramica sulle opzioni System Request Key.
- /usr/share/doc/kernel-doc-<*version*>/Documentation/sysctl/ — Una directory contenente una varietà di suggerimenti su sysctl, incluso la modifica dei valori che riguardano il kernel (kernel.txt), l'accesso dei file system (fs.txt), e l'utilizzo della memoria virtuale (vm.txt).
- /usr/share/doc/kernel-doc-<*version*>/Documentation/networking/ip-sysctl.txt — Una panoramica dettagliata delle opzioni di networking IP.

5.5.2. Siti Web utili

- http://www.linuxhq.com/ — In questo sito si trova un database completo contenente le sorgenti, le patch e la documentazione relativa a diverse versioni del kernel di Linux.

Capitolo 6.

Utenti e gruppi

Il controllo degli *utenti* e dei *gruppi* è un elemento principale dell'amministrazione del sistema di Red Hat Enterprise Linux.

Gli *utenti* possono essere persone, cioè account riuniti in utenti fisici, o utenti logici, vale a dire account che esistono per applicazioni specifiche.

I *gruppi* sono espressioni logiche dell'organizzazione unendo gli utenti che hanno un fine comune. Gli utenti presenti all'interno di un gruppo possono leggere, scrivere o eseguire i file posseduti da quel gruppo.

Entrambi i tipi di utenti dispongono di numeri d'identificazione chiamati rispettivamente*userid* (*UID*) e di un *groupid* (*GID*).

L'utente che crea un file viene designato come proprietario dello stesso, altresì viene designato al file stesso anche un gruppo. È da segnalare l'assegnazione al file in questione, dei permessi separati di lettura, scrittura ed esecuzione per il proprietario del file, per il gruppo e per altri utenti. Il proprietario del file può essere modificato solo dall'utente root, mentre i permessi per l'accesso possono essere modificati sia dall'utente root che dal proprietario del file.

Red Hat Enterprise Linux supporta l'*access control lists* (*ACLs*) per i file e le directory il quale abilita i permessi da impostare per utenti specifici esternamente al proprietario. Per maggiori informazioni sull'uso di ACL, consultare il capitolo intitolato *Access Control Lists* nella *Red Hat Enterprise Linux System Administration Guide*.

La gestione appropriata degli utenti e dei gruppi e la gestione efficace dei permessi dei file, sono tra le attività più importanti che un amministratore di sistema deve svolgere. Per informazioni più dettagliate sulle strategie, e sulla gestione degli utenti e dei gruppi, consultate il capitolo intitolato *Gestione degli User Account e dell'accesso alle risorse* nella *Red Hat Enterprise Linux Introduzione al System Administration*.

6.1. Tool per la creazione di utenti e gruppi

La gestione degli utenti e dei gruppi può rivelarsi un compito noioso, ma Red Hat Enterprise Linux fornisce alcuni tool e convenzioni per semplificare la gestione da parte degli amministratori.

Il modo più semplice di gestire utenti e gruppi è quello di utilizzare l'applicazione grafica **Utente Manager** (**system-config-users**). Per ulteriori informazioni su **Utente Manager**, consultate il capitolo *Configurazione dell'utente e del gruppo* nella *Red Hat Enterprise Linux System Administration Guide*.

I seguenti strumenti della linea di comando possono essere usati per gestire gli utenti e i gruppi:

- `useradd`, `usermod`, e `userdel` — Metodi standard per l'aggiunta, la modifica o la cancellazione degli account degli utenti.
- `groupadd`, `groupmod`, and `groupdel` — Metodi standard per l'aggiunta, la modifica o la cancellazione degli account dei gruppi.
- `gpasswd` — Metodo standard per l'amministrazione del file `/etc/group`.
- `pwck`, `grpck` — Tool usati per la verifica della password, gruppi, e file shadow associati.
- `pwconv`, `pwunconv` — Tool usati per la conversione a password shadow e successivamente a password standard.

Per una panoramica sulla gestione degli utenti e dei gruppi, consultare la *Red Hat Enterprise Linux Introduzione al System Administration*. Per saperne di piú sugli strumenti della linea di comando per la gestione degli utenti e gruppi, consultare il capitolo *Configurazione dell'utente e del gruppo* nella *Red Hat Enterprise Linux System Administration Guide*.

6.2. Utenti standard

Tabella 6-1 elenca gli utenti standard configurati nel file `/etc/passwd` da una installazione **Completa**. Il groupid (GID) contenuto in questa tabella, rappresenta il *gruppo primario* dell'utente. Per un elenco di gruppi standard, consultate la Sezione 6.3.

Utente	UID	GID	Directory home	Shell
root	0	0	`/root`	`/bin/bash`
bin	1	1	`/bin`	`/sbin/nologin`
daemon	2	2	`/sbin`	`/sbin/nologin`
adm	3	4	`/var/adm`	`/sbin/nologin`
lp	4	7	`/var/spool/lpd`	`/sbin/nologin`
sync	5	0	`/sbin`	`/bin/sync`
shutdown	6	0	`/sbin`	`/sbin/shutdown`
halt	7	0	`/sbin`	`/sbin/halt`
mail	8	12	`/var/spool/mail`	`/sbin/nologin`
news	9	13	`/etc/news`	
uucp	10	14	`/var/spool/uucp`	`/sbin/nologin`
operator	11	0	`/root`	`/sbin/nologin`
games	12	100	`/usr/games`	`/sbin/nologin`
gopher	13	30	`/var/gopher`	`/sbin/nologin`
ftp	14	50	`/var/ftp`	`/sbin/nologin`
nobody	99	99	`/`	`/sbin/nologin`
rpm	37	37	`/var/lib/rpm`	`/sbin/nologin`
vcsa	69	69	`/dev`	`/sbin/nologin`
dbus	81	81	`/`	`/sbin/nologin`
ntp	38	38	`/etc/ntp`	`/sbin/nologin`
canna	39	39	`/var/lib/canna`	`/sbin/nologin`
nscd	28	28	`/`	`/sbin/nologin`
rpc	32	32	`/`	`/sbin/nologin`
postfix	89	89	`/var/spool/postfix`	`/sbin/nologin`
mailman	41	41	`/var/mailman`	`/sbin/nologin`
named	25	25	`/var/named`	`/bin/false`

Utente	UID	GID	Directory home	Shell
amanda	33	6	`var/lib/amanda/`	`/bin/bash`
postgres	26	26	`/var/lib/pgsql`	`/bin/bash`
exim	93	93	`/var/spool/exim`	`/sbin/nologin`
sshd	74	74	`/var/empty/sshd`	`/sbin/nologin`
rpcuser	29	29	`/var/lib/nfs`	`/sbin/nologin`
nsfnobody	65534	65534	`/var/lib/nfs`	`/sbin/nologin`
pvm	24	24	`/usr/share/pvm3`	`/bin/bash`
apache	48	48	`/var/www`	`/sbin/nologin`
xfs	43	43	`/etc/X11/fs`	`/sbin/nologin`
gdm	42	42	`/var/gdm`	`/sbin/nologin`
htt	100	101	`/usr/lib/im`	`/sbin/nologin`
mysql	27	27	`/var/lib/mysql`	`/bin/bash`
webalizer	67	67	`/var/www/usage`	`/sbin/nologin`
mailnull	47	47	`/var/spool/mqueue`	`/sbin/nologin`
smmsp	51	51	`/var/spool/mqueue`	`/sbin/nologin`
squid	23	23	`/var/spool/squid`	`/sbin/nologin`
ldap	55	55	`/var/lib/ldap`	`/bin/false`
netdump	34	34	`/var/crash`	`/bin/bash`
pcap	77	77	`/var/arpwatch`	`/sbin/nologin`
radiusd	95	95	`/`	`/bin/false`
radvd	75	75	`/`	`/sbin/nologin`
quagga	92	92	`/var/run/quagga`	`/sbin/login`
wnn	49	49	`/var/lib/wnn`	`/sbin/nologin`
dovecot	97	97	`/usr/libexec/dovecot`	`/sbin/nologin`

Tabella 6-1. Utenti standard

6.3. Gruppi standard

Tabella 6-2 riporta i gruppi standard configurati da una installazione **Everything**. I gruppi sono conservati nel file `/etc/group`.

Gruppo	GID	Componenti
root	0	root
bin	1	root, bin, daemon
daemon	2	root, bin, daemon

Gruppo	GID	Componenti
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	
disk	6	root
lp	7	daemon, lp
mem	8	
kmem	9	
wheel	10	root
mail	12	mail, postfix, exim
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	
lock	54	
nobody	99	
utenti	100	
rpm	37	
utmp	22	
floppy	19	
vcsa	69	
dbus	81	
ntp	38	
canna	39	
nscd	28	
rpc	32	
postdrop	90	
postfix	89	
mailman	41	
exim	93	
named	25	
postgres	26	
sshd	74	

Gruppo	GID	Componenti
rpcuser	29	
nfsnobody	65534	
pvm	24	
apache	48	
xfs	43	
gdm	42	
htt	101	
mysql	27	
webalizer	67	
mailnull	47	
smmsp	51	
squid	23	
ldap	55	
netdump	34	
pcap	77	
quaggavt	102	
quagga	92	
radvd	75	
slocate	21	
wnn	49	
dovecot	97	
radiusd	95	

Tabella 6-2. Gruppi standard

6.4. User Private Group

Red Hat Enterprise Linux utilizza uno schema *user private group* (*UPG*), che semplifica l'utilizzo dei gruppi UNIX.

Un UPG viene creato ogni qualvolta viene aggiunto un nuovo utente al sistema. Un UPG possiede lo stesso nome dell'utente per il quale è stato creato, e solo quel particolare utente é un membro UPG.

Gli UPG garantiscono una impostazione sicura dei permessi di default per file o directory appena create, i quali sono in grado di abilitare sia l'utente che *il gruppo di quell'utente* ad eseguire modifiche ai file o alle directory in questione.

L'impostazione che determina i permessi applicati ai nuovi file o directory viene chiamata *umask*, essa viene configurata nel file `/etc/bashrc`. Tradizionalmente, sui sistemi UNIX la `umask` é `022`, tale impostazione permette solo all'utente che ha creato il file o la directory, di eseguire le modifiche. Con questo schema tutti gli altri utenti, *incluso i membri dell'utente che ha creato il gruppo*, non sono abilitati ad eseguire alcuna modifica. Tuttavia, con lo schema UPG, questa "protezione di gruppo" non è necessaria, in quanto ogni utente possiede il proprio gruppo privato.

6.4.1. Directory di gruppo

Molte organizzazioni IT preferiscono la creazione di un gruppo per ogni progetto principale, assegnando successivamente un certo numero di persone, atte all'accesso del suddetto progetto se necessario. Con questo schema tradizionale, la gestione dei file si è rivelata complessa; quando un utente crea un file, quest'ultimo viene associato al gruppo primario a cui appartiene l'utente. Quando un singolo utente lavora su più progetti, risulta essere difficile associare i file corretti con il gruppo appropriato. Con lo schema UPG, invece, i gruppi vengono assegnati automaticamente ai file creati all'interno di una directory con il bit *setgid* impostato. Il bit setgid semplifica notevolmente la gestione dei progetti di gruppo che condividono una directory comune, in quanto qualsiasi file creato da un utente all'interno della directory, viene posseduto dal gruppo che detiene la directory.

Supponiamo, per esempio, che un gruppo di persone lavora sui file nella directory `/usr/lib/emacs/site-lisp/`. Alcune persone possono modificare la directory ma ovviamente non tutti i componenti del gruppo. Cosí create prima un gruppo `emacs`, come riportato dal seguente comando:

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

Per associare il contenuto della directory al gruppo `emacs`, digitate:

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

È ora possibile aggiungere gli utenti appropriati al gruppo con il comando `gpasswd`:

```
/usr/bin/gpasswd -a <username> emacs
```

Per abilitare gli utenti a creare file all'interno della directory, usare il seguente comando:

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

Un nuovo file creato viene assegnato al gruppo privato di default dell'utente. Successivamente, impostare al setgid bit, che assegna ogni cosa creata nella directory, lo stesso permesso della directory (`emacs`). Usare il seguente comando:

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

A questo punto, perché l'impostazione di umask é 002, tutti i membri del gruppo `emacs` possono creare e modificare i file nella directory `/usr/lib/emacs/site-lisp/` senza che l'amministratore deve cambiare i permessi del file, ogni qualvolta che gli utenti scrivono nuovi file.

6.5. Password Shadow

Negli ambienti multiutente é molto importatnte usare le *password shadow* (fornite dal pacchetto `shadow-utils`). Così facendo si aumenta la sicurezza dei file di autenticazione del sistema. Per questo motivo, il programma di installazione abilita per default le password shadow.

Il seguente è un elenco dei vantaggi offerti dalle password shadow rispetto allo standard precedente di archiviazione delle password nei sistemi basati su UNIX:

- Sicurezza del sistema migliorata spostando le password cifrate, in genere contenute in `/etc/passwd`, in `/etc/shadow`, un file leggibile solo da utenti root.
- Informazioni relative all'invecchiamento della password.
- Capacità di utilizzare il file `/etc/login.defs` per rafforzare i criteri di sicurezza.

Molte utility fornite dal pacchetto `shadow-utils` lavorano in modo corretto con o senza abilitare le password shadow. Comunque, poichè le informazioni sulla password sono contenute esclusivamente nel file `/etc/shadow`, qualsiasi comando che crea o modifica tali informazioni non avrá alcun effetto.

Di seguito viene riportata una lista di comandi non validi se non si abilitano prima le password shadow:

- `chage`
- `gpasswd`
- `/usr/sbin/usermod` o le opzioni `-e` o `-f`
- `/usr/sbin/useradd` o le opzioni `-e` o `-f`

6.6. Risorse aggiuntive

Per maggiori informazioni sugli utenti e sui gruppi, e sui tool per la loro gestione, fare riferimento alle seguenti risorse.

6.6.1. Documentazione installata

- Pagine man correlate — Vi è un certo numero di pagine man per ogni applicazione e file di configurazione interessato nella gestione degli utenti e dei gruppi. Il seguente è un elenco di alcune delle pagine man più importanti.

  Applicazioni amministrative di utenti e gruppi

  - `man chage` — Un comando utilizzato per modificare le policy di invecchiamento delle password e per la scadenza dell'account.
  - `man gpasswd` — Metodo standard per l'amministrazione del file `/etc/group`.
  - `man groupadd` — Un comando per aggiungere i gruppi.
  - `man grpck` — Un comando usato per verificare il file file `/etc/group`.
  - `man groupdel` — Un comando usato per rimuovere i gruppi.
  - `man groupmod` — Un comando usato per modificare l'appartenenza del gruppo.
  - `man pwck` — Un comando usato per verificare i file `/etc/passwd` e `/etc/shadow`.
  - `man pwconv` — Uno strumento per la conversione a password shadow da password standard.
  - `man pwconv` — Uno strumento per la conversione da password shadow a password standard.
  - `man useradd` — Un comando usato per aggiungere utenti.
  - `man userdel` — Un comando usato per rimuovere utenti.
  - `man usermod` — Un comando usato per modificare gli utenti.

File di configurazione

- `man 5 group` — Il file contenente le informazioni del gruppo per il sistema.
- `man 5 passwd` — Il file contenente le informazioni dell'utenteper il sistema.
- `man 5 shadow` — Il file contenente le password e le informazioni inerenti la scadenza dell'account per il sistema.

6.6.2. Libri correlati

- *Red Hat Enterprise Linux Introduzione al System Administration*; Red Hat, Inc. — Questo manuale fornisce una panoramica sui concetti e sulle tecniche di gestione del sistema. Il capitolo intitolato *Gestione degli account dell'utente e accesso alle risorse* presenta delle informazioni interessanti per la gestione dell'account del gruppo e dell'utente.

- *Red Hat Enterprise Linux System Administration Guide*; Red Hat, Inc. — Questo manuale contiene più informazioni sulla gestione degli utenti e dei gruppi ed anche sulla configurazione avanzata del permesso usando le ACL. Consultare i capitoli intitolati *Configurazione dell'utente e del gruppo* e *Access Control Lists* per maggiori informazioni.

- *Red Hat Enterprise Linux Security Guide*; Red Hat, Inc. — Questo manuale fornisce aspetti relativi alla sicurezza degli account di un utente, e come scegliere una password molto sicura.

Capitolo 7.

Il sistema X Window

Sebbene il kernel sia il fulcro di Red Hat Enterprise Linux, per molti utenti, l'interlocutore del sistema operativo è l'ambiente grafico fornito dal *Sistema X Windows*, più semplicemente noto come *X*.

UNIX™, che può vantare la presenza degli ambienti 'windowing' da decenni, ha anticipato molti dei principali sistemi operativi esistenti. Il sistema X è ormai l'ambiente grafico predominante per i sistemi operativi simili a UNIX.

L'ambiente grafico per Red Hat Enterprise Linux é fornito da X.Org Foundation™, un consorzio open source creato per gestire lo sviluppo e la strategia per il sistema X Window e per le tecnologie correlate. X.Org rappresenta un progetto in rapida espansione con centinaia di sviluppatori intorno al mondo. Contiene una larga gamma di supporto per una varietá di dispositivi hardware e architetture, e puó essere eseguito su diversi sistemi operativi e piattaforme. Questa release di Red Hat Enterprise Linux, include in modo specifico la release X11R6.8 del sistema X Window.

Il sistema X Window usa un'architettura server-client. Il *server X* (il binario `Xorg`), è in ascolto per connessioni provenienti dalle applicazioni *X client*, tramite una rete o una interfaccia loopback locale. Il server comunica con l'hardware, come ad esempio la scheda video, monitor, la tastiera e il mouse. Le applicazioni X client sono presenti nello spazio-utente, creando una *graphical user interface* (*GUI*) per l'utente, passando altresì le richieste al server X.

7.1. La release X11R6.8

Red Hat Enterprise Linux 4 utilizza la release X11R6.8 come base del sistema X Window, la quale include numerosi miglioramenti tecnologici di X.Org, come ad esempio il supporto 3D per le accelerazioni hardware, l'estensione XRender per font anti-aliased, un design modulare basato sul driver, e un supporto per video hardware moderni e per dispositivi ad input.

Importante

Red Hat Enterprise Linux non fornisce più i pacchetti server XFree86™. Prima di eseguire l'aggiornamento e passare all'ultima versione di Red Hat Enterprise Linux, assicuratevi che la vostra scheda video sia compatibile con la release X11R6.8, controllando l'elenco di compatibilità hardware di Red Hat all'indirizzo http://hardware.redhat.com/.

I file relativi alla release X11R6.8 risiedono principalmente in due posizioni:

/usr/X11R6/

Contiene il server X ed altre applicazioni client e i file di testo X, le librerie, i moduli e la documentazione.

`/etc/X11`

Contiene tutti i file di configurazione per X client e per le applicazioni server. Ciò include i file di configurazione per lo stesso server X, il font server `xfs` piú vecchio, i display manager X, e molti altri componenti di base.

É importante notare che il file di configurazione per l'architettura del font basato su Fontconfig é `/etc/fonts/fonts.conf` (il quale sostituisce il file `/etc/X11/XftConfig`). Consultare la Sezione 7.4 per maggiori informazioni.

Poichè il server X esegue dei compiti avanzati su di una vasta gamma di array hardware, esso necessita una configurazione dettagliata. Il programma di installazione installa e configura X automaticamente, a meno che i pacchetti della release X non sono stati selezionati per l'installazione. Tuttavia, se il monitor o la scheda video cambia, X deve essere configurato nuovamente. Il miglior modo per fare questo, é di usare lo **Strumento di configurazione X** (`system-config-display`).

Per avviare lo **Strumento di configurazione X** da una sessione X attiva, andare su **Pulsante menu principale** (sul pannello) => **Impostazioni del sistema** => **Display**. Dopo aver usato **Strumento di configurazione X** durante una sessione X, i cambiamenti avranno effetto dopo che l'utente ha effettuato un log out e successivamente un log in. Per maggiori informazioni sull'uso di **Strumento di configurazione X** consultare il capitolo intitolato *Configurazione del sistema Window X* nella *Red Hat Enterprise Linux System Administration Guide*.

In alcune situazioni, riconfigurare il server X puó richiedere una modifica manuale del file di configurazione, `/etc/X11/xorg.conf`. Per informazioni sulla struttura di questo file, consultate la Sezione 7.3.

7.2. Ambienti desktop e Window Manager

Una volta che il server X è in esecuzione, le applicazioni X client si possono collegare ad esso, creando una GUI per l'utente. È possibile ottenere una gamma di GUI con Red Hat Enterprise Linux, dal *Tab Window Manager*, all'ambiente desktop *GNOME* interattivo e molto sviluppato, conosciuto dagli utenti di Red Hat Enterprise Linux.

Per creare una GUI piú avanzata, due classi principali di applicazioni del client X, devono essere collegate al server X: un *ambiente desktop* e un *window manager*.

7.2.1. Ambienti desktop

Un ambiente desktop unisce diversi client X che possono essere lanciati insieme usando metodi simili, utilizzando un ambiente di sviluppo comune.

Gli ambienti desktop contengono funzioni avanzate che consentono ai client X e ad altri processi correnti di comunicare fra loro, permettendo anche a tutte le applicazioni scritte, di funzionare in quell'ambiente ed effettuare compiti avanzati, fra cui la possibilità di utilizzare la tecnica di trascinamento e rilascio (drag-and-drop) del testo.

Red Hat Enterprise Linux fornisce due ambienti desktop:

- *GNOME* — L'ambiente desktop di default per Red Hat Enterprise Linux basato sul toolkit grafico GTK+ 2.
- *KDE* — Un ambiente desktop alternativo basato sul toolkit grafico Qt 3.

Entrambi GNOME e KDE hanno delle applicazioni di produttivitá avanzate, come ad esempio word processors, spreadsheets, e Web browser e fornisce degli strumenti per personalizzare l'aspetto della GUI. In aggiunta, se entrambi GTK+ 2 e le librerie Qt sono presenti, le applicazioni KDE possono essere eseguite in GNOME e viceversa.

7.2.2. Window Manager

I *Window Manager* sono programmi del client X che controllano il modo in cui vengono posizionati, ridimensionati o spostati gli altri client X. I Window Manager possono disporre anche di barre dei titoli per finestre, anteprima tastiera mediante tastiera o mouse, corrispondenze tasti e pulsanti mouse specificate dall'utente. I Window Manager operano con un insieme di client X differenti, proteggono il programma e gli conferiscono un aspetto particolare e una posizione sullo schermo.

Con Red Hat Enterprise Linux vengono incluse quattro window manager:

- `kwin` — Il window manager *KWin* é il window manager di default per KDE. Esso é un window manager efficiente che supporta i temi personali.
- `metacity` — Il window manager *Metacity* é il window manager di default per GNOME. È un window manager semplice ed efficiente che supporta i temi personali.
- `mwm` — Il window manager *Motif* é un window manager basico, un window manager del tipo standalone. Poichè è stato creato per essere un window manager che può essere usato da solo, esso non dovrebbe essere usato insieme con GNOME o KDE.
- `twm` — *Tab Window Manager*, in grado di fornire un set di tool di base di qualsiasi window manager, e puó essere usato sia da solo che con un ambiente desktop. É installato come parte della release X11R6.8.

I suddetti Window Manager possono essere eseguiti senza gli ambienti desktop, in modo da ottenere una migliore visione delle differenze presenti. Per fare questo, digitare il comando `xinit -e<percorso-verso-il-Window-Manager>`, dove `<percorso-verso-il-Window-Manager>` è la posizione del file binario del Window Manager. Questo file può essere individuato digitando `which <nome-Window-Manager>`, dove `<nome-Window-Manager>` è il nomke del window manager che state interrogando.

7.3. File di configurazione del server X

Il server X é un eseguibile a binario singolo (`/usr/X11R6/bin/Xorg`) che dinamicamente carica qualsiasi modulo del server X, necessario al momento dell'esecuzione dalla directory `/usr/X11R6/lib/modules/`. Alcuni di questi moduli sono caricati automaticamente dal server, mentre altri sono facoltativi e devono essere specificati nel file di configurazione del server X.

Il server X e i file di configurazione associati, sono archiviati nella directory `/etc/X11/`. Il file di configurazione per il server X è `/etc/X11/xorg.conf`. Una volta installato Red Hat Enterprise Linux, i file di configurazione per X vengono creati mediante informazioni raccolte sull'hardware del sistema, durante il processo di installazione.

7.3.1. `xorg.conf`

Poichè è molto rara la necessità di modificare manualmente il file `/etc/X11/xorg.conf`, é utile conoscere le varie sezioni ed i parametri delle opzione disponibili, in modo particolare quando si effettua un troubleshooting.

7.3.1.1. La struttura

Il file `/etc/X11/xorg.conf` é costituito da tante sezioni diverse le quali affrontano aspetti specifici dell'hardware del sistema.

Ogni sezione inizia con una riga `Section "<nome della-sezione>"` (dove `<nome della-sezione>` é il titolo della sezione) e finisce con una riga `EndSection`. All'interno di ogni sezione, ci sono le righe contenenti i nomi dell'opzione e almeno un valore dell'opzione, alcune volte riportato tra virgolette (`"`).

Le righe che iniziano con il carattere (`#`), non vengono lette dal server X e sono usate per commenti del tipo human-readable.

Alcune opzioni all'interno del file `/etc/X11/Xxorg.conf` accettano un interruttore boolean il quale è in grado di abilitare o disabilitare i contenuti. I valori boolean accettabili sono:

- `1`, `on`, `true`, o `yes` — Imposta l'opzione su on.
- `0`, `off`, `false`, o `no` — Imposta l'opzione su off.

Di seguito sono riportate alcune delle sezioni piú importanti visualizzate in un file tipico `/etc/X11/xorg.conf`. Per maggiori informazioni riguardanti i file di configurazione del server X, consultate la pagina man di `xorg.conf`.

7.3.1.2. `ServerFlags`

La sezione `ServerFlags` contiene varie impostazioni del server X globale. Qualsiasi impostazione in questa sezione puó essere sovrascritta dalle opzioni posizionate nella sezione `ServerLayout` (consultare la Sezione 7.3.1.3 per maggiori informazioni).

Ogni entry all'interno della sezione `ServerFlags` è presente sulla propria riga e inizia con il termine `Option` seguita da una opzione racchiusa da delle virgolette (["]).

Il seguente é un esempio di sezione `ServerFlags`:

```
Section "ServerFlags"
      Option "DontZap" "true"
EndSection
```

Il seguente é un elenco di alcune delle opzioni piú utili:

- `"DontZap" "<boolean>"` — Quando il valore di *<boolean>* é impostato su vero, questa impostazione previene l'uso della combinazione [Ctrl]-[Alt]-[Backspace] per la terminazione del server X.
- `"DontZoom" "<boolean>"` — Quando questo valore di *<boolean>* é impostato su vero, questa impostazione previene il cycling attraverso le risoluzioni video configurate usando le combinazioni [Ctrl]-[Alt]-[Keypad-Plus] e [Ctrl]-[Alt]-[Keypad-Minus]

7.3.1.3. `ServerLayout`

La sezione `ServerLayout` raggruppa i dispositivi input e output controllati dal server X. Questa sezione specifica un dispositivo output e almeno due dispositivi input (una tastiera e un mouse).

Il seguente esempio illustra una sezione tipica di `ServerLayout`:

```
Section  "ServerLayout"
        Identifier     "Default Layout"
        Screen      0  "Screen0" 0 0
        InputDevice    "Mouse0" "CorePointer"
        InputDevice    "Keyboard0" "CoreKeyboard"
EndSection
```

Le seguenti entry sono comunemente usate nella sezione `ServerLayout`:

- `Identifier` — Specifica un nome unico per questa sezione `ServerLayout`.
- `Screen` — Specifica il nome di una sezione `Screen` da usare con il server X. Puó essere presente piú di una opzione `Screen`.

  Il seguente é un esempio di una entry tipica `Screen`:

  ```
  Screen      0  "Screen0" 0 0
  ```

  Il primo numero presente in questo esempio della entry `Screen (0)`, indica che il primo connettore monitor o *head* sulla scheda video usa la configurazione specificata nella sezione `Screen` con l'identificatore `"Screen0"`.

  Se la scheda video ha piú di una testina, un'altra entry `Screen` sará necessaria con un numero diverso e un diverso identificatore della sezione `Screen`.

Il numero alla destra di `"Screen0"` indica le coordinate assolute X e Y nell'angolo alto a sinistra della schermata (`0 0` per default).

- `InputDevice` — Specifica un nome di una sezione `InputDevice` da usare con il server X.

  È necessaria la presenza di almeno due entry `InputDevice`: una per il mouse di default e una per la tastiera di default. Le opzioni `CorePointer` e `CoreKeyboard` indicano che essi sono il mouse e la tastiera primaria.

- `Option "<option-name>"` — Una entry facoltativa che specifica parametri aggiuntivi per la sezione. Qualsiasi opzione elencata qui, sovrascrive quelle elencate nella sezione `ServerFlags`.

  Sostituire *<nome-opzione>* con una opzione valida elencata per questa sezione nella pagina man `xorg.conf`.

É possibile creare piú di una sezione `ServerLayout`. Tuttavia, il server leggerá solo il primo, a meno che una sezione `ServerLayout` alternata viene specificata come argomento della linea di comando.

7.3.1.4. `Files`

La sezione `Files` imposta i percorsi per i servizi vitali per il server, come ad esempio il percorso del font.

Il seguente esempio riporta una sezione `Files` tipica:

```
Section "Files"
        RgbPath      "/usr/X11R6/lib/X11/rgb"
        FontPath     "unix/:7100"
EndSection
```

Le seguenti entry sono usate comunemente nella sezione `Files`:

- `RgbPath` — Specifica la posizione dell'RGB color database. Questo database definisce tutti i nomi dei colori validi in X, correlandoli a valori RGB specifici.
- `FontPath` — Specifica dove il server X deve collegarsi per ottenere i font dal font server `xfs`.

  Per default, il `FontPath` é `unix/:7100`. Questo indica al server X di ottenere le informazioni sul font usando i socket del dominio UNIX, per l'inter-process communication (IPC) sulla porta 7100.

  Consultate la Sezione 7.4 per maggiori informazioni riguardanti X e sui font.

- `ModulePath` — Un parametro facoltativo che specifica le directory alternate che memorizzano i moduli del server X.

7.3.1.5. `Module`

La sezione `Module` specifica i moduli dalla directory `/usr/X11R6/lib/modules/` che devono essere caricati dal server X. I moduli aggiungono maggiore funzionalitá al server X.

Il seguente esempio illustra una tipica sezione `Module`:

```
Section "Module"
 Load  "dbe"
 Load  "extmod"
 Load  "fbdevhw"
 Load  "glx"
 Load  "record"
 Load  "freetype"
 Load  "type1"
 Load  "dri"
EndSection
```

7.3.1.6. `InputDevice`

Ogni sezione `InputDevice` configura un dispositivo input per il server X. I sistemi generalmente hanno almeno due sezioni `InputDevice`, una tastiera e un mouse.

Il seguente esempio illustra una sezione `InputDevice` tipica per un mouse:

```
Section "InputDevice"
 Identifier  "Mouse0"
 Driver      "mouse"
 Option     "Protocol" "IMPS/2"
 Option     "Device" "/dev/input/mice"
 Option     "Emulate3Buttons" "no"
EndSection
```

Le seguenti entry sono usate comunemente nella sezione `InputDevice`:

- `Identifier` — Specifica un nome unico per questa sezione `InputDevice`. Questa é una entry necessaria.
- `Driver` — Specifica il nome del dispositivo driver X che deve essere caricato per il dispositivo.
- `Option` — Specifica le opzioni pertinenti al dispositivo.

  Per un mouse, queste opzioni includono generalmente:

  - `Protocol` — Specifica il protocollo usato dal mouse, come ad esempio `IMPS/2`.
  - `Device` — Specifica la posizione del dispositivo fisico.
  - `Emulate3Buttons` — Specifica se abilitare un mouse a tre pulsanti quando entrambi i pulsanti sono pigiati contemporaneamente.

  Consultate la pagina man di `xorg.conf` per un elenco di opzioni valide per questa sezione.

Per default la sezione `InputDevice` presenta alcuni commenti per abilitare gli utenti a configurare le opzioni aggiuntive.

7.3.1.7. `Monitor`

Ogni sezione `Monitor` configura un tipo di monitor usato dal sistema. Poichè una sezione `Monitor` é il minimo, si possono verificare esempi aggiuntivi per ogni tipo di monitor in uso con la macchina.

Il modo migliore di configurare un monitor é quello di configurare X durante il processo di installazione o usando lo **Strumento di configurazione X**. Per maggiori informazioni sull'uso dello **Strumento di configurazione X**, fare riferimento al capitolo intitolato *Configurazione del sistema X Window* nella *Red Hat Enterprise Linux System Administration Guide*.

Questo esempio riporta una sezione `Monitor` tipica per un monitor:

```
Section "Monitor"
 Identifier   "Monitor0"
 VendorName   "Monitor Vendor"
 ModelName    "DDC Probed Monitor - ViewSonic G773-2"
 DisplaySize  320 240
 HorizSync    30.0 - 70.0
 VertRefresh  50.0 - 180.0
EndSection
```

Avviso

Prestate attenzione se modificate manualmente i valori nella sezione `Monitor` di `/etc/X11/xorg.conf`. Valori inappropriati possono danneggiare o distruggere il monitor. Consultate la documentazione del monitor per un elenco dei parametri operativi sicuri.

Di seguito sono riportate le entry comuni usate nella sezione `Monitor`:

- `Identifier` — Specifica un nome unico per questa sezione `Monitor`. Questa é una entry necessaria.
- `VendorName` — Un parametro facoltativo che specifica il produttore del monitor.
- `ModelName` — Un parametro facoltativo che specifica il nome del modello del monitor.
- `DisplaySize` — Un parametro facoltativo che specifica in millimetri la misura fisica dell'area del monitor.
- `HorizSync` — Specifica la portata delle frequenze sync orizontali compatibile con il monitor in kHz. Questi valori aiutano il server X a determinare la validitá delle entry `Modeline` interne o specificate per il monitor.
- `VertRefresh` — Specifica la portata delle frequenze verticali di 'refresh' supportate dal monitor in kHz. Questi valori aiutano il server X a determinare la validitá delle entry `Modeline` interne o specificate per il monitor.
- `Modeline` — Un parametro facoltativo che specifica le modalitá di video aggiuntivi per il monitor a risoluzioni particolari, con alcune risoluzioni di ricaricamento verticali e orizzontali. Consultate la pagina man `xorg.conf`, per una spiegazione piú dettagliata delle entry `Modeline`.
- `Option "<nome-opzione>"` — Una entry facoltativa che specifica i parametri aggiuntivi per la sezione. Sostituire *<nome-opzione>* con una valida opzione elencata per questa sezione nella pagina man `xorg.conf`.

7.3.1.8. `Device`

Ogni sezione `Device` configura una scheda video sul sistema. Una sezione `Device` é il minimo, istanze aggiuntive possono verificarsi per ogni scheda video installata sulla macchina.

Il modo migliore di configurare un monitor é quello di configurare X durante il processo di installazione o usando lo **Strumento di configurazione X**. Per maggiori informazioni sull'uso dello **Strumento di configurazione X**, fare riferimento al capitolo intitolato *Configurazione del sistema X Window* nella *Red Hat Enterprise Linux System Administration Guide*.

Il seguente esempio illustra una sezione `Device` tipica per il mouse:

```
Section "Device"
 Identifier  "Videocard0"
 Driver      "mga"
 VendorName  "Videocard vendor"
 BoardName   "Matrox Millennium G200"
 VideoRam    8192
        Option      "dpms"
EndSection
```

Le seguenti entry sono usate comunemente nella sezione `Device`:

- `Identifier` — Specifica un nome unico per la sezione `Device`. Questa é una entry necessaria.

- `Driver` — Specifica quale driver deve essere caricato dal server X, in modo da utilizzare la scheda video. Un elenco dei driver puó essere trovato in `/usr/X11R6/lib/X11/Cards`, il quale viene installato con il pacchetto `hwdata`.
- `VendorName` — Un parametro facoltativo che specifica il produttore del monitor.
- `BoardName` — Un parametro facoltativo che specifica il nome della scheda video.
- `VideoRam` — Un parametro facoltativo che specifica la quantitá di RAM disponibile sulla scheda video in kilobytes. Questa impostazione é solo necessaria per le schede video alle quali il server X non puó rilevare la quantitá di RAM video.
- `BusID` — Una entry facoltativa che specifica la posizione del bus della scheda video. Questa opzione é solo necessaria per sistemi con schede multiple.
- `Screen` — Una entry facoltativa che specifica quale connettore monitor o testina sulla scheda video, la sezione `Device` puó configurare. Questa opzione é utile per schede video con testine multiple.

  Se monitor multipli sono collegati a testine diverse sulla stessa scheda video, allora devono esistere sezioni `Device` separate, e ogni sezione deve avere un valore `Screen` diverso.

  I valori per la entry `Screen` devono essere interi. Il primo testo sulla scheda video ha un valore pari a `0`. Il valore per ogni testo aggiuntivo aumenta questo valore di uno.
- `Option "<nome-opzione>"` — Una entry facoltativa che specifica i parametri aggiuntivi per la sezione. Sostituire *<nome-opzione>* con una valida opzione elencata per questa sezione nella pagina man `xorg.conf`.

  Una delle opzioni piú comuni é `"dpms"`, la quale attiva un 'Service Star energy compliance' per il monitor.

7.3.1.9. `Screen`

Ogni sezione `Screen` collega una scheda video (o testina della scheda video) a un monitor, riferendosi alla sezione `Device` e alla sezione `Monitor`. Poichè una sezione `Screen` é il minimo, istanze aggiuntive possono verificarsi per ogni combinazione scheda video e monitor presenti sulla macchina.

Il seguente esempio illustra una sezione `Screen` tipica:

```
Section "Screen"
 Identifier "Screen0"
 Device     "Videocard0"
 Monitor    "Monitor0"
 DefaultDepth     16
 SubSection "Display"
  Depth     24
  Modes    "1280x1024" "1280x960" "1152x864" "1024x768" "800x600" "640x480"
 EndSubSection
 SubSection "Display"
  Depth     16
  Modes    "1152x864" "1024x768" "800x600" "640x480"
 EndSubSection
EndSection
```

Leseguenti entry sono comunemente usate nella sezione `Screen`:

- `Identifier` — Specifica un nome unico per questa sezione `Screen`. Questa é una entry necessaria.
- `Device` — Specifica il nome unico di una sezione `Device`. Questa é una entry necessaria.
- `Monitor` — Specifica un nome unico di una sezione `Monitor`. Questa é una entry necessaria.

- `DefaultDepth` — Specifica l'intensitá del colore in bit. Nell'esempio precedente, `16`, il quale fornisce migliaia di colori, esso è il default. Sono permesse delle entry `DefaultDepth` multiple, ma è necessario inserirne almeno una.
- `SubSection "Display"` — Specifica le modalitá disponibili della schermata con una particolare intensitá di colore. Una sezione `Screen` puó avere sottosezioni `Display` multiple, ma almeno una sottosezione per la profonditá del colore specificato nella entry `DefaultDepth` è necessaria.
- `Option "<nome-opzione>"` — Una entry facoltativa che specifica i parametri aggiuntivi per la sezione. Sostituire *<nome-opzione>* con una valida opzione elencata per questa sezione nella pagina man `xorg.conf`.

7.3.1.10. DRI

La sezione facoltativa `DRI` specifica i parametri per il *Direct Rendering Infrastructure* (*DRI*). DRI é una interfaccia che permette alle applicazioni software 3D di avvantaggiarsi delle capacitá di accelerazione hardware 3D presenti in molti hardware video moderni. In aggiunta, DRI puó migliorare le prestazioni 2D tramite accelerazioni hardware, se supportate dal driver della scheda video.

Questa sezione viene ignorata a meno che DRI é abilitato nella sezione `Module`.

Di seguito viene riportato un esempio tipico di sezione `DRI`:

```
Section "DRI"
        Group         0
        Mode          0666
EndSection
```

Poichè diverse schede video usano DRI in modo diverso, non alterate i valori per questa sezione senza aver fatto riferimento a http://dri.sourceforge.net/.

7.4. Font

Red Hat Enterprise Linux usa due metodi per la gestione e la visualizzazione dei font con X. Il nuovo sottosistema font Fontconfig semplifica la gestione dei font, e fornisce contenuti di visualizzazione avanzati, come ad esempio anti-aliasing. Questo sistema é usato automaticamente per le applicazioni programmate usando il toolkit grafico Qt 3 o GTK+ 2.

Per compatibilitá, Red Hat Enterprise Linux include il sottosistema font originale, chiamato il sottosistema principale del font X. Questo sistema, il quale ha piú di 15 anni, é basato intorno all'*X Font Server* (*xfs*).

Questa sezione mostra come configurare i font per l'uso da parte di X dei due sistemi.

7.4.1. Fontconfig

Il sottosistema del font Fontconfig permette alle applicazioni di accedere direttamente i font sul sistema, e usare Xft o altri meccanismi per conferire ai font Fontconfig una caratteristica anti-aliasing avanzata. Applicazioni grafiche possono usare la libreria Xft con Fontconfig per riportare un testo sullo schermo.

Con l'andare del tempo, il sottosistema font Fontconfig/Xft, sostituirà il sottosistema principale del font X.

Importante

Il sottosistema del font Fontconfig non risulta essere funzionante con**OpenOffice.org** il quale usa la propria tecnologia font rendering.

É importante notare che Fontconfig usa il file di configurazione `/etc/fonts/fonts.conf`, e non dovrebbe essere modificato manualmente.

Suggerimento

A causa della transizione al nuovo sistema dei font, le applicazioni GTK+ 1.2 non vengono influenzate da alcun cambiamento fatto tramite il dialogo **Font Preferences** (il quale si puó accedere selezionando **Pulsante Menu principale** [sul pannello] => **Preferenze** => **Font**). Per queste applicazioni, un font puó essere configurato aggiungendo le seguenti righe al file `~/.gtkrc.mine`:

```
style "user-font" {

fontset = "<font-specification>"

}

widget_class "*" style "user-font"
```

Sostituire <*specificazione-font*> con una specificazione del font usato dalle applicazioni X tradizionali, come ad esempio `-adobe-helvetica-medium-r-normal--*-120-*-*-*-*-*-*`. Un elenco completo dei font principali puó essere ottenuto eseguendo `xlsfonts` o creandolo interattivamente usando il comando `xfontsel`.

7.4.1.1. Aggiunta di font a Fontconfig

Aggiungere nuovi font al sottosistema Fontconfig é un processo molto diretto.

1. Per poter aggiungere dei font, copiate i nuovi font nella directory `/usr/share/fonts/`. È consigliabile creare una nuova sottodirectory, come ad esempio `local/`, per poter distinguere tra i font di un utente e quelli installati per default.

   Per aggiungere i font ad un utente individuale, copiare i nuovi font nella directory `.fonts/` all'interno della home directory dell'utente.

2. Usare il comando `fc-cache` per aggiornare il cache delle informazioni del font, come riportato nel seguente esempio:

   `fc-cache <path-to-font-directory>`

   In questo comando, sostituire <*percorso-per-la directory-font*> con la directory contenente i nuovi font (`/usr/share/fonts/local/` o `/home/`<*utente*< `/.fonts/`).

Suggerimento

Gli utenti individuali possono anche installare i font in modo grafico, digitando `fonts:///` nella barra dell'indirizzo di **Nautilus**, trasportando li i nuovi file font.

Importante

Se il font file name termina con una estensione `.gz`, esso è compresso e non piú utilizzato fino a quando non viene decompresso. Per fare ció, usare il comando `gunzip` oppure fate un doppio clic sul file e trasportate il font in una directory in **Nautilus**.

7.4.2. Core X Font System

Per compatibilitá, Red Hat Enterprise Linux fornisce il sottosistema principale del font X, il quale usa l'X Font Server (`xfs`) per fornire i font per le applicazioni del client X.

Il server X và alla ricerca di font server specificati nella direttiva `FontPath` all'interno della sezione `Files` del file di configurazione `/etc/X11/xorg.conf`. Consultate la Sezione 7.3.1.4 per maggiori informazioni sulla entry `FontPath`.

Il server X si collega al server `xfs` su di una porta specificata, in modo da poter ottenere informazioni sui font. Per questa ragione, il servizio `xfs` deve essere in esecuzione in modo da effettuare l'avvio di X. Per maggiori informazioni su come configurare i servizi per un runlevel particolare, consultate il capitolo intitolato *Controllo dell'accesso ai servizi* nella *Red Hat Enterprise Linux System Administration Guide*.

7.4.2.1. Configurazione `xfs`

Lo script `/etc/rc.d/init.d/xfs` avvia il server `xfs`. Diverse opzioni possono essere configurate all'interno del suo file di configurazione, `/etc/X11/fs/config`.

Di seguito viene riportato un elenco delle opzioni più comuni:

- `alternate-servers` — Specifica un elenco di font server alternativi da usare se questo font server non é disponibile. Una virgola deve separare ogni font server nell'elenco.
- `catalogue` — Specifica un ordine dell'elenco dei percorsi font da usare. Una virgola deve separare ogni percorso font nell'elenco.

  Usare la riga `:unscaled` immediatamente dopo il percorso del font per far si che i font non proporzionati in quel percorso vengano caricati per primi. Successivamente specificare nuovamente l'intero percorso, in modo tale che altri font proporzionati vengano a loro volta caricati.
- `client-limit` — Specifica il numero massimo di client che il font server serve. Il default é `10`.
- `clone-self` — Permette al font server di clonare una nuova versione di se stesso quando il `client-limit` viene colpito. Per default, questa opzione é `on`.
- `default-point-size` — Specifica il default point size per qualsiasi font che non specifica questo valore. Il valore per questa opzione é impostato in decimi di punti. Il default di `120` corrisponde a 12 punti font.
- `default-resolutions` — Specifica un elenco di soluzioni supportate dal server X. Ogni risoluzione nell'elenco deve essere separata da una virgola.
- `deferglyphs` — Specifica se ritardare il caricamento di *glyphs* (il grafico usato per rappresentare visivamente un font). Per disabilitare questo contenuto per tutti i font, usare `all`, oppure per eseguire questo contenuto su font con soli 16-bit usare `16`.
- `error-file` — Specifica il percorso e il nome del file di una posizione dove gli errori `xfs` sono registrati.

- `no-listen` — Previene `xfs` dall'ascolto di protocolli particolari. Per default questa opzione é impostata su `tcp` per prevenire l'ascolto di `xfs` su porte TCP, tale procedura viene eseguita per ragioni di sicurezza.

Suggerimento

Se si usa `xfs` per servire i font attraverso la rete, rimuovere questa riga.

- `port` — Specifica la porta TCP sulla quale `xfs` effettua l'ascolto se `no-listen` non esiste oppure se non é commentato.
- `use-syslog` — Specifica se usare o meno il log di errore del sistema.

7.4.2.2. Aggiungere dei font a `xfs`

Per aggiungere font al sottosistema core X font (`xfs`), seguire le seguenti fasi:

1. Se non esiste giá, creare una directory chiamata `/usr/share/fonts/local/` usando il seguente comando come un utente root:
   ```
   mkdir /usr/share/fonts/local/
   ```
   Se é necessario creare la directory `/usr/share/fonts/local/`, essa deve essere aggiunta al percorso `xfs` usando il seguente comando come un utente root:
   ```
   chkfontpath --add /usr/share/fonts/local/
   ```
2. Copiare il nuovo file font nella directory `/usr/share/fonts/local/`
3. Aggiornare le informazioni del font emettendo il seguente comando come root:
   ```
   ttmkfdir -d /usr/share/fonts/local/ -o /usr/share/fonts/local/fonts.scale
   ```
4. Ricaricare il file di configurazione del font server `xfs` emettendo il seguente comando come un utente root:
   ```
   service xfs reload
   ```

7.5. Runlevel e X

Nella maggior parte dei casi, l'installazione di default di Red Hat Enterprise Linux configura una macchina in modo da avviarsi in un ambiente di login grafico, conosciuto come runlevel 5. É possibile, tuttavia, effettuare un avvio nella modalitá utenti multipli di solo testo, chiamata anche come runlevel 3 iniziando una sessione X da li.

Per maggiori informazioni sui runlevel, consultare la Sezione 1.4.

Le seguenti sottosezioni riportano il modo attraverso il quale X viene avviato sia nel runlevel 3 che nel runlevel 5.

7.5.1. Runlevel 3

Se vi trovate nel runlevel 3, il miglior modo di avviare una sessione X è quello di effettuare un login e digitare `startx`. Il comando `startx` è un front-end per il comando `xinit`, il quale lancia il server X (`Xorg`) e collega ad esso le applicazioni dei client X. Poichè l'utente ha già eseguito il login nel sistema all'interno del runlevel 3, `startx` non avvia il display manager o non effettua le autenticazioni degli utenti. Consultate la Sezione 7.5.2 per maggiori informazioni sui display manager.

Quando viene eseguito il comando `startx`, esso và alla ricerca di un file `.xinitrc` nella home directory dell'utente, in modo da definire l'ambiente desktop e possibilmente altri client X da eseguire. Se non è presente alcun file `.xinitrc`, viene utilizzato il file `/etc/X11/xinit/xinitrc` di default del sistema.

Lo script di default `xinitrc` cerca quindi i file definiti dall'utente e i file del sistema di default, includendo `.Xresources`, `.Xmodmap` e `.Xkbmap` nella home directory dell'utente, e i file `Xresources`, `Xmodmap` e `Xkbmap` nella directory `/etc/X11`. I file `Xmodmap` e `Xkbmap`, se presenti, sono usati dall'utility `xmodmap` per configurare la tastiera. Il file `Xresources` viene letto per assegnare valori di preferenza specifici alle applicazioni.

Una volta impostate queste opzioni, lo script `xinitrc` esegue gli script presenti in `/etc/X11/xinit/xinitrc.d`. Fra gli script più importanti contenuti in questa directory vi è `xinput`, che configura le impostazioni, per esempio la lingua di default da usare.

Successivamente, lo script `xinitrc` cerca di eseguire `.Xclients` nella home directory dell'utente, e si rivolge a `/etc/X11/xinit/Xclients` nel caso in cui il primo non fosse disponibile. Lo scopo del file `Xclients` è di avviare l'ambiente desktop o, se possibile, anche solo un window manager di base. Lo script `.Xclients` nella home directory dell'utente avvia l'ambiente desktop specificato dall'utente nel file `.Xclients-default`. Se `.Xclients` non è disponibile nella home directory dell'utente, lo script standard `/etc/X11/xinit/Xclients` cerca di avviare un altro ambiente desktop, prima con GNOME e successivamente con KDE seguito da `twm`.

L'utente viene riportato ad una sessione in modalitá di testo dopo aver abbandonato il runlevel 3.

7.5.2. Runlevel 5

Quando il sistema esegue un avvio nel runlevel 5, viene lanciata un'applicazione speciale del client X chiamata display manager. È necessario che un utente esegua l'autenticazione, utilizzando il display manager, prima di lanciare un ambiente desktop oppure un window manager.

A seconda degli ambienti desktop installati sul vostro sistema Red Hat Linux, sono disponibili tre diversi display manager per la gestione dell'autenticazione utente.

- `GNOME` — Il display manager di default per Red Hat Enterprise Linux, `GNOME` abilita l'utente a configurare le impostazioni della lingua, dello spegnimento, dell'avvio o di login nel sistema.
- `KDE` — Il display manager di KDE abilita l'utente allo spegnimento, al riavvio ed al log in nel sistema.
- `xdm` — Un display manager di base che permette all'utente di effettuare solo una registrazione nel sistema.

Quando si effettua l'avvio nel runlevel 5, lo script `prefdm` determina il display manager preferito riferendosi al file `/etc/sysconfig/desktop`. Un elenco delle opzioni per questo file è disponibile all'interno del file `/usr/share/doc/initscripts-<`*`numero-versione`*`>/sysconfig.txt` (dove < *`numero-versione`*> è il numero della versione del pacchetto `initscripts`).

I display manager fanno riferimento al file `/etc/X11/xdm/Xsetup_0` per impostare la schermata di registrazione. Effettuata la registrazione nel sistema, lo script `/etc/X11/xdm/GiveConsole` assegna all'utente la proprietà della console. Successivamente, lo script `/etc/X11/xdm/Xsession` entra in esecuzione per compiere molti dei compiti di cui si occupa in genere lo script `xinitrc` all'avvio di X nel runlevel 3, incluse le impostazioni del sistema e le risorse dell'utente, oltre all'esecuzione degli script nella directory `/etc/X11/xinit/xinitrc.d`.

I display manager `GNOME` e `KDE` consentono agli utenti di specificare quale ambiente desktop utilizzare durante l'autenticazione, selezionandolo dal menu **Sessioni** (si puó accedere selezionando **Pulsante menu principale** [sul pannello] => **Preferenze** => **Piú Preferenze** => **Sessioni**). Se l'ambiente desktop non è specificato nel display manager, lo script `/etc/X11/xdm/Xsession` controlla i file `.xsession` e `.Xclients` nella home directory dell'utente, per decidere quale ambiente desktop

deve essere caricato. Come ultima risorsa viene utilizzato il file `/etc/X11/xinit/Xclients`, per selezionare un ambiente desktop oppure un Window Manager da usare allo stesso modo del runlevel 3.

Quando l'utente termina una sessione X sul display predefinito (`:0`) abbandonandola, lo script `/etc/X11/xdm/TakeConsole` si avvia e assegna nuovamente la proprietà della console all'utente root. Il display manager originale, che è rimasto in esecuzione dopo la registrazione dell'utente, assume il controllo generando un nuovo display manager. Questo riavvia il server X, visualizza una nuova finestra di login e avvia ancora l'intero processo.

L'utente viene riportato al display manager dopo aver abbandonato X dal runlevel 5.

Per ulteriori informazioni relative al controllo dell'autenticazione degli utenti da parte del display manager, consultate /usr/share/doc/gdm-<*version-number*>/README (dove <*version-number*> é il numero della versione per il pacchetto `gdm` installato) e la pagina man di `xdm`.

7.6. Risorse aggiuntive

Vi sono ancora molte altre informazioni disponibili sul server X, sui client che si collegano ad esso, e sui vari window manager e ambienti desktop.

7.6.1. Documentazione installata

- `/usr/X11R6/lib/X11/doc/README` — descrive brevemente l'architettura XFree86 e fornisce ai nuovi utenti consigli su come reperire maggiori informazioni sul progetto XFree86.
- `/usr/X11R6/lib/X11/doc/README.Config` — Spiega le opzioni avanzate di configurazione per gli utenti della versione 3 di XFree86.
- `man xorg.conf` — Contiene delle informazioni sui file di configurazione `xorg.conf`, insieme con il significato e la sintassi delle diverse sezioni all'interno dei file.
- `man X.Org` — La pagina man primaria per informazioni sulla X.Org Foundation.
- `man Xorg` — Descrive X11R6.8 display server.

7.6.2. Siti Web utili

- http://www.X.org/ — La home page di X.Org Foundation, la quale fornisce la release X11R6.8 del sistema X Window. La suddetta release è presente con Red Hat Enterprise Linux per controllare l'hardware necessario e per fornire un ambiente GUI.
- http://xorg.freedesktop.org/ — La home page della release XR116.8, la quale è in grado di fornire dei binari ed una documentazione per il sistema X Window.
- http://dri.sourceforge.net/ — La home page del progetto DRI (Direct Rendering Infrastructure). Il DRI è il componente principale dell'accelerazione 3D hardware di X.
- http://www.redhat.com/mirrors/LDP/HOWTO/XFree86-HOWTO — Un documento HOWTO che spiega in modo dettagliato l'installazione manuale e la configurazione personalizzata di XFree86.
- http://www.gnome.org — Home page del progetto GNOME.
- http://nexp.cs.pdx.edu/fontconfig/ — La home del sottosistema font Fontconfig per X.

7.6.3. Libri correlati

- *The Concise Guide to XFree86 for Linux* di Aron Hsiao; Que — Fornisce la visione dell'operatività di XFree86 su sistemi Linux da un punto di vista professionale.
- *The New XFree86* di Bill Ball; Prima Publishing — Fornisce una buona panoramica generale di XFree86 e della sua interazione con i più diffusi ambienti desktop, quali GNOME e KDE.
- *Beginning GTK+ and GNOME* di Peter Wright; Wrox Press, Inc. — Introduce ai programmatori l'architettura di GNOME, mostrando loro come acquistare familiarità con GTK+.
- *GTK+/GNOME Application Development* di Havoc Pennington; New Riders Publishing — Uno sguardo approfondito nel cuore della programmazione GTK+, che dedica particolare attenzione ai codici campione e alle API disponibili.
- *KDE 2.0 Development* di David Sweet e Matthias Ettrich; Sams Publishing — Istruisce gli sviluppatori principianti e più esperti su come trarre vantaggio dalle istruzioni fontamentali per l'ambiente richieste per creare applicazioni QT per KDE.

II. Riferimento dei servizi di rete

È possibile impiegare una larga gamma di servizi di rete con Red Hat Enterprise Linux. Questa sezione descrive come vengono configurate le interfacce di rete, fornendo anche dei dettagli inerenti ai servizi critici di rete come ad esempio NFS, FTP, Server HTTP Apache, Sendmail, Postfix, Fetchmail, Procmail, BIND, e LDAP.

Sommario

8. Interfacce di rete 107
9. Network File System (NFS) 119
10. Server HTTP Apache 133
11. E-mail 169
12. BIND (Berkeley Internet Name Domain) 193
13. LDAP (Lightweight Directory Access Protocol) 213
14. Samba 225
15. FTP 251

Capitolo 8.

Interfacce di rete

Con Red Hat Enterprise Linux, tutte le comunicazioni di rete avvengono fra *interfacce* software configurate e *dispositivi di networking fisici* collegati al sistema.

I file di configurazione delle interfacce di rete e gli script che le attivano o disattivano, sono contenuti nella directory `/etc/sysconfig/network-scripts`. Anche se il numero ed il tipo dei file dell'interfaccia possono variare da sistema a sistema, sono presenti tre categorie di file in questa directory:

- *file di configurazione delle interfaccie*
- *script di controllo delle interfaccie*
- *file di funzione della rete*

I file, in ognuno di questa categoria, lavorano insieme per abilitare vari dispositivi di rete.

Questo capitolo spiega il rapporto esistente tra questi file e come essi vengono usati.

8.1. File di configurazione per la rete

Prima di trattare i file di configurazione delle interfacce, parleremo dei file di configurazione primari usati nella configurazione di rete. Comprendere l'importanza del ruolo di questi file nell'impostazione dello stack di rete, può essere utile per imparare a personalizzare al meglio un sistema Red Hat Enterprise Linux.

I file primary di configurazione di rete sono i seguenti:

- `/etc/hosts` —lo scopo principale di questo file è quello di risolvere gli hostname che non si possono risolvere in altro modo. Può anche essere utilizzato per risolvere gli hostname su piccole reti prive di server DNS. Indipendentemente dal tipo di rete su cui si trova il computer, questo file dovrebbe contenere una linea in cui è specificato l'indirizzo IP del dispositivo di loopback (`127.0.0.1`) come `localhost.localdomain`. Per maggiori informazioni, consultate la pagina man `hosts`.
- `/etc/resolv.conf` — Questo file specifica l'indirizzo IP dei server DNS e il dominio di ricerca. Se non configurato, questo file viene popolato dagli script di inizializzazione della rete. Per ulteriori informazioni su questo file, consultate la pagina man `resolv.conf`.
- `/etc/sysconfig/network` — Specifica le informazioni host e il routing per tutte le interfacce di rete. Per saperne di più su questo file e quali direttive esso accetta, consultate la Sezione 4.1.25.
- `/etc/sysconfig/network-scripts/ifcfg-<interface-name>` — Per ogni interfaccia di rete, vi è uno script di configurazione dell'interfaccia corrispondente. Ognuno di questi file fornisce informazioni specifiche in merito a una determinata interfaccia di rete. Per ulteriori dettagli su questo tipo di file e sulle direttive che accetta, consultate la Sezione 8.2.

Attenzione

La directory `/etc/sysconfig/networking/` viene usata da **Strumento di amministrazione di rete** (`system-config-network`) e il suo contenuto non dovrebbe essere modificato manualmente. In aggiunta qualsiasi utilizzo dello **Strumento di amministrazione di rete**, compreso il lancio dell'applicazione, annullerà qualsiasi direttiva precedentemente impostata in

`/etc/sysconfig/network-scripts`. È fortemente consigliato l'utilizzo di un solo metodo per la configurazione di rete per evitare così di cancellare la configurazione.

Per maggiori informazioni sulla configurazione delle interfacce di rete usando **Strumento di amministrazione di rete**, consultate il capitolo intitolato *Configurazione della rete* nella *Red Hat Enterprise Linux System Administration Guide*.

8.2. File di configurazione delle interfacce

I file di configurazione delle interfacce controllano il funzionamento di un determinato dispositivo di interfaccia di rete. All'avvio del sistema, Red Hat Linux utilizza i file per determinare quali interfacce attivare automaticamente e come configurarle in modo corretto. Solitamente, i file sono chiamati `ifcfg-<nome>`, dove <*nome*> si riferisce al nome del dispositivo controllato dal file di configurazione.

8.2.1. Interfacce Ethernet

Uno dei file più comuni è `ifcfg-eth0`, il quale controlla la prima *scheda di interfaccia di rete* o *NIC* nel sistema. Un sistema con più schede NIC contiene diversi file `ifcfg-eth` numerati. Poiché ogni dispositivo ha il proprio file di configurazione, l'utente può controllare da vicino il funzionamento di ogni singola interfaccia.

Di seguito viene riportato un esempio di un file `ifcfg-eth0` per un sistema che utilizza un indirizzo IP fisso:

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.1.0
NETMASK=255.255.255.0
IPADDR=10.0.1.27
USERCTL=no
```

I valori richiesti in un file di configurazione dell'interfaccia, possono variare in funzione di altri valori. Per esempio, il file `ifcfg-eth0` di un'interfaccia che utilizza DHCP è piuttosto diverso, a causa del fatto che le informazioni IP sono ora fornite dal server DHCP:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Lo **Strumento di amministrazione di rete** (`system-config-network`) rappresenta un modo semplice per apportare cambiamenti ai vari file di configurazione dell'interfaccia di rete (consultare il capitolo *Configurazione della rete* nel *Red Hat Enterprise Linux System Administration Guide* per istruzioni più dettagliate sull'uso di questo tool).

Potete anche modificare manualmente il file di configurazione per una determinata interfaccia di rete.

In ogni file di configurazione delle interfacce sono presenti i valori seguenti:

- `BOOTPROTO=`<*protocol*>, dove <*protocol*> è uno di questi:
  - `none` — non utilizzare alcun protocollo di avvio.
  - `bootp` — utilizzare il protocollo BOOTP.
  - `dhcp` — utilizzare il protocollo DHCP. utilizzare il protocollo DHCP.

- `BROADCAST=<indirizzo>`, dove `<indirizzo>` è l'indirizzo broadcast. Questa direttiva è stata disapprovata, in quanto il valore viene calcolato automaticamente con `ifcalc`.
- `DEVICE=<nome>`, dove `<nome>` è il nome del dispositivo fisico (tranne per i dispositivi PPP allocati dinamicamente, dove invece corrisponde al *nome logico*).
- `DHCP_HOSTNAME` — Usare questa opzione solo se il server DHCP richiede al client di specificare un hostname prima di ricevere un indirizzo IP. (Il demone del server DHCP in Red Hat Enterprise Linux non supporta questa caratteristica.)
- `DNS{1,2}=<indirizzo>`, dove `<indirizzo>` è l'indirizzo di un server dei nomi da inserire in `/etc/resolv.conf` qualora la direttiva `PEERDNS` sia impostata su `yes`.
- `ETHTOOL_OPTS=<options>`, dove `<options>` rappresenta qualsiasi delle opzioni specifiche al dispositivo supportato da `ethtool`. Per esempio, se desiderate forzare 100MB, duplex completo:
  `ETHTOOL_OPTS="autoneg off speed 100 duplex full"`

  Nota bene, se desiderate modificare le impostazioni duplex o la velocità, è quasi sempre necessario disabilitare autonegotiation con l'opzione `autoneg off`. Tale operazione deve essere fatta per prima, poichè le entry dell'opzione seguono l'ordine prestabilito.
- `GATEWAY=<indirizzo>`, dove `<indirizzo>` corrisponde all'indirizzo IP del router della rete o del dispositivo gateway (se presente).
- `HWADDR=<MAC-address>`, dove `<MAC-address>` è l'indirizzo hardware del dispositivo Ethernet nella forma di `AA:BB:CC:DD:EE:FF`. Questa direttiva è utile per le macchine con NIC multipli, per assicurare l'assegnazione corretta dei nomi del dispositivo alle interfacce, senza dare importanza all'ordine di caricamento configurato per ogni modulo NIC. Questa direttiva *non* deve essere usata insieme con `MACADDR`.
- `IPADDR=<indirizzo>`, dove `<indirizzo>` corrisponde all'indirizzo IP.
- `MACADDR=<MAC-address>`, dove `<MAC-address>` è l'indirizzo hardware del dispositivo Ethernet nella forma di `AA:BB:CC:DD:EE:FF`. Questa direttiva viene usata per sovrascrivere l'altra assegnata al NIC fisico. Questa direttiva *non* dovrebbe essere assegnata insieme con `HWADDR`.
- `MASTER=<bond-interface>`, dove `<bond-interface>` è l'interfaccia channel bonding alla quale è collegata l'interfaccia Ethernet.

  Questa direttiva è usata insieme con la direttiva `SLAVE`.

  Consultare la Sezione 8.2.3 per maggiori informazioni sulle interfacce channel bonding.
- `NETMASK=<mask>`, dove `<mask>` è il valore della maschera di rete.
- `NETWORK=<indirizzo>`, dove `<indirizzo>` è l'indirizzo della rete. Questa direttiva è stata deprecata, in quanto il valore viene calcolato automaticamente con `ifcalc`.
- `ONBOOT=<risposta>`, dove `<risposta>` è una delle seguenti:
  - `yes` — il dispositivo dovrebbe essere attivato all'avvio.
  - `no` — il dispositivo non dovrebbe essere attivato all'avvio.

- `PEERDNS=<risposta>`, dove `<risposta>` è una delle seguenti:
  - `yes` — Modifica `/etc/resolv.conf` se la direttiva DNS è stata impostata. Se state utilizzando DHCP, allora l'opzione `yes` è quella di default.
  - `no` — Non modificare `/etc/resolv.conf`.

- `SLAVE=<bond-interface>`, dove `<bond-interface>` è una dei seguenti:

- `yes` — Questo dispositivo è controllato dall'interfaccia channel bonding specificata nella direttiva `MASTER`.
- `no` — Questo dispositivo *non* è controllato dall'interfaccia channel bonding specificata nella direttiva `MASTER`.

Questa direttiva è usata insieme con la direttiva `MASTER`.

Consultare la Sezione 8.2.3 per maggiori informazioni sulle interfacce channel bond.

- `SRCADDR=<indirizzo>`, dove `<indirizzo>` è l'indirizzo IP sorgente specificato per i pacchetti in uscita.
- `USERCTL=<risposta>`, dove `<risposta>` è una delle seguenti:
  - `yes` — gli utenti non root sono autorizzati a controllare il dispositivo.
  - `no` — gli utenti non root non sono autorizzati a controllare il dispositivo.

8.2.2. Interfacce IPsec

Con Red Hat Enterprise Linux è possibile collegarsi ad altri host o reti usando un collegamento IP sicuro, conosciuto anche come IPsec. Per maggiori informazioni per l'IP sec usando lo **Strumento di amministrazione di rete**, (`system-config-network`), leggete il capitolo intitolato *Configurazione della rete*, che si trova nella *Red Hat Enterprise Linux System Administration Guide*. Per informazioni su come impostare manualmente IPsec, consultare il capitolo intitolato *Virtual Private Networks* nella *Red Hat Enterprise Linux Security Guide*.

Il seguente rappresenta il file `ifcfg` per un collegamento IPsec network-to-network per il LAN A. Il nome unico per identificare il collegamento in questo esempio è `ipsec1`, in questo modo il file risultante viene chiamato `/etc/sysconfig/network-scripts/ifcfg-ipsec1`.

```
TYPE=IPsec
ONBOOT=yes
IKE_METHOD=PSK
SRCNET=192.168.1.0/24
DSTNET=192.168.2.0/24
DST=X.X.X.X
```

Nell'esempio sopra riportato, `X.X.X.X` rappresenta l'indirizzo IP publicly routable del router IPsec di destinazione.

Di seguito viene riportato un elenco in ogni file di configurazione delle interfacce sono presenti i valori seguenti:

- `DST=<address>`, dove `<address>` è l'indirizzo IP del router o dell'host di destinazione IPsec. Questo viene usato per entrambe le configurazioni IPsec host-to-host e network-to-network.
- `DSTNET=<network>`, dove `<network>` è l'indirizzo della rete di destinazione IPsec. Viene usato solo per i collegamenti IPsec network-to-network.
- `SRC=<address>`, dove `<address>` è l'indirizzo IP del router o dell'host sorgente dell'IPsec. Questa impostazione è facoltativa e viene usata solo per i collegamenti IPsec host-to-host.
- `SRCNET=<network>`, dove `<tnetwork>` è l'indirizzo di rete della rete sorgente IPsec. Viene usato solo per collegamenti IPsec network-to-network.
- `TYPE=<interface-type>`, dove `<interface-type>` è `IPSEC`. Entrambe le applicazioni fanno parte del pacchetto `ipsec-tools`.

Consultate `/usr/share/doc/initscripts-<version-number>/sysconfig.txt` (sostituire `<version-number>` con il numero della versione del pacchetto `initscripts` installato) per i parametri di configurazione se usate la cifratura manuale della chiave insieme con IPsec.

Il demone di gestione della chiave IKEv1 di `racoon` tratta e configura un insieme di parametri per IPSec. È in grado di utilizzare delle chiavi pre-condivise, delle firme RSA, o GSS-API. Se viene usato `racoon` per gestire automaticamente la chiave di codifica, sono necessarie le seguenti opzioni:

- `IKE_METHOD=<encryption-method>`, dove `<encryption-method>` può essere `PSK`, `X509`, o `GSSAPI`. Se viene specificato `PSK`, anche il parametro `IKE_PSK` deve essere impostato. Se si specifica `X509`, bisogna impostare il parametro `IKE_CERTFILE`.
- `IKE_PSK=<shared-key>`, dove viene condiviso `<shared-key>`, un valore segreto per il metodo PSK (chiavi precondivise).
- `IKE_CERTFILE=<cert-file>`, dove `<cert-file>` è un file valido del certificato X.509 per l'host.
- `IKE_PEER_CERTFILE=<cert-file>`, dove `<cert-file>` è un file valido del certificato X.509 per l'host *remoto*.
- `IKE_DNSSEC=<answer>`, dove `<answer>` è `yes`. Il demone `racoon` riprende il certificato X.509 dell'host remoto tramite DNS. Se viene specificato un `IKE_PEER_CERTFILE`, *non* includere questo parametro.

Per maggiori informazioni sugli algoritmi disponibili per IPsec, consultare la pagina man `setkey`. Per maggiori informazioni su `racoon`, consultare le pagine man `racoon` e `racoon.conf`.

8.2.3. Interfacce Channel Bonding

Red Hat Enterprise Linux permette agli amministratori di unire le interfacce di rete multiple insieme in un singolo canale usando il modulo del kernel `bonding` e una interfaccia di rete speciale chiamata interfaccia channel bonding. Il channel bonding permette a due o più interfacce di agire come se fossero una unica interfaccia, aumentando simultaneamente la larghezza della banda fornendo così una ridondanza.

Per creare una interfaccia channel bonding, creare un file nella directory `/etc/sysconfig/network-scripts/` chiamato `ifcfg-bond<N>`, sostituendo `<N>` con il numero per l'interfaccia, come ad esempio `0`.

Il contenuto del file può essere identico a qualsiasi tipo di interfaccia alla quale ci si sta legando, come ad esempio una interfaccia Ethernet. La sola differenza è che la direttiva `DEVICE=` deve essere `bond<N>`, sostituendo `<N>` con il numero per l'interfaccia.

Il seguente è un esempio del file di configurazione channel bonding:

```
DEVICE=bond0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.1.0
NETMASK=255.255.255.0
IPADDR=10.0.1.27
USERCTL=no
```

Dopo aver creato l'interfaccia channel bonding, le interfacce di rete da unire devono essere configurate aggiungendo le direttive `MASTER=` e `SLAVE=` ai loro file di configurazione. I file di configurazione per ogni interfaccia channel bonded, possono essere quasi identici.

Per esempio, se il channel bonding unisce due interfacce Ethernet, `eth0` e `eth1` potrebbero somigliare al seguente esempio:

```
DEVICE=eth<N>
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
USERCTL=no
```

In questo esempio, sostituire *<N>* con il valore numerico per l'interfaccia.

Il modulo del Kernel deve essere caricato per far si che l'interfaccia channel bonding possa essere valida. Per assicurarsi che il modulo sia stato caricato quando si usa l'interfaccia channel bonding, aggiungere la seguente riga a `/etc/modules.conf`:

```
alias bond<N> bonding
```

Sostituire *<N>* con il numero dell'interfaccia, come ad esempio `0`. Per ogni interfaccia channel bonding configurata, ci dovrebbe essere una entry corrispondente in `/etc/modules.conf`.

Una volta configurato `/etc/modules.conf`, l'interfaccia channel bonding e le interfacce di rete, è necessario usare il comando `ifup` per ottenere l'interfaccia channel bonding.

Importante

Gli aspetti più importanti inerenti l'interfaccia channel bonding, vengono controllati attraverso il modulo del Kernel. Per maggiori informazioni su come controllare i moduli `bonding`, consultare la Sezione A.3.2.

8.2.4. File alias e cloni

Due tipi di file di configurazione delle interfacce meno usati sono *alias* e *clone*.

I file di configurazione dell'interfaccia Alias, i quali vengono usati principalmente per unire gli indirizzi multipli ad una singola interfaccia, usano, per il naming, il seguente schema:`ifcfg-<if-name>:<alias-value>`.

Per esempio, un file `ifcfg-eth0:0` può essere configurato in modo da specificare `DEVICE=eth0:0` e un indirizzo IP statico 10.0.0.2., servendo come alias di una interfaccia Ethernet già configurata per ricevere le proprie informazioni IP tramite DHCP in `ifcfg-eth0`. Con questa configurazione, il dispositivo `eth0` è legato a un indirizzo IP dinamico, ma la stessa scheda di rete fisica può ricevere delle richieste tramite l'indirizzo IP fisso 10.0.0.2.

Attenzione

Le interfacce alias non supportano DHCP.

Un file clone di configurazione dell'interfaccia, dovrebbe usare il seguente formato, `ifcfg-<if-name>-<clone-name>`. Mentre un file alias abilita indirizzi multipli per una interfaccia già esistente, un file clone viene usato per specificare le opzioni aggiuntive per una interfaccia. Per esempio, una interfaccia Ethernet DHCP standard chiamata `eth0`, potrebbe somigliare a quanto di seguito riportato:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
```

Poichè il valore di default per la direttiva `USERCTL` è `no`, se non specificata, gli utenti non possono attivare e disattivare l'interfaccia. Per dare agli utenti la possibilità di controllare l'interfaccia,create un clone copiando `ifcfg-eth0` in `ifcfg-eth0-user` e aggiungendo la riga seguente a `ifcfg-eth0-user`:

```
USERCTL=yes
```

In questo modo l'utente attiva l'interfaccia `eth0` con il comando `ifup eth0-user`, perchè le opzioni di configurazione di `ifcfg-eth0` e `ifcfg-eth0-user` vengono combinate. L'esempio riportato è molto semplice, questo metodo può essere usato con varie opzioni e interfacce.

Il modo più semplice di creare file di configurazione delle interfacce alias e cloni, consiste nell'usare il tool grafico **Strumento di amministrazione di rete**. Per maggiori informazioni su come utilizzare questo tool, consultate il capitolo *Configurazione della rete* nella *Red Hat Enterprise Linux System Administration Guide*.

8.2.5. Interfacce di dialup

Se vi collegate ad Internet tramite una connessione dialup, l'interfaccia avrà bisogno di un file di configurazione.

I file di interfaccia PPP sono chiamati usando il formato seguente `ifcfg-ppp<X>` (dove *<X>* è un numero unico che corrisponde ad un'interfaccia specifica).

Il file di configurazione dell'interfaccia PPP viene creato automaticamente quando si usa `wvdial`, **Strumento di amministrazione di rete** o **Kppp** per creare un account dialup. È possibile creare e modificare questo file manualmente.

I file `ifcfg-ppp0` hanno all'incirca questo aspetto:

```
DEVICE=ppp0
NAME=test
WVDIALSECT=test
MODEMPORT=/dev/modem
LINESPEED=115200
PAPNAME=test
USERCTL=true
ONBOOT=no
PERSIST=no
DEFROUTE=yes
PEERDNS=yes
DEMAND=no
IDLETIMEOUT=600
```

SLIP (Serial Line Internet Protocol) è un'altra interfaccia di dialup, sebbene il suo utilizzo sia meno frequente. I file SLIP hanno nomi di file di configurazione delle interfacce quali `ifcfg-sl0`.

Oltre a quelle già elencate, esistono altre opzioni da utilizzare con questi file:

- `DEFROUTE=`*<risposta>*, dove *<risposta>* è una delle seguenti:
  - `yes` — imposta l'interfaccia come quella di default.
  - `no` — non imposta l'interfaccia come quella di default.

- `DEMAND=`*<risposta>*, dove *<risposta>* è una delle seguenti:
  - `yes` — Questa interfaccia consente a `pppd` di avviare una connessione quando qualcuno tenta di usarlo.

  - `no` — per quest'interfaccia deve essere stabilita una connessione in modo manuale.

- `IDLETIMEOUT=<valore>`, dove `<valore>` corrisponde al numero di secondi di inattività che precede lo scollegamento dell'interfaccia.
- `INITSTRING=<stringa>`, dove `<stringa>` rappresenta la stringa di inizializzazione trasmessa al dispositivo del modem. L'opzione èessenzialmente usata con interfacce SLIP.
- `LINESPEED=<valore>`, dove `<valore>` è la frequenza di baud (baud rate) del dispositivo. I valori standard possibili sono `57600`, `38400`, `19200`, e `9600`.
- `MODEMPORT=<dispositivo>`, dove `<dispositivo>` corrisponde al nome del dispositivo seriale utilizzato per stabilire la connessione per l'interfaccia.
- `MTU=<valore>`, dove `<valore>` è il parametro *(MTU) Maximum Transfer Unit* dell'interfaccia. Il parametro MTU si riferisce al numero massimo di byte di dati che una struttura può trasportare, senza contare le sue informazioni di testo. In alcune situazioni di dialup, impostando il parametro su di un valore di `576` ne risulta in una perdita di pochi pacchetti con un leggero miglioramento sul rendimento per un collegamento.
- `NAME=<nome>`, dove `<nome>` è il riferimento al titolo attribuito a un insieme di configurazioni di connessione dialup.
- `PAPNAME=<nome>`, dove `<nome>` è il nome utente assegnato durante lo scambio di *Password Authentication Protocol(PAP)*, che avviene per abilitare i collegamenti ad un sistema remoto.
- `PERSIST=<risposta>`, dove `<risposta>` è una delle seguenti:
  - `yes` —l'interfaccia deve rimanere sempre attiva, anche dopo lo scollegamento del modem.
  - `no` — l'interfaccia non deve rimanere sempre attiva.

- `REMIP=<indirizzo>`, dove `<indirizzo>` è l'indirizzo IP del sistema remoto. Solitamente non è specificato.
- `WVDIALSECT=<nome>`, dove `<nome>` associa l'interfaccia alla configurazione del dialer in `/etc/wvdial.conf`, che contiene il numero telefonico da comporre e altre informazioni importanti per l'interfaccia.

8.2.6. Altre interfacce

Ecco riportati i file di configurazione più utilizzati per le interfacce:

- `ifcfg-lo` — Una *interfaccia di loopback* locale utilizzata per operazioni di controllo, e in molteplici applicazioni che richiedono un indirizzo IP in grado di indicare lo stesso sistema. Qualunque dato trasferito al dispositivo loopback, viene immediatamente ritornato al livello di rete dell'host.

  
  Avvertenza

  Non modificate mai lo script dell'interfaccia loopback `/etc/sysconfig/network-scripts/ifcfg-lo` manualmente. Facendo questo, il sistema operativo potrebbe non funzionare correttamente.

- `ifcfg-irlan0` — Una *interfaccia a infrarossi* consente il passaggio di informazioni tra dispositivi, come un laptop e una stampante, attraverso una connessione a infrarossi che funziona in modo simile ad un dispositivo Ethernet, ad eccezione del fatto che normalmente si verifica mediante una connessione peer-to-peer.

- `ifcfg-plip0` — Una connessione *Parallel Line Interface Protocol (PLIP)* funziona praticamente allo stesso modo di un dispositivo Ethernet, ad eccezione di un utilizzo diuna porta parallela.
- `ifcfg-tr0` — A causa di una grande diffusione di Ethernet, le topologie *Token Ring* non sono così diffuse sulle *Reti di area locale* (*LAN*) come erano una volta.

8.3. Script di controllo delle interfacce

Gli script di controllo delle interfacce attivano e disattivano le interfacce di sistema. Esistono due script primari di controllo delle interfacce, `/sbin/ifdown` e `/sbin/ifup`, che usano altri script di controllo contenuti nella directory `/etc/sysconfig/network-scripts`.

Gli script delle interfacce `ifdown` e `ifup` sono link simbolici per gli script contenuti nella directory `/sbin`. Quando viene chiamato uno di questi script, è necessario specificare un valore dell'interfaccia come ad esempio:

```
ifup eth0
```

Attenzione

Gli script delle interfacce `ifdown` e `ifup` sono i soli script che l'utente dovrebbe usare per attivare e disattivare le interfacce di rete.

I seguenti script sono usati solo come riferimento.

Due file usati per effettuare diversi compiti di inizializzazione della rete durante il processo di attivazione di una interfaccia di rete, sono `/etc/rc.d/init.d/functions` e `/etc/sysconfig/network-scripts/network-functions`. Consultare la Sezione 8.4 per maggiori informazioni.

Dopo aver verificato se è stata specificata una interfaccia e se l'utente che esegue la richiesta ha il permesso di controllare l'interfaccia, viene chiamato lo script idoneo che, in pratica, si occupa di attivare e disattivare l'interfaccia. Di seguito sono elencati gli script di controllo delle interfacce trovati all'interno della directory `/etc/sysconfig/network-scripts/`:

- `ifup-aliases` — configura gli alias IP dei file di configurazione delle interfacce quando più indirizzi IP sono associati all'interfaccia.
- `ifup-ippp` e `ifdown-ippp` — Vengono usate per attivare e disattivare le interfacce ISDN.
- `ifup-ipsec` and `ifdown-ipsec` — Usati per attivare o disattivare le interfacce IPsec.
- `ifup-ipv6` e `ifdown-ipv6` — Usati per attivare o disattivare le interfacce IPv6.
- `ifup-ipx` — Usato per attivare un'interfaccia IPX.
- `ifup-plip` — Usato per attivare un'interfaccia PLIP.
- `ifup-plusb` — Usato per attivare un'interfaccia USB per le connessioni di rete.
- `ifdown-post` e `ifup-post` — Contengono i comandi da eseguire dopo che un'interfaccia è stata attivata o disattivata.
- `ifup-ppp` and `ifdown-ppp` — Usati per attivare o disattivare un'interfaccia PPP.
- `ifup-routes` — Aggiunge instradamenti statici per un particolare dispositivo quando la sua interfaccia viene attivata.

- `ifdown-sit` e `ifup-sit` — Contiene le chiamate della funzione relativa all'attivazione e alla disattivazione del tunnel IPv6 all'interno di una connessione IPv4.
- `ifup-sl` e `ifdown-sl` — Usati per attivare o disattivare una interfaccia SLIP.
- `ifup-wireless` — Usato per attivare un'interfaccia di tipo wireless.

Avvertenza

Ricordate che in seguito alla rimozione o alla modifica degli script nella directory `/etc/sysconfig/network-scripts/` varie connessioni dell'interfaccia, possono agire in modo inaspettato. Pertanto solo utenti esperti possono modificare gli script relativi all'interfaccia della rete.

Il modo più facile per manipolare tutti gli script di rete contemporaneamente è di usare il comando `/sbin/service` sul servizio di rete (`/etc/rc.d/init.d/network`), come illustrato nel seguente comando:

```
/sbin/service network <action>
```

In questo esempio, <*azione*> può essere `start`, `stop`, o `restart`.

Per visualizzare un'elenco dei dispositivi configurati e che sono attualmente attivi sulle interfacce di rete, utilizzate il comando:

```
/sbin/service network status
```

8.4. File di funzione di rete

Red Hat Enterprise Linux utilizza diversi file che contengono funzioni comuni importanti, usati per attivare e disattivare le interfacce. Invece di forzare ogni file di controllo delle interfacce a contenere queste funzioni, esse sono riunite in alcuni file che possono essere utilizzati quando necessario.

Il file `/etc/sysconfig/network-scripts/network-functions` contiene le funzioni IPv4 più utilizzate, utili per molti script di controllo delle interfacce. Queste funzioni consentono di contattare i programmi in esecuzione che hanno richiesto informazioni sui cambiamenti nello stato di in una interfaccia, impostare gli hostname, trovare un dispositivo gateway, controllare se un dispositivo è attivo o inattivo e aggiungere un instradamento di default.

Poichè le funzioni richieste per le interfacce IPv6 sono diverse da quelle delle interfacce IPv4, esiste un file `/etc/sysconfig/network-scripts/network-functions-ipv6` che contiene tutte queste informazioni. Le funzioni di questi file possono configurare e cancellare gli instradamenti IPv6 statici, aggiungono e rimuovono i tunnel, aggiungono e rimuovono indirizzi IPv6 da una interfaccia e verificano l'esistenza di un indirizzo IPv6 in una interfaccia.

8.5. Risorse addizionali

Le seguenti risorse spiegano in modo più dettagliato le interfacce di rete.

8.5.1. Documentazione Installata

- `/usr/share/doc/initscripts-`<*versione*>`/sysconfig.txt` — Una guida alle opzioni disponibili per i file di configurazione della rete, comprese le opzioni IPv6, non trattate in questo capitolo.

- `/usr/share/doc/iproute-<versione>/ip-cref.ps` — Questo file contiene una ricca fonte di informazione sul comando `ip`, che può essere utilizzato anche per manipolare le tabelle di instradamento. Per consultare questo file, utilizzate **gg**vo **kghostview**.

Capitolo 9.

Network File System (NFS)

Un *Network File System* (*NFS*) consente di montare delle partizioni su un sistema remoto e utilizzarle come se fossero filesystem locali. Ció permette l'amministratore del sistema di immagazzinare le risorse in una posizione centrale sulla rete, garantendo agli utenti autorizzati la possibilità di accedervi costantemente.

In questo capitolo, vengono presentati solo i concetti fondamentali relativi a NFS, con l'aggiunta di qualche informazione supplementare; pertanto, se desiderate delle istruzioni specifiche circa la configurazione e il funzionamento di NFS su macchine client o server, dovrete consultare il capitolo *Network File System (NFS)* nella *Red Hat Enterprise Linux System Administration Guide*.

9.1. Come funziona

Al momento sono disponibili tre versioni di NFS. La versione 2 (NFSv2), che esiste già da alcuni anni, è ampiamente supportata. La versione 3 (NFSv3) offre alcune opzioni aggiuntive, come un file handling di lunghezza variabile e rapporti di errore più completi, ma non è completamente compatibile con i client di NFSv2. La versione 4 (NFSv4) include il Kerberos security, opera attraverso dei firewall e su Internet, non necessita più di portmapper, supporta le ACL, e utilizza delle operazioni di tipo stateful. Red Hat Enterprise Linux supporta le versioni dei client NFSv2, NFSv3 e client NFSv4, e durante l'esecuzione di un mounting tramite NFS, Red Hat Enterprise Linux utilizza NSFv4 per default in caso di connessione con un server che supporta tale versione.

Tutte le versioni di NFS possono usare *Transmission Control Protocol* (*TCP*) in esecuzione attraverso una rete IP, richiesto anche da NFSv4. NFSv2 e NFSv3 possono utilizzare *User Datagram Protocol* (*UDP*) in esecuzione attraverso una rete IP, in modo da fornire un collegamento di rete di tipo stateless tra il client ed il server.

Quando si utilizza con UDP NFSv2 o NFSv3, il collegamento UDP di tipo stateless in condizioni normali minimizza il traffico di rete, in quanto il server NFS invia un cookie al client dopo che lo stesso client viene autorizzato ad accedere al volume condiviso. Questo cookie è un valore casuale memorizzato dalla parte del server, viene trasmesso con le richieste RPC inviate dal client. Il server NFS può essere riavviato senza influenzare i client lasciando intatti il cookie. Tuttavia UDP è di tipo stateless, se il server si arresta inaspettatamente, i client UDP continuano a saturare la rete con delle richieste per il server. Per questa ragione, TCP è il protocollo preferito quando ci si collega ad un server NFS.

Quando si utilizza NFSv4, si viene a creare un collegamento di tipo stateless, e l'autenticazione dell'utente e del gruppo di Kerberos, insieme ad alcuni livelli di sicurezza, vengono resi disponibili in modo facoltativo. NFSv4 non presenta alcuna interazione con portmapper, `rpc.mountd`, `rpc.lockd`, e `rpc.statd`, poichè essi sono stati trasferiti all'interno del kernel. NFSv4 è in ascolto sulla porta TCP 2049.

Nota Bene

Con Red Hat Enterprise Linux, per default, UDP è il protocollo di trasporto per NFS. Consultate il capitolo intitolato *Network File System (NFS)* nella *Red Hat Enterprise Linux System Administration Guide* per maggiori informazioni sul collegamento ai server NFS usando TCP. UDP può essere usato a scopo di compatibilità se necessario, ma un suo uso esteso è deprecato.

NFS effettua l'autenticazione solo quando un sistema client cerca di eseguire un montaggio della risorsa NFS condivisa. Per limitare l'accesso al servizio NFS, vengono usati i wrappers TCP, i quali leggono i file `/etc/hosts.allow` e `/etc/hosts.deny` per stabilire se concedere o negare a un determinato client l'accesso al server NFS. Per maggiori informazioni su come configurare i controlli di accesso con wrapper TCP, consultate il Capitolo 17.

Una volta passati i wrapper TCP da parte del client, il server NFS fa riferimento al suo file di configurazione, `/etc/exports`, per determinare se il client possiede i privilegi minimi necessari per montare i filesystem esportati. Dopo aver autorizzato l'accesso, tutte le operazioni di file e directory sono disponibili per l'utente.

Avvertenza

Se si utilizza NFSv2 oppure NFSv3, i quali non supportano l'autenticazione di Kerberos, i privilegi di montaggio NFS vengono garantiti al client host e non all'utente. Quindi, i filesystem esportati sono accessibili da un utente su di un client host con permessi di accesso. Quando si configurano le condivisioni NFS, fate molta attenzione su quale host ottenere i permessi di lettura/scrittura (`rw`).

Importante

Per far funzionare correttamente NFS con una installazione di default di Red Hat Enterprise Linux, con firewall abilitati, è necessario configurare IPTables insieme con la porta 2049 TCP di default.

Lo script di inizializzazione di NFS ed il processo `rpc.nfsd`, abilitano ora il processo di binding a qualsiasi porta specificata durante l'avvio del sistema. Tuttavia tale processo potrebbe essere propenso ad errori, se tale porta risulta non disponibile, oppure se si verifica un conflitto con un altro demone.

9.1.1. Servizi richiesti

Per permettere la condivisione dei file NFS, Red Hat Enterprise Linux utilizza un supporto a livello kernel combinato con una serie di processi del demone. NFSv2 e NFSv3 si affidano al *Remote Procedure Calls* (*RPC*), per codificare e decodificare le richieste tra i client ed i server. I servizi RPC con Linux sono controllati dal servizio `portmap`. Per condividere o montare i filesystem NFS, i seguenti servizi funzionano insieme, a seconda di quale versione di NFS è stata implementata:

- `nfs` — Inizia i processi RPC appropriati per le richieste del servizio per i filesystem NFS condivisi.
- `nfslock` — Un servizio facoltativo che inizia i processi RPC appropriati, per abilitare i client NFS ad eseguire un bloccaggio dei file sul server.
- `portmap` — Il servizio RPC, per Linux, risponde alle richieste per i servizi RPC e imposta i collegamenti per il servizio RPC richiesto. Con NFSv4 tale procedura non viene utilizzata.

I seguenti processi RPC lavorano insieme per facilitare i servizi NFS:

- `rpc.mountd` — Questo processo riceve la richiesta di montaggio da un client NFS e verifica se il filesystem richiesto è stato esportato. Viene iniziato automaticamente dal servizio `nfs` e non richiede una configurazione da parte dell'utente. Tale procedura non viene utilizzata con NFSv4.
- `rpc.nfsd` — Questo processo implementa il server NFS. Funziona con il kernel di Linux per soddisfare le richieste dinamiche dei client NFS, come per esempio l'aggiunta di thread del server ogni qualvolta che si collega un client NFS. Questo processo corrisponde al servizio `nfs`.

- `rpc.lockd` — Un processo facoltativo che permette ai client NFS di bloccare i file presenti sul server. Questo processo corrisponde al servizio `nfslock`. Tale procedura non viene utilizzata con NFSv4.
- `rpc.statd` — Questo processo implementa il protocollo RPC *Network Status Monitor (NSM)*, il quale notifica ai client NFS quando un server NFS viene riavviato in seguito ad uno spegnimento non corretto. Questo processo viene avviato automaticamente dal servizio `nfslock` e non richiede una configurazione da parte dell'utente. Tale procedura non viene utilizzata con NFSv4.
- `rpc.rquotad` — Questo processo fornisce le informazioni sulla user quota per gli utenti remoti. Viene iniziato automaticamente dal servizio `nfs` e non necessita della configurazione da parte dell'utente.
- `rpc.idmapd` — Questo processo fornisce il client NFSv4 e le chiamate server, le quali eseguono la mappatura tra i nomi NFSv4 di tipo on-the-wire (i quali rappresentano delle stringhe sotto forma di user@domain), e gli UID e GID locali. Per un funzionamento corretto di `idmapd` con NFSv4, è necessario configurare `/etc/idmapd.conf`. Questo servizio è necessario con NFSv4.
- `rpc.svcgssd` — Questo processo fornisce il meccanismo di trasporto del server per il processo di autenticazione (Versione 5 di Kerberos) con NFSv4. Questo servizio è necessario con NFSv4.
- `rpc.gssd` — Questo processo fornisce il meccanismo di trasporto del client per il processo di autenticazione (Versione 5 di Kerberos) con NFSv4. Questo servizio è necessario con NFSv4.

9.1.2. NFS e `portmap`

Nota Bene

La seguente sezione viene applicata solo alle implementazioni NFSv2 o NFSv3, che necessitano del servizio `portmap` per una backward compatibility.

Il servizio `portmap` è necessario per mappare le richieste RPC ai servizi corretti. I processi RPC notificano al `portmap` il proprio avvio, rivelando il numero della porta che stanno monitorando e quali numeri di programmi RPC sono pronti a servire. Il sistema client poi contatta `portmap` sul server con un particolare numero di programma RPC. A questo punto, il servizio `portmap` reindirizza il client al numero di porta corretto perché possa comunicare con il servizio desiderato.

Dal momento che i servizi basati su RPC si affidano al `portmap` per effettuare tutte le connessioni con le richieste in ingresso dei client, è chiaro che `portmap` deve essere disponibile prima che i servizi di cui sopra siano avviati.

Il servizio `portmap` utilizza i wrappers TCP per il controllo dell'accesso, e le regole del controllo all'accesso per `portmap` influenzano *tutti* i servizi basati su RPC. Alternativamente, potete specificare a quale demone RPC di NFS applicare una determinata regola. Le pagine man relative a `rpc.mountd` e `rpc.statd` contengono informazioni sulla sintassi precisa di queste regole.

9.1.2.1. Troubleshooting NFS e `portmap`

Poiché `portmap` serve a coordinare i servizi RPC con i numeri di porta utilizzati per comunicare tra loro, può essere utile visualizzare lo stato dei servizi RPC correnti, utilizzando `portmap` nelle operazioni di troubleshooting. Il comando `rpcinfo` mostra ogni singolo servizio RPC con accanto il suo numero di porta, il numero di programma RPC, la versione ed il tipo di protocollo IP (TCP o UDP).

Se volete accertarvi che i servizi RPC di NFS corretti siano abilitati per il `portmap`, emettere il seguente comando come root:

```
rpcinfo -p
```

Quanto segue è un esempio di output del seguente comando:

```
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100021    1   udp  32774  nlockmgr
    100021    3   udp  32774  nlockmgr
    100021    4   udp  32774  nlockmgr
    100021    1   tcp  34437  nlockmgr
    100021    3   tcp  34437  nlockmgr
    100021    4   tcp  34437  nlockmgr
    100011    1   udp    819  rquotad
    100011    2   udp    819  rquotad
    100011    1   tcp    822  rquotad
    100011    2   tcp    822  rquotad
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100005    1   udp    836  mountd
    100005    1   tcp    839  mountd
    100005    2   udp    836  mountd
    100005    2   tcp    839  mountd
    100005    3   udp    836  mountd
    100005    3   tcp    839  mountd
```

Osservando l'output di questo comando, si nota che i servizi NFS corretti sono in esecuzione. Se uno dei servizi NFS non si avvia in modo corretto, `portmap` non sarà in grado di mappare sulla porta corretta, le richieste RPC dei client relative a quel servizio. In molti casi, se NFS non è presente nell'output `rpcinfo`, il riavvio di NFS causa la corretta registrazione del servizio con `portmap`, con un consequente avvio delle sue funzioni. Per informazioni su come iniziare NFS, consultare la Sezione 9.2.

Altre utili opzioni sono disponibili per il comando `rpcinfo`. Consultate la pagina man per maggiori informazioni.

9.2. Come avviare e arrestare NFS

Per eseguire un server NFS, il servizio `portmap` deve essere in esecuzione. Per verificare che `portmap` è attivo, digitare il seguente comando come utente root:

```
/sbin/service portmap status
```

Se il servizio `portmap` è in esecuzione, il servizio `nfs` potrà essere avviato. Per avviare un server NFS, digitare come utente root:

```
/sbin/service nfs start
```

Per arrestare il server, digitare come utente root:

```
/sbin/service nfs stop
```

L'opzione `restart` rappresenta un modo semplice su come arrestare e avviare NFS. Questo è il modo più efficiente per confermare i cambiamenti sulla configurazione dopo aver modificato il file di configurazione per NFS.

Per riavviare il server, digitare come root:

```
/sbin/service nfs restart
```

L'opzione `condrestart` (*conditional restart*) avvia `nfs` solo se è in esecuzione. Questa opzione è utile anche per gli script, in quanto non avvia il demone se non è in esecuzione.

Per riavviare il server in modo condizionato, digitare come root:

```
/sbin/service nfs condrestart
```

Per ricaricare il file di configurazione del server NFS senza riavviare il servizio, digitare come utente root:

```
/sbin/service nfs reload
```

Per default, il servizio `nfs` *non* si avvia automaticamente al momento dell'avvio. Per configurare NFS in modo da avviarsi al momento dell'avvio, usare una utility initscript come ad esempio `/sbin/chkconfig`, **/sbin/ntsysv**, o il programma **Strumento di configurazione dei servizi**. Consultare il capitolo *Controllo dell'accesso ai servizi* in *Red Hat Enterprise Linux System Administration Guide* per maggiori informazioni su questi tool.

9.3. Configurazione del server NFS

Sono presenti tre modi per configurare un server NFS con Red Hat Enterprise Linux: usare lo **Strumento di configurazione del server NFS** (`system-config-nfs`), modificare manualmente il suo file di configurazione (`/etc/exports`), o usare il comando `/usr/sbin/exportfs`.

Per informazioni sull'uso dello **Strumento di configurazione del server NFS**, consultate il capitolo intitolato *Network File System (NFS)* nella *Red Hat Enterprise Linux System Administration Guide*. In questa sezione si affrontano la modifica manuale di `/etc/exports` e l'uso del comando `/usr/sbin/exportfs` per esportare i file system NFS.

9.3.1. Il file di configurazione `/etc/exports`

Il file `/etc/exports` controlla verso quali host remoti vengono esportati determinati filesystem, specificando altresì particolari opzioni. Le linee vuote vengono ignorate, i commenti si possono eseguire usando il carattere (`#`), e le linee lunghe possono essere spezzate con il carattere (`\`).Ogni filesystem esportato dovrebbe avere la propria linea. Gli elenchi degli host autorizzati posti dopo un filesystem esportato devono essere separati tra loro da uno spazio. Le opzioni relative a ciascun host devono essere poste tra parentesi direttamente (ovvero senza spazi di separazione) dopo l'identificatore dell'host.

Una riga per i filesystem esportati ha la seguente struttura:

```
<export> <host1>(<options>) <hostN>(<options>)...
```

In questa struttura, sostituire *<export>* con la directory esportata, sostituire *<host1>* con l'host o la rete sulla quale è stata condivisa l'esportazione, e sostituire *<options>* con le opzioni per l'host o per la rete. Host aggiuntivi possono essere specificati in un elenco separato da uno spazio.

I seguenti metodi possono essere usati per specificare gli host name:

- *host singolo* — viene specificato un particolare host con un nome di dominio completamente qualificato, un hostname o un indirizzo IP.

- *wildcards* — Dove un asterisco `*`o un punto interrogativo `?` vengono utilizzati per prendere in considerazione un raggruppamento di nomi del dominio completamente qualificato, corrispondenti ad una riga particolare di lettere. Le Wildcard non devono essere usate con gli indirizzi IP; tuttavia, è possibile che possano funzionare in modo accidentale se il bloccaggio DNS inverso non và a buon fine.

  Tuttavia, fate attenzione utilizzando le wildcard con i nomi del dominio, poiché esse tendono a essere più precisi di quanto si pensi. Per esempio, l'uso di `*.example.com` come wildcard, consentirà al dominio sales.example.com di accedere al filesystem esportato, mentre non lo permetterà a bob.sales.example.com. Per far corrispondere entrambe le possibilità, specificare `*.example.com` e `*.*.example.com`.

- *reti IP* — Consente di far corrispondere gli host sulla base dei loro indirizzi IP all'interno di una rete più ampia. Per esempio, `192.168.0.0/28` permette ai primi 16 indirizzi IP, dal 192.168.0.0 al 192.168.0.15, di accedere al filesystem esportato, mentre non lo consente all'indirizzo 192.168.0.16 e seguenti.

- *netgroups* — Permette l'utilizzo di un nome netgroup NIS, scritto come `@<group-name>`. In questo modo, il server NIS diventa effettivamente responsabile del controllo degli accesi a questo filesystem esportato; si possono aggiungere e rimuovere utenti da un gruppo NIS senza intaccare `/etc/exports`.

Nella sua forma più semplice, `/etc/exports` specifica solo la directory esportata e gli host abilitati all'accesso, come nel seguente esempio:

```
/exported/directory bob.example.com
```

Nell'esempio, `bob.example.com` può montare `/exported/directory/`. Poichè non viene specificata alcuna opzione in questo esempio, verranno usate le seguenti opzioni NFS di default:

- `ro` — I file system esportati sono di sola lettura. Gli host remoti non saranno in grado di modificare i dati condivisi sul file system. Per consentire agli host di apportare delle modifiche al file system, dovete specificare l'opzione lettura/scrittura (`rw`).
- `wdelay` — Consente al server NFS di posticipare un salvataggio su disco nel caso sospetti l'arrivo imminente di un'altra richiesta di scrittura. Questo può accrescere le prestazioni riducendo il numero di volte in cui comandi di scrittura diversi devono accedere al disco. Utilizzate `no_wdelay` per disattivare questa opzione, che funziona solo se state utilizzando l'opzione `sync`.
- `root_squash` — Fa in modo che tutti gli accessi dei client al filesystem esportato, effettuati da utenti root sulle macchine client, avvengano come user ID per l'utente `nobody`. Questo in effetti "declassa" il potere dell'utente root remoto a quello del più semplice utente locale, impedendo una alterazione dei file non autorizzata sul server remoto. In alternativa, l'opzione `no_root_squash` disabilita questa funzione. Per applicare l'opzione di squash a tutti gli utenti remoti, compreso l'utente root, dovete usare l'opzione `all_squash`. Per specificare gli ID utente e di gruppo da utilizzare per gli utenti remoti da un particolare host, servitevi rispettivamente delle opzioni `anonuid` e `anongid`. In questo modo, potete creare uno speciale account utente per consentire agli utenti remoti di NFS di condividere e specificare `(anonuid=`*`<valore-uid>`*`,anongid=`*`<valore-gid>`*`)`, dove il *`<valore-uid>`* rappresenta il numero dell'ID utente e il *`<valore-gid>`* rappresenta il numero dell'ID di gruppo.

Importante

Per default, le *access control lists* (*ACL*) sono supportate da NFS sotto Red Hat Enterprise Linux. Per disabilitare questa caratteristica, specificare l'opzione `no_acl` quando si esegue l'esportazione del file system. Per saperne di più, consultate il capitolo intitolato *Network File System (NFS)* nella *Red Hat Enterprise Linux System Administration Guide*.

Ogni valore di default per il file system esportato deve essere sovrascritto in modo esplicito. Per esempio, se l'opzione `rw` non viene specificata, allora il file system esportato viene condiviso come di sola lettura. La seguente rappresenta un esempio di riga da `/etc/exports`, la quale sovrascrive due opzioni di default:

```
/another/exported/directory 192.168.0.3(rw,sync)
```

In questo esempio `192.168.0.3` può montare `/another/exported/directory/` in modo lettura/scrittura e tutto ciò che viene trasferito sul disco, viene confermato prima che la richiesta di scrittura del client venga completata.

Inoltre, sono disponibili altre opzioni in caso non sia presente alcun valore di default. Inoltre includono la capacità di disabilitare i controlli sui sottoalberi, il permesso di accedere da porte non sicure e di bloccare i file in modo non sicuro (procedura necessaria per certe implementazioni dei client NFS meno recenti). Per maggiori dettagli su queste opzioni meno usate e meno diffuse, consultate la pagina man relativa a `exports`.

Avvertenza

Il modo in cui viene formattato il file `/etc/exports` è molto importante, soprattutto per quanto riguardo l'uso degli spazi. Ricordatevi sempre di separare con uno spazio i filesystem esportati dagli host e gli host tra di loro. Non ci devono però essere altri spazi nel file, a parte quelli eventualmente usati nelle linee di commento.

Per esempio, le due linee seguenti non hanno lo stesso significato:

```
/home bob.example.com(rw)
/home bob.example.com (rw)
```

La prima linea abilita i soli utenti di `bob.example.com` ad accedere nella directory `/home` in modalità lettura/scrittura. La seconda riga permette agli utenti di `bob.example.com` di montare la directory in sola lettura (configurazione di default), mentre tutti gli altri possonomontarla in modalità lettura/scrittura.

Per maggiori informazioni su come configurare un server NFS modificando `/etc/exports`, consultate il capitolo intitolato *Network File System (NFS)* nella *Red Hat Enterprise Linux System Administration Guide*.

9.3.2. Il comando `exportfs`

Tutti i filesystem esportati verso utenti remoti tramite NFS, insieme al livello di accesso per i suddetti file system, sono elencati nel file `/etc/exports`. Quando si avvia il servizio `nfs`, il comando `/usr/sbin/exportfs` lancia e legge questo file, passa il controllo a `rpc.mountd` (se NFSv2 o NFSv4) per il processo di montaggio, e successivamente a `rpc.nfsd` dove i filesystem vengono resi disponibili agli utenti remoti.

Quando emesso manualmente, il comando `/usr/sbin/exportfs` permette agli utenti root, di selezionare le directory da esportare o meno senza dover riavviare i vari servizi di NFS. Quando vengono passate le opzioni corrette, il comando `/usr/sbin/exportfs` salva i file system esportati su `/var/lib/nfs/xtab`. Poiché `rpc.mountd` si rivolge al file `xtab` nel decidere i privilegi di accesso ad un filesystem, le modifiche all'elenco dei filesystem esportati hanno effetto immediato.

Il seguente è un elenco delle opzioni più usate, disponibile per `/usr/sbin/exportfs`:

- `-r` — Fa sì che tutte le directory elencate in `/etc/exports` vengano esportate mediante la creazione di un nuovo elenco export in `/etc/lib/nfs/xtab`. Questa opzione aggiorna in modo effettivo l'elenco delle esportazioni in base alle modifiche apportate a `/etc/exports`.

- `-a` — Seleziona quali directory esportare e quali no, in base alle altre opzioni scelte per `/usr/sbin/exportfs`. Se non vengono specificate altre opzioni, `/usr/sbin/exportfs` esporta tutti i file system specificati in `/etc/exports`.
- `-o` *`file-systems`* — Permette all'utente di specificare le directory da esportare non presenti nell'elenco di `/etc/exports`. Sostituire *`file-systems`* con file system aggiuntivi da esportare. Questi file system devono essere formattati nello stesso modo in cui vengono specificati in `/etc/exports`. Consultate la Sezione 9.3.1 per maggiori informazioni sulla sintassi `/etc/exports`. Questa opzione viene usata spesso per provare un file system esportato, prima di aggiungerlo in modo permanente all'elenco dei file system da esportare.
- `-i` — Ignora `/etc/exports`; solo le opzioni fornite dalla linea di comando vengono usate per definire i file system esportati.
- `-u` — Non esporta tutte le directory condivise. Il comando `/usr/sbin/exportfs -ua` sospende la condivisione NFS dei file, mentre mantiene attivi i vari demoni. Per riprendere la condivisione in NFS, digitate `exportfs -r`.
- `-v` — Operazioni complesse: i filesystem da esportare o da non esportare vengono visualizzati molto più nel dettaglio quando viene eseguito il comando `exportfs`.

Se non viene fornita alcuna opzione al comando `/usr/sbin/exportfs`, visualizza un elenco degli attuali file system esportati.

Per maggiori informazioni sul comando `/usr/sbin/exportfs`, consultare la pagina man `exportfs`.

9.3.2.1. Utilizzo del comando `exportfs` con NFSv4

Poichè NFSv4 non utilizza più il protocollo `rpc.mountd` utilizzato in NFSv3 e NFSv3, il montaggio dei filesystem è stato modificato.

Un client NFSv4 possiede ora l'abilità di visualizzare tutte le esportazioni servite dal server NFSv4, come filesystem singolo e chiamate pseudo-file system NFSv4. Su Red Hat Enterprise Linux, lo pseudo-filesystem viene identificato come un filesystem singolo, identificato con l'opzione `fsid=0`.

Per esempio, è possibile eseguire i seguenti comandi su di un server NFSv4:

```
mkdir /exports
mkdir /exports/opt
mkdir /exports/etc
mount --bind /usr/local/opt /exports/opt
mount --bind /usr/local/etc /exports/etc
exportfs -o fsid=0,insecure,no_subtree_check gss/krb5p:/exports
exportfs -o rw,nohide,insecure,no_subtree_check gss/krb5p:/exports/opt
exportfs -o rw,nohide,insecure,no_subtree_check gss/krb5p:/exports/etc
```

In questo esempio vengono forniti ai client una serie di filesystem multipli da montare, utilizzando l'opzione `--bind`.

9.4. File di configurazione del client NFS

Le condivisioni NFS vengono montate da parte del client usando il comando `mount`. Il formato del comando è il seguente:

`mount -t <`*`nfs-type`*`> -o <`*`options`*`> <`*`host`*`>:<`*`/remote/export`*`> <`*`/local/directory`*`>`

Sostituire <*`nfs-type`*> con `nfs` per server NFSv2 o NFSv3, oppure `nfs4` per server NFSv4.Sostituire <*`options`*> con un elenco di opzioni separato da una virgola per il file system

NFS (consultate la Sezione 9.4.3 per maggiori informazioni). Sostituire *<host>* con l'host remoto, *</remote/export>* con la directory remota montata, e sostituire *</local/directory>* con la directory locale dove il file system remoto deve essere montato.

Consultare la pagina man `mount` per maggiori informazioni.

Se si accede ad una condivisione NFS emettendo manualmente il comando `mount`, il file system deve essere rimontato manualmente dopo il riavvio del sistema. Red Hat Enterprise Linux offre due modi per il montaggio automatico dei file system remoti al momento dell'avvio: il file `/etc/fstab` o il servizio `autofs`.

9.4.1. `/etc/fstab`

Il servizio `netfs` al momento dell'avvio, fa riferimento al file `/etc/fstab`, in questo modo le righe che si riferiscono alle condivisioni NFS, hanno lo stesso effetto come se si digitasse manualmente il comando `mount` durante il processo di avvio.

Un esempio di linea `/etc/fstab` per montare una esportazione NFS, ha il seguente aspetto:

<server>:*</remote/export>* *</local/directory>* *<nfs-type>* *<options>* 0 0

Sostituire *<server>* con l'hostname, l'indirizzo IP o con il nome del dominio completamente qualificato del server che esporta il file system.

Sostituire *</remote/export>* con il percorso per la directory esportata.

Sostituire *</local/directory;>* con il file system locale sul quale è montata la directory esportata. Questo mount point deve esistere già prima che il file `/etc/fstab` venga letto, altrimenti l'operazione di montaggio è destinata a fallire.

Sostituire *<nfs-type>* con `nfs` per server NFSv2 o NFSv3, oppure con `nfs4` per server NFSv4.

Sostituire *<options>* con un elenco, separato da una virgola, delle opzioni per il file system NFS (consultare la Sezione 9.4.3 per maggiori informazioni). Consultare la pagina man `fstab` per informazioni aggiuntive.

9.4.2. `autofs`

Uno degli effetti collaterali nell'utilizzo del file `/etc/fstab` è rappresentato dal fatto che, a prescindere da quanto utilizziate il file system NFS montato, il vostro sistema deve comunque dedicare parte delle sue risorse per mantenerlo in funzione. Se sul sistema sono montati solo un paio di file system, il problema non è così grave; se però il sistema deve mantenere contemporaneamente in funzione decine di file system, le prestazioni generali possono risentirne. In alternativa al file `/etc/fstab` potete usare `automount`, una utility basata su kernel che monta e smonta automaticamente i filesystem NFS, riducendo il consumo di risorse.

Il servizio `autofs` viene utilizzato per controllare il comando `automount` attraverso il file di configurazione primario `/etc/auto.master`. Mentre `automount` può essere specificato sulla linea di comando, è più opportuno specificare i mount point, l'hostname, la directory esportata e le opzioni all'interno di un gruppo di file, invece di digitare il tutto manualmente.

I file di configurazione di `autofs` sono organizzati secondo un rapporto genitore-figlio. Un file di configurazione principale (`/etc/auto.master`) elenca i mount point sul sistema, che sono collegati a un particolare *tipo di mappa*, che assume la forma di altri file di configurazione, programmi, mappe NIS e altri metodi di montaggio meno comuni. Il file `auto.master` contiene delle linee che si rivolgono a ciascuno di questi mount point, organizzate come segue:

<mount-point> *<map-type>*

La parte <*mount-point*> indica la posizione sulla quale eseguire il montaggio sul file system locale. Il <*map-type*> si riferisce al modo in cui verrà montato il mount point. Il metodo più comune per il montaggio automatico delle esportazioni NFS è quello di usare un file come tipo di mappa per un particolare mount point. Il file mappa, di solito chiamato `auto.`<*mount-point*>, dove per <*mount-point*> si intende il mount point designato in `auto.master`, contiene linee simili a questa:

```
</local/directory>  -<options>  <server>:</remote/export>
```

Sostituire </*local/directory*;> con il file system locale sul quale è montata la directory esportata. Questo mount point deve esistere già prima che il file mappa venga letto, altrimenti l'operazione di montaggio non riesce.

Sostituire <*options*> con un elenco, separato da una virgola, di opzioni per il file system NFS (consultare la Sezione 9.4.3 per maggiori informazioni). Assicurarsi di includere il carattere trattino (-) immediatamente prima dell'elenco delle opzioni.

Sostituire <*server*> con l'hostname, l'indirizzo IP o con il nome del dominio completamente qualificato del server che esporta il file system.

Sostituire </*remote/export*> con il percorso per la directory esportata.

Sostituire <*options*> con un elenco, separato da una virgola, di opzioni per il file system NFS (consultare la Sezione 9.4.3 per maggiori informazioni).

I file di configurazione di `autofs`, che possono essere utilizzati per svariati montaggi su molti tipi di dispositivi e filesystem, sono particolarmente utili nella creazione di montaggi NFS. Per esempio, alcune organizzazioni salvano la directory `/home` di un utente su di un server centrale tramite una condivisione NFS, successivamente, configurano il file `auto.master` su ciascuna delle workstation in modo che si rivolgano a un file `auto.home` contenente le specifiche su come montare la directory `/home` tramite NFS. In questo modo, l'utente ha accesso ai dati personali e ai file di configurazione contenuti nella directory `/home` collegandosi da un punto qualsiasi della rete interna. In un caso come questo, il file `auto.master` ha il seguente aspetto:

```
/home   /etc/auto.home
```

In questo modo, il mount point di `/home/` sul sistema locale è impostato per essere configurato dal file `/etc/auto.home`, che ha un aspetto simile al seguente:

```
*  -fstype=nfs4,soft,intr,rsize=32768,wsize=32768,nosuid  server.example.com:/home
```

Secondo questa linea, qualsiasi directory alla quale un utente cerchi di accedere sotto la directory `/home` locale (per via dell'asterisco) dovrebbe risultare in un montaggio NFS sul sistema `server.example.com` sul mount point di `/home`. Le opzioni di montaggio specificano che ogni NFS nella directory `/home` deve servirsi di una particolare serie di impostazioni. Per maggiori informazioni sulle opzioni di montaggio, tra cui quelle incluse in questo esempio, consultate la Sezione 9.4.3.

Per maggiori informazioni sui file di configurazione `autofs`, consultare la pagina man `auto.master`.

9.4.3. Opzioni comuni di montaggio NFS

Oltre al montaggio di un filesystem tramite NFS su di un host remoto, si possono specificare numerose altre opzioni al momento del montaggio, che possono facilitare tale operazione. Queste opzioni possono essere utilizzate con comandi manuali `mount`, impostazioni `/etc/fstab` e `autofs`.

Le opzioni che seguono sono le più diffuse per i montaggi NFS:

- `fsid=num` — Forza la gestione del file e le impostazioni degli attributi in modo da essere *num*, invece di un numero derivato dal numero maggiore e minore del dispositivo a blocco presente sul filesystem montato. Il valore `0` rappresenta un significato particolare se utilizzato con NFSv4. NFSv4 presenta un concetto root dei filesystem esportati. Il punto di esportazione, esportato con `fsid=0` viene utilizzato come il suddetto root.
- `hard` o `soft` — Specificano se il programma che utilizza un file tramite il collegamento NFS deve arrestarsi e attendere (`hard`) che il server torni online, nel caso in cui l'host che sta servendo il file system esportato non sia disponibile, o se deve invece inviare un rapporto di errore (`soft`).

  Se specificate `hard`, non sarete in grado di terminare il processo in attesa che la comunicazione NFS riprenda, a meno che non specifichiate anche l'opzione `intr`.

  Se indicate l'opzione `soft`, potete impostare un'opzione aggiuntiva del tipo `timeo=`<*valore*>, dove <*value*> specifica il numero di secondi che devono trascorrere prima di riportare l'errore.
- `intr` — Fa sì che le richieste NFS vengano interrotte qualora si verifichi un arresto del server o nel caso non fosse possibile raggiungerlo.
- `nfsvers=2` or `nfsvers=3` — Specifica la versione del protocollo NFS da usare. Questo è utile per gli host che eseguono server NFS multipli. Se non vengono specificate le versioni, NFS utilizza la versione più aggiornata supportata dal kernel e dal comando `mount`. Questa opzione non viene supportata con NFSv4 e non deve essere utilizzata.
- `noacl` — Disabilita la processazione ACL. Tale processo potrebbe essere utile quando ci si trova di fronte a versioni più vecchie di Red Hat Enterprise Linux, Red Hat Linux, o Solaris, poichè la tecnologia ACL più recente, non è compatibile con i sistemi più obsoleti.
- `nolock` — A volte è richiesto nei collegamenti con il server NFS di vecchia generazione. Disabilita il blocco del file.
- `noexec` — Non permette l'esecuzione di binari sui file system montati. È utile se il vostro sistema sta montando tramite NFS un file system non Linux contenente binari incompatibili.
- `nosuid` — Disabilita l'identificatore impostato dall'utente o i bit dell'identificatore impostato dal gruppo. Questo evita agli utenti remoti di ottenere privilegi più elevati, eseguendo un programma setuid.
- `port=num` — Specifica il valore numerico della porta del server NFS. Se *num* è `0` (il default), allora `mount` interroga portmapper dell'host remoto per sapere il numero della porta da usare. Se il demone NFS dell'host remoto non è registrato con il proprio portmapper, verrà utilizzato il numero della porta standard di NFS di TCP 2049.
- `rsize=num` e `wsize=num` — Queste impostazioni aumentano la velocita di comunicazione NFS per operazioni di lettura (`rsize`) e scrittura (`wsize`) impostando una dimensione maggiore per i blocchi di dati, in byte, da trasferire in una volta. Fate attenzione quando modificate questi valori; alcuni kernel di Linux e schede di rete di vecchia generazione non funzionano molto bene con blocchi di dimensioni maggiori. Per NFSv2 o NFSv3, i valori di default per entrambi i parametri è 8192. Per NFSv4, i valori di default per entrambi i parametri è di 32768.
- `sec=mode` — Specifica il tipo di sicurezza da utilizzare quando si autentica un collegamento NFS.

  `sec=sys` è l'impostazione di default che utilizza GID e UID UNIX locali per mezzo di AUTH_SYS, per autenticare le operazioni NFS.

  `sec=krb5` utilizza Kerberos V5 invece di GID e UID UNIX locali per autenticare gli utenti.

  `sec=krb5i` utilizza Kerberos V5 per autenticare gli utenti ed eseguire il controllo dell'integrità delle operazioni NFS, utilizzando le checksum per prevenire l'alterazione dei dati.

  `sec=krb5p` utilizza Kerberos V5 per l'autenticazione degli utenti, per il controllo dell'integrità, e per la codifica del traffico NFS per prevenire l'azione di sniffing del traffico. Ciò rappresenta l'impostazione più sicura, ma al tempo stesso presenta la possibilità più alta di verifica di un overhead.

- `tcp` — Specifica al momento del montaggio di NFS, l'uso del protocollo TCP.
- `udp` — Specifica al montaggio NFS di usare il protocollo UDP.

Nelle pagine man di `mount` e `nfs`, sono elencate molte altre opzioni.

9.5. Sicurezza e NFS

NFS è molto utile per condividere in modo traparente, interi file system con un gran numero di host conosciuti. Comunque, al di là della facilità d'uso, esistono numerosi problemi di sicurezza.

Dovete tenere in considerazione i seguenti punti quando esportate file system NFS su un server o li montate su di un client. così potrete ridurre al minimo i rischi legati alla sicurezza di NFS e sarete in grado di proteggere meglio i vostri dati.

Per un elenco abbreviato sulle fasi che un amministratore può intraprendere per rendere sicuri i server NFS, consultate il capitolo *Sicurazza del server* nella *Red Hat Enterprise Linux Security Guide*.

9.5.1. Accesso Host

A seconda dell'ambiente di rete esistente, e dei problemi riguardanti la sicurezza, è possibile scegliere la versione di NFS a voi più idonea. Le seguenti sezioni affrontano le differenze nell'implementazione delle misure di sicurezza con NFSv2, NFSv3, e NFSv4. L'utilizzo di NFSv4 è consigliato rispetto alle altre versioni di NFS.

9.5.1.1. Utilizzo di NFSv2 o NFSv4

NFS controlla chi può montare un file system esportato in base all'host che effettua la richiesta di montaggio, non in base all'utente che utilizza il file system. Occorre fornire agli host dei diritti specifici perché possano montare il file system esportato. Non è possibile controllare l'accesso degli utenti, a differenza dei permessi di file e directory. In altre parole, quando esportate un file system tramite NFS state anche permettendo a tutti gli utenti su qualsiasi host remoto collegati al server NFS, di accedere ai dati condivisi. Per limitare tali rischi, gli amministratori possono sempre abilitare un accesso di sola lettura, limitando il potere degli utenti e dei gruppi ID tramite l'opzione squash. Sfortunatamente, queste soluzioni possono intaccare l'uso originario della condivisione NFS.

Inoltre, se un aggressore assume il controllo del server DNS utilizzato dal sistema che esporta il file system NFS, il sistema associato a un particolare hostname o a un nome di dominio completamente qualificato può essere indirizzato verso una macchina non autorizzata. A questo punto, tale macchina non autorizzata *è* il sistema che ha il permesso di montare la condivisione NFS, dal momento che non vengono scambiate informazioni di sorta relative al nome utente e password mirate ad aumentare la sicurezza del montaggio NFS.

Le wildcard vanno usate con cautela quando si esegue una esportazione di directory tramite NFS, in quanto è possibile raggiungere anche sistemi di cui non conoscete l'esistenza.

È possibile altresì limitare l'accesso al servizio `portmap` tramite i wrapper TCP. L'accesso alle porte usate da `portmap`, `rpc.mountd`, e `rpc.nfsd`, può essere limitato creando delle regole per il firewall con `iptables`.

Per informazioni su come rendere sicuro NFS e `portmap`, consultate il capitolo intitolato *Sicurazza del server* nella *Red Hat Enterprise Linux Security Guide*. Informazioni aggiuntive sui firewall sono disponibili sul Capitolo 18.

9.5.1.2. Utilizzo di NFSv4

Con NFSv4 si è verificata una vera e propria rivoluzione per quanto concerne il processo di autenticazione e le problematiche riguardanti la sicurezza delle esportazioni NFS. NFSv4 permette l'implementazione del modulo RPCSEC_GSS, il meccanismo GSS-API versione 5 di Kerberos, SPKM-3, e LIPKEY. Con NFSv4, i meccanismi riguardanti la sicurezza sono orientati al modello di autenticazione individuale degli utenti, e non delle macchine client come previsto con NFSv2 e NFSv3.

Nota Bene

Prima di configurare un server NFSv4, si presume che sia stato precedentemente installato un server ticket-granting di Kerberos (KDC), e che lo stesso sia stato configurato correttamente.

NFSv4 include un supporto basato su ACL su modello Microsoft Windows NT, e non sul modello POSIX, grazie alle sue caratteristiche e al suo largo impiego. NFSv2 e NFSv3 non presentano alcun supporto per gli attributi delle ACL native.

Un'altra caratteristica importante riguardante la sicurezza di NFSv4, è rappresentata dalla rimozione del demone `rpc.mountd`. Infatti il demone `rpc.mountd` presentava alcune vulnerabilità a causa del modo con il quale gestiva i file handler.

Per maggiori informazioni su RPCSEC_GSS, e sul modo di operare di `rpc.svcgssd` e `rpc.gssd`, consultate http://www.citi.umich.edu/projects/nfsv4/gssd/.

9.5.2. Permessi dei file

Una volta che il filesystem NFS è stato montato in modalità lettura/scrittura da un host remoto, la protezione per ciascuno dei file condivisi é rappresentata dai propri permessi. Se due utenti che condividono lo stesso valore di ID montano lo stesso filesystem NFS, l'uno sarà in grado di modificare i file dell'altro e viceversa. Inoltre, chiunque si colleghi come root sul sistema client pò utilizzare il comando `su -` per assicurarsi i permessi per accedere a determinati file attraverso la condivisione NFS. Per maggiori informazioni sui conflitti userid e NFS, consultare il capitolo intitolato *Gestione degli account e dei Gruppi* in *Red Hat Enterprise Linux Introduzione al System Administration*.

Per default, le access control lists (ACL) sono supportate da NFS sotto Red Hat Enterprise Linux. Non è consigliato disabilitare questa caratteristica. Per maggiori informazioni, consultare il capitolo *Network File System (NFS)* nella *Red Hat Enterprise Linux System Administration Guide*.

Il modo di operare per default, quando si esporta un filesystem tramite NFS è il *root squashing* che imposta l'ID utente di chiunque acceda alla condivisione NFS come utente root sulla propria macchina locale su un valore di un account del server `nfsnobody`. È altamente sconsigliato disabilitare questa opzione.

Se esportate una condivisione NFS di sola lettura, dovreste usare anche l'opzione `all_squash`, che attribuisce un user ID dell'utente `nfsnobody`, a chiunque acceda il vostro file system esportato.

9.6. Risorse aggiuntive

L'amministrazione di un server NFS può rappresentare una sorta di sfida. Per esportare filesystem NFS o montarli come client, sono disponibili numerose opzioni, alcune delle quali non sono state menzionate in questo capitolo. Per maggiori dettagli, dunque, consultate queste ulteriori fonti di informazione.

9.6.1. Documentazione installata

- `/usr/share/doc/nfs-utils-<version-number>/` — Sostituire <*numero-versione*> con il numero della versione del pacchetto NFS installato. Questa directory tratta l'implementazione di NFS in Linux e offre una panoramica delle varie configurazioni NFS, descrivendone gli effetti sulle prestazioni del trasferimento dei file.
- `man mount` — offre una descrizione esauriente delle varie opzioni di montaggio relative alla configurazione di server e client NFS.
- `man fstab` — Fornisce dettagli in merito al formato del file `/etc/fstab`, utilizzato per montare i filesystem all'avvio del sistema.
- `man nfs` — Fornisce le informazioni riguardanti le opzioni di montaggio e di esportazione del filesystem specifiche per NFS.
- `man exports` — Mostra le opzioni comunemente utilizzate nel file `/etc/exports` per l'esportazione di filesystem NFS.

9.6.2. Siti web utili

- http://nfs.sourceforge.net/ — La home di Linux NFS project, luogo di aggiornamenti sullo stato del progetto.
- http://www.citi.umich.edu/projects/nfsv4/linux/ — Un NFSv4 per le risorse del kernel 2.6 di Linux.
- http://www.nfsv4.org — La home di Linux NFS project versione 4 e di tutti gli standard correlati.
- http://www.vanemery.com/Linux/NFSv4/NFSv4-no-rpcsec.html — Descrive in modo dettagliato NFSv4 con il Fedora Core 2, il quale include il kernel 2.6.
- http://www.nluug.nl/events/sane2000/papers/pawlowski.pdf — Un eccellente whitepaper sui miglioramenti e sui nuovi contenuti del protocollo della versione 4 di NFS.

9.6.3. Libri correlati

- *Managing NFS and NIS* di Hal Stern, Mike Eisler e Ricardo Labiaga; O'Reilly & Associates — un'eccellente guida di riferimento circa le numerose opzioni di montaggio ed esportazione disponibili per NFS.
- *NFS Illustrated* di Brent Callaghan; Addison-Wesley Publishing Company — mette a confronto NFS con altri filesystem di rete e spiega nel dettaglio come avviene la comunicazione NFS.
- *Red Hat Enterprise Linux System Administration Guide*; Red Hat, Inc. — Il capitolo *Network File System (NFS)* spiega in modo abbreviato come impostare i client NFS e i server.
- *Red Hat Enterprise Linux Security Guide*; Red Hat, Inc. — Il capitolo *Sicurezza del server* spiega i diversi modi per rendere sicuro NFS a gli altri servizi.

Capitolo 10.

Server HTTP Apache

Server HTTP Apache è un potente Web server open source sviluppato dalla Apache Software Foundation (http://www.apache.org). Red Hat Enterprise Linux include la versione 2.0 di Server HTTP Apache oltre a numerosi moduli server progettati per potenziarne le funzionalità.

Il file di configurazione di default di Server HTTP Apache si adatta bene alle esigenze tanto che potrebbe non rendersi mai necessario modificare le impostazioni di default. Questo capitolo riporta molte delle direttive trovate all'interno del suo file di configurazione (`/etc/httpd/conf/httpd.conf`) utili per coloro che desiderano una configurazione personalizzata o necessitano di convertire un file di configurazione da un formato 1.3 di un Server HTTP Apache piú vecchio.

Avvertenza

Se intendete utilizzare l'utility grafica **Strumento di configurazione di HTTP** (`system-config-httpd`), *non* modificate manualmente il file di configurazione di Server HTTP Apache, in quanto lo **Strumento di configurazione di HTTP** rigenera questo file ogni volta che viene utilizzato.

Per maggiori informazioni sullo **Strumento di configurazione di HTTP**, consultate il capitolo relativo alla *configurazione Server HTTP Apache* nella *Red Hat Enterprise Linux System Administration Guide*.

10.1. Server HTTP Apache 2.0

Esistono notevoli differenze tra la versione 2.0 e la versione 1.3 del Server HTTP Apache, (quest'ultima disponibile con Red Hat Linux 2.1 e sulle versioni precedenti). Questa sezione esamina alcune delle nuove caratteristiche del Server HTTP Apache 2.0 e riporta le modifiche più importanti . Se dovete migrare un file di configurazione della versione 1.3 sul formato 2.0, consultate la Sezione 10.2.

10.1.1. Caratteristiche del Server HTTP Apache 2.0

Server HTTP Apache 2.0 include le seguenti caratteristiche:

- *Apache API* — I moduli utilizzano un set più potente di Application Programming Interfaces (API).

Importante

I moduli creati per Server HTTP Apache 1.3 non funzioneranno se non viene effettuato l'aggiornamento alla nuova API. Se non siete certi del fatto che un modulo particolare sia supportato, consultate lo sviluppatore *prima* dell'aggiornamento.

- *Filtro* — i moduli hanno la possibilità di funzionare come filtri del contenuto. Per ulteriori informazioni sul funzionamento dei filtri, consultate la Sezione 10.2.4.
- *Supporto IPv6* — Ha la capacità di supportare il formato IP addressing di nuova concezione.
- *Direttive semplificate* — Numerose direttive sono state rimosse, mentre altre sono state semplificate. Per ulteriori informazioni sulle direttive specifiche, consultate la Sezione 10.5.

- *Risposte agli errori in più lingue* — Quando utilizzate documenti *SSI* (*Server Side Include*), le pagine di risposta agli errori personalizzabili possono essere distribuite in più lingue.

Un elenco più esauriente di modifiche è disponibile online all'indirizzo http://httpd.apache.org/docs-2.0/.

10.1.2. Modifiche ai pacchetti nel Server HTTP Apache 2.0

Iniziando con Red Hat Enterprise Linux 3, i pacchetti Server HTTP Apache sono stati rinominati. Altresì altri pacchetti sono stati rinominati, eliminati o incorporati in altri pacchetti.

Di seguito viene riportato un elenco delle modifiche:

- I pacchetti `apache`, `apache-devel` e `apache-manual` sono stati rinominati rispettivamente come `httpd`, `httpd-devel` e `httpd-manual`.
- Il pacchetto `mod_dav` è stato incorporato nel pacchetto `httpd`.
- I pacchetti `mod_put` e `mod_roaming` sono stati rimossi, poichè la loro funzionalità è un sottoinsieme di quella fornita da `mod_dav`.
- I pacchetti `mod_auth_any` e `mod_bandwidth` sono stati rimossi.
- Il numero di versione del pacchetto `mod_ssl` è ora sincronizzato con il pacchetto `httpd`. Ciò significa che il pacchetto `mod_ssl` per Server HTTP Apache 2.0 dispone di un numero di versione *inferiore* rispetto al pacchetto `mod_ssl` per Server HTTP Apache 1.3.

10.1.3. Modifiche al filesystem nel Server HTTP Apache 2.0

In seguito all'aggiornamento del Server HTTP Apache 2.0 sono presenti le seguenti modifiche alla struttura del filesystem:

- *È stata aggiunta una nuova directory di configurazione, `/etc/httpd/conf.d/`.* — Questa nuova directory viene utilizzata per archiviare i file di configurazione per i moduli in singoli pacchetti, come `mod_ssl`, `mod_perl` e `php`. Al server viene indicato di caricare i file di configurazione da questo percorso tramite la direttiva `Include conf.d/*.conf` che si trova nel file di configurazione di Server HTTP Apache `/etc/httpd/conf/httpd.conf`.

  
  Importante

  È importante che la linea che presenta la nuova directory di configurazione, venga inserita al momento della migrazione di una configurazione esistente.

- *I programmi `ab` e `logresolve` sono stati spostati.* — queste utility sono state spostate dalla directory `/usr/sbin/` alla directory `/usr/bin/`. In questo modo gli script con percorsi assoluti per questi file binari non avranno esito positivo.
- *Il comando `dbmmanage` è stato sostituito.* — Il comando `dbmmanage` è stato sostituito da `htdbm`. Per ulteriori informazioni, consultate la Sezione 10.2.4.5.
- *Il file di configurazione `logrotate` è stato rinominato.* — tale file è stato rinominato da `/etc/logrotate.d/apache` a `/etc/logrotate.d/httpd`.

La sezione successiva spiegherà come eseguire la migrazione di una configurazione Server HTTP Apache 1.3 al formato 2.0.

10.2. Migrazione dei file di configurazione del Server HTTP Apache 1.3

Questa sezione si riferisce a coloro che desiderano eseguire una migrazione del file di configurazione del Server HTTP Apache 1.3, utilizzato da Server HTTP Apache 2.0.

Se avete aggiornato il server da Red Hat Enterprise Linux 2.1 a Red Hat Enterprise Linux 4, il nuovo file di configurazione per il pacchetto Server HTTP Apache 2.0 viene installato come `/etc/httpd/conf/httpd.conf.rpmnew` e il file della versione 1.3 originale `httpd.conf` rimarrà invariato. Dipende da voi se utilizzare il nuovo file di configurazione e migrare le vecchie impostazioni oppure utilizzare il file esistente come base e modificarlo secondo le necessità; tuttavia, alcune parti del file sono state modificate più di altre e un approccio vario è in genere la scelta migliore. I file di configurazione per entrambe le versioni 1.3 e 2.0 sono suddivisi in tre sezioni.

Se il file `/etc/httpd/conf/httpd.conf` è una versione modificata della nuova versione di default, e avete salvato una copia dell'originale, potrebbe essere più semplice richiamare il comando `diff`, come nell'esempio riportato di seguito (registrato come utente root):

```
diff -u httpd.conf.orig httpd.conf | less
```

Questo comando evidenzia le modifiche effettuate. Se non disponete di una copia del file originale, estraetela da un pacchetto RPM mediante i comandi `rpm2cpio` e `cpio` come nell'esempio riportato di seguito:

```
rpm2cpio apache-<version-number>.i386.rpm | cpio -i --make
```

Nel comando precedentemente riportato, sostituire *<numero-versione>* con il numero della versione per il pacchetto `apache`.

È infine utile sapere che Server HTTP Apache dispone di una modalità di verifica degli errori all'intero della configurazione. Per accedervi, digitate il comando riportato di seguito:

```
apachectl configtest
```

10.2.1. Configurazione dell'ambiente globale

La sezione sull'ambiente globale del file di configurazione contiene le direttive che influiscono sul funzionamento globale del Server HTTP Apache, come il numero di richieste che può gestire e le posizioni dei vari file. Questa sezione richiede un grande numero di modifiche, e dovrebbe basarsi sul file di configurazione del Server HTTP Apache 2.0 durante la migrazione delle vecchie impostazioni all'interno di esso.

10.2.1.1. Interfaccia e Port binding

Le direttive `BindAddress` e `Port` non esistono più. La funzione relativa è ora fornita da una direttiva più flessibile `Listen`.

Se avete impostato `Port 80` nel file di configurazione della versione 1.3, dovete modificare l'opzione in `Listen 80` nel file di configurazione 2.0. Se avete impostato `Port` a un valore *diverso da 80* dovete anche aggiungere il numero di porta al contenuto della direttiva `ServerName`.

Per esempio, quella riportata di seguito è una direttiva del Server HTTP Apache 1.3:

```
Port 123
ServerName www.example.com
```

Per migrare questa impostazione sul Server HTTP Apache 2.0, utilizzate la struttura riportata di seguito:

```
Listen 123
ServerName www.example.com:123
```

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- `http://httpd.apache.org/docs-2.0/mod/mpm_common.html#listen`
- `http://httpd.apache.org/docs-2.0/mod/core.html#servername`

10.2.1.2. Regolazione della dimensione del pool del server

Quando Server HTTP Apache accetta le richieste, esso invia i processi figlio o thread in modo da gestirli. Questo gruppo di processi figlio o thread è conosciuto come *pool del server*. Con Server HTTP Apache 2.0, la responsabilità per la creazione e il mantenimento di questi pool del server è stata riassunta in un gruppo di moduli chiamati *Multi-Processing Modules* (*MPM*). A differenza di altri moduli, solo un modulo del gruppo MPM può essere caricato dal Server HTTP Apache. Con la versione 2.0 sono disponibili tre moduli MPM: `prefork`, `worker`, e `perchild`. Attualmente sono solo disponibili gli MPM `prefork` e `worker`, anche se l'MPM `perchild` potrebbe essere reso disponibile in futuro.

La caratteristica originale del Server HTTP Apache 1.3 è stata spostata nell'MPM `prefork`. L'MPM `prefork` accetta le stesse direttive del Server HTTP Apache 1.3, di conseguenza le seguenti direttive possono essere migrate direttamente:

- `StartServers`
- `MinSpareServers`
- `MaxSpareServers`
- `MaxClients`
- `MaxRequestsPerChild`

L'MPM `worker` implementa un server multi-process, multi-threaded che fornisce maggiore scalabilità. Quando si usa questo MPM, le richieste sono gestite dai thread, conservando le risorse del sistema e permettendo ad un gran numero di richieste di essere servite in modo efficiente. Anche se alcune delle direttive accettate dall'MPM `worker` sono le stesse di quelle accettate dall'MPM `prefork`, i valori per quelle direttive non dovrebbero essere trasferiti direttamente da una installazione Server HTTP Apache 1.3. È meglio invece usare i valori di default come guida, per poi provare a determinare quali valori funzionano meglio.

Importante

Per usare l'MPM `worker`, creare il file `/etc/sysconfig/httpd`, ed aggiungere la seguente direttiva:

```
HTTPD=/usr/sbin/httpd.worker
```

Per ulteriori informazioni sugli MPM, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mpm.html

10.2.1.3. Supporto DSO (Dynamic Shared Object)

Sono molte le modifiche necessarie in questo caso ed è consigliabile che chiunque tenti di modificare una configurazione Server HTTP Apache 1.3 per adeguarsi alla versione 2.0 (in contrapposizione alla migrazione delle modifiche nella configurazione della versione 2.0), copi questa sezione dal file di configurazione del Server HTTP Apache 2.0.

Per coloro che non desiderano copiare la sezione dalla configurazione Server HTTP Apache 2.0, dovrebbero tener presente di quanto segue:

- Le direttive `AddModule` `ClearModuleList` non esistono più. Queste direttive erano utilizzate per garantire l'abilitazione dei moduli nell'ordine corretto. L'API di Apache 2.0 consente ai moduli di specificare l'ordine, eliminando la necessità di queste due direttive.
- L'ordine delle righe `LoadModule`, in molti casi non è più importante.
- Molti moduli sono stati aggiunti, rimossi, rinominati, suddivisi o incorporati in altri.
- Le linee `LoadModule` per i moduli dei pacchetti dei loro RPM (`mod_ssl`, `php`, `mod_perl` e simili) non sono più necessarie perchè possono essere disponibili nei file della directory `/etc/httpd/conf.d/`.
- Le varie definizioni di `HAVE_XXX` non sono più definite.

Importante

Se modificate il file originale, si prega di notare che é molto importante che `httpd.conf` contenga la seguente direttiva:

```
Include conf.d/*.conf
```

L'omissione di questa direttiva porta al fallimento di tutti i moduli contenuti nei propri RPM, (come `mod_perl`, `php` e `mod_ssl`).

10.2.1.4. Altre modifiche all'ambiente globale

Le direttive riportate di seguito sono state rimosse dalla configurazione del Server HTTP Apache 2.0:

- *`ServerType`* — Server HTTP Apache può essere eseguito solo come `ServerType standalone` rendendo inutile questa direttiva.
- *`AccessConfig`* e *`ResourceConfig`* — Queste direttive sono state rimosse poichè rispecchiano la funzione della direttiva `Include`. Se avete impostato le direttive `AccessConfig` e `ResourceConfig` dovete sostituirle con le direttive `Include`.

  Per garantire che i file vengano letti nell'ordine stabilito dalle vecchie direttive, le direttive `Include` devono essere collocate alla fine del file `httpd.conf`, con la direttiva corrispondente a `ResourceConfig` che precede quella corrispondente a `AccessConfig`. Se avete utilizzato i valori predefiniti, dovete includerli in modo esplicito come file `conf/srm.conf` e `conf/access.conf`.

10.2.2. Configurazione del server principale

La sezione relativa alla configurazione del server principale del file di configurazione consente di impostare il server principale, che risponde a qualsiasi richiesta che non venga gestita da una definizione `<VirtualHost>`. I valori in questo caso forniscono inoltre valori predefiniti per qualsiasi sezione `<VirtualHost>` possiate definire.

Le direttive utilizzate in questa sezione sono state modificate in minima parte tra la versione 1.3 e 2.0 del Server HTTP Apache. Se la configurazione del vostro server principale è stata personalizzata in modo considerevole, potrebbe essere più semplice modificare la configurazione esistente per adattarsi a Server HTTP Apache 2.0. Solo gli utenti con sezioni del server principale in parte personalizzate, devono migrare le proprie modifiche nella configurazione di default 2.0.

10.2.2.1. Mappatura di `UserDir`

La direttiva `UserDir` è utilizzata per abilitare URL come `http://example.com/~bob/` per mappare una sottodirectory all'interno della home directory dell'utente `bob`, come `/home/bob/public_html`. Un effetto collaterale di questa caratteristica può consentire a un potenziale aggressore di determinare se un determinato nome utente sia presente nel sistema. Pertanto la configurazione di default del Server HTTP Apache 2.0 disabilita questa direttiva.

Per abilitare la mappatura di `UserDir`, modificate la direttiva in `httpd.conf` da:

```
UserDir disable
```

a quanto riportato di seguito:

```
UserDir public_html
```

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_userdir.html#userdir

10.2.2.2. Accesso

Le direttive di accesso riportate di seguito sono state rimosse:

- `AgentLog`
- `RefererLog`
- `RefererIgnore`

Tuttavia i log referer ed agent sono ancora disponibili mediante l'utilizzo delle direttive `CustomLog` e `LogFormat`.

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog
- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#logformat

10.2.2.3. Indicizzare le directory

La direttiva `FancyIndexing` è stata finalmente rimossa. La stessa funzionalità è disponibile attraverso l'*option* `FancyIndexing` all'interno della direttiva `IndexOptions`.

L'opzione `VersionSort` per la direttiva `IndexOptions` fa sì che i file contenenti i numeri della versione vengano ordinati in modo naturale. Per esempio, `httpd-2.0.6.tar` viene visualizzato prima di `httpd-2.0.36.tar` nella pagine dell'indice delle directory.

I valori predefiniti per le direttive `ReadmeName` e `HeaderName` sono stati modificati da `README` e `HEADER` a `README.html` e `HEADER.html`.

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#indexoptions
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#readmename
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#headername

10.2.2.4. Negoziazione del contenuto

La direttiva `CacheNegotiatedDocs` richiede ora l'argomento `on` o `off`. Le istanze esistenti di `CacheNegotiatedDocs` devono essere sostituite con `CacheNegotiatedDocs on`.

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_negotiation.html#cachenegotiateddocs

10.2.2.5. Error Documents

Per utilizzare un messaggio hard-coded con la direttiva `ErrorDocument`, il messaggio deve essere compreso tra virgolette ["], invece di essere preceduto dalle stesse come nel Server HTTP Apache 1.3.

Per esempio, quella riportata di seguito è una direttiva del Server HTTP Apache 1.3:

```
ErrorDocument 404 "The document was not found
```

Per migrare una impostazione `ErrorDocument` al Server HTTP Apache 2.0, utilizzate la struttura riportata di seguito:

```
ErrorDocument 404 "The document was not found"
```

Notare nell'esempio precedente della direttiva `ErrorDocument`, le virgolette alla fine.

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/core.html#errordocument

10.2.3. Configurazione dell'Host Virtuale

Il contenuto di tutte le sezioni <VirtualHost> deve essere migrato in modo simile alla sezione del server principale come descritto nella Sezione 10.2.2.

Importante

La configurazione dell'host virtuale SSL/TLS è stata spostata all'esterno del file di configurazione del server principale nel file `/etc/httpd/conf.d/ssl.conf`.

Per ulteriori informazioni su questo argomento, consultate il capitolo intitolato *Configurazione del server securo HTTP di Apache* nella *Red Hat Enterprise Linux System Administration Guide* e nella documentazione indicata nel seguente URL:

- http://httpd.apache.org/docs-2.0/vhosts/

10.2.4. Moduli e Server HTTP Apache 2.0

Nel Server HTTP Apache 2.0 il sistema dei moduli è stato modificato per consentire agli stessi di essere collegati o combinati in modo diverso. Gli script *Common Gateway Interface* (*CGI*), per esempio, possono generare documenti HTML analizzati dal server che possono poi essere elaborati da `mod_include`. In questo modo si apre una vasta gamma di possibilità in relazione al modo in cui i moduli possono essere combinati per raggiungere un obiettivo specifico.

Questo sistema funziona in base al fatto che ciascuna richiesta viene servita da esattamente un modulo *handler* seguito da zero o più moduli *filtro*.

Con il Server HTTP Apache 1.3, per esempio, uno script Perl sarebbe stato gestito completamente dal modulo Perl (`mod_perl`). Con il Server HTTP Apache 2.0 la richiesta viene inizialmente *gestita* dal modulo principale — il quale serve i file statici — e viene poi *filtrata* da `mod_perl`.

L'impiego dettagliato di questa e di altre nuove caratteristiche del Server HTTP Apache 2.0 va oltre lo scopo di questo documento, tuttavia, la modifica ha ramificazioni se viene usata la direttiva `PATH_INFO`, per un documento gestito da un modulo che viene ora implementato come filtro, in quanto ogni modulo contiene informazioni sul percorso dopo il nome del file vero. Il modulo principale, che gestisce inizialmente la richiesta, non comprende per default `PATH_INFO` e restituisce gli errori `404 Not Found` per le richieste che contengono tali informazioni. Potete utilizzare la direttiva `AcceptPathInfo` per obbligare il modulo principale ad accettare le richieste con `PATH_INFO`.

Di seguito viene riportato un esempio di questa direttiva:

```
AcceptPathInfo on
```

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/core.html#acceptpathinfo
- http://httpd.apache.org/docs-2.0/handler.html
- http://httpd.apache.org/docs-2.0/filter.html

10.2.4.1. Il modulo `suexec`

In Server HTTP Apache 2.0, il modulo `mod_suexec` utilizza la direttiva `SuexecUserGroup` invece delle direttive `User` e `Group`, le quali vengono a loro volta usate per configurare gli host virtuali. Le direttive `User` e `Group` possono, in generale, essere ancora usate, ma sono sconsigliate per configurare gli host virtuali.

Per esempio, quella riportata di seguito è una direttiva del Server HTTP Apache 1.3:

```
<VirtualHost vhost.example.com:80>
    User someone
    Group somegroup
</VirtualHost>
```

Per migrare questa impostazione sul Server HTTP Apache 2.0, utilizzate la struttura riportata di seguito:

```
<VirtualHost vhost.example.com:80>
    SuexecUserGroup someone somegroup
</VirtualHost>
```

10.2.4.2. Il modulo `mod_ssl`

La configurazione per `mod_ssl` è stata spostata dal file `httpd.conf` nel file `/etc/httpd/conf.d/ssl.conf`. Perchè questo file venga caricato e perchè `mod_ssl` funzioni correttamente, dovete disporre dell'istruzione `Include conf.d/*.conf` nel vostro file `httpd.conf` come descritto nella Sezione 10.2.1.3.

Le direttive `ServerName` negli host virtuali SSL devono specificare in modo esplicito il numero di porta.

Per esempio, quella riportata di seguito è una direttiva del Server HTTP Apache 1.3:

```
<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.example.name
    ...
</VirtualHost>
```

Per migrare questa impostazione sul Server HTTP Apache 2.0, utilizzate la struttura riportata di seguito:

```
<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.host.name:443
    ...
</VirtualHost>
```

È importante notare anche che entrambe le direttive `SSLLog` e `SSLLogLevel` sono state rimosse. Il modulo `mod_ssl` ubbidisce ora alle direttive `ErrorLog` e `LogLevel`. Consultare la Sezione 10.5.35 e la Sezione 10.5.36 per maggiori informazioni su queste direttive.

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html
- http://httpd.apache.org/docs-2.0/vhosts/

10.2.4.3. Il modulo `mod_proxy`

Le istruzioni di controllo dell'accesso proxy sono ora collocate nel blocco `<Proxy>` invece di `<Directory proxy:>`.

La funzionalità di caching del vecchio file `mod_proxy` è stata suddivisa nei tre moduli riportati di seguito:

- `mod_cache`
- `mod_disk_cache`
- `mod_mem_cache`

Questi moduli utilizzano in genere direttive simili alle versioni più vecchie del modulo `mod_proxy`, ma è consigliabile verificare ogni direttiva prima di migrare ogni impostazione della cache.

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_proxy.html

10.2.4.4. Il modulo `mod_include`

Il modulo `mod_include` è ora implementato come filtro (per ulteriori informazioni sui filtri, consultate la Sezione 10.2.4) ed è pertanto abilitato in modo diverso.

Per esempio, quella riportata di seguito è una direttiva del Server HTTP Apache 1.3:

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Per migrare questa impostazione sul Server HTTP Apache 2.0, utilizzate la struttura riportata di seguito:

```
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
```

Da notare che la direttiva `Options +Includes` è ancora necessaria per la sezione `<Directory>` o in un file `.htaccess`.

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_include.html

10.2.4.5. I moduli `mod_auth_dbm` e `mod_auth_db`

Server HTTP Apache 1.3 supporta due moduli di autenticazione, `mod_auth_db` e `mod_auth_dbm` che utilizzavano rispettivamente i database Berkeley e DBM. Questi moduli sono stati combinati in un singolo modulo chiamato `mod_auth_dbm` in Server HTTP Apache 2.0, che è in grado di accedere a numerosi formati di database. Per migrare da `mod_auth_db`, i file di configurazione devono essere modificati sostituendo `AuthDBUserFile` e `AuthDBGroupFile` con gli equivalenti `mod_auth_dbm`, `AuthDBMUserFile` e `AuthDBMGroupFile`. Dovete inoltre aggiungere la direttiva `AuthDBMType DB` per indicare il tipo di file del database utilizzato.

L'esempio riportato di seguito mostra una configurazione `mod_auth_db` per il Server HTTP Apache 1.3:

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBUserFile /var/www/authdb
  require valid-user
</Location>
```

Per migrare questa impostazione alla versione 2.0 del Server HTTP Apache, utilizzate la struttura riportata di seguito:

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBMUserFile /var/www/authdb
  AuthDBMType DB
  require valid-user
</Location>
```

La direttiva `AuthDBMUserFile` può anche essere utilizzata nei file `.htaccess`.

Lo script Perl `dbmmanage`, utilizzato per manipolare i database dei nomi utente e password, è stato sostituito da `htdbm` nel Server HTTP Apache 2.0. Il programma `htdbm` offre funzionalità equivalenti e come `mod_auth_dbm` può operare un'ampia serie di formati del database. L'opzione `-T` può essere utilizzata nella riga di comando per specificare il formato da utilizzare.

La Tabella 10-1 mostra come migrare da un database in formato DBM al formato `htdbm` mediante `dbmmanage`.

Azione	dbmmanage command (1.3)	Equivalent htdbm command (2.0)
Aggiungere l'utente al database (mediante la password)	`dbmmanage authdb add username password`	`htdbm -b -TDB authdb username password`
Aggiungere l'utente al database (richiesta della password)	`dbmmanage authdb adduser username`	`htdbm -TDB authdb username`
Rimuovere l'utente dal database	`dbmmanage authdb delete username`	`htdbm -x -TDB authdb username`
Elencare gli utenti nel database	`dbmmanage authdb view`	`htdbm -l -TDB authdb`
Verificare una password	`dbmmanage authdb check username`	`htdbm -v -TDB authdb username`

Tabella 10-1. Migrazione da `dbmmanage` a `htdbm`

Le opzioni `-m` e `-s` funzionano con `dbmmanage` e `htdbm`, attivando l'utilizzo degli algoritmi MD5 o SHA1 per la codifica delle password.

Quando create un nuovo database con `htdbm`, deve essere utilizzata l'opzione `-c`.

Per ulteriori informazioni su questo argomento, consultate la documentazione indicata di seguito nel sito Web di Apache Software Foundation:

- http://httpd.apache.org/docs-2.0/mod/mod_auth_dbm.html

10.2.4.6. Il modulo `mod_perl`

La configurazione per `mod_perl` è stata spostata da `httpd.conf` nel file

/etc/httpd/conf.d/perl.conf. Perchè questo file venga caricato e perchè mod_perl funzioni, dovete disporre dell'istruzione Include conf.d/*.conf nel file httpd.conf come descritto nella Sezione 10.2.1.3.

Le occorrenze di Apache:: in httpd.conf devono essere sostituite con ModPerl::. Inoltre è stato modificato il modo in cui vengono registrati gli handler.

Quella riportata di seguito è un esempio di configurazione Server HTTP Apache 1.3 mod_perl:

```
<Directory /var/www/perl>
    SetHandler perl-script
    PerlHandler Apache::Registry
    Options +ExecCGI
</Directory>
```

Quella riportata di seguito è il mod_perl equivalente per Server HTTP Apache 2.0:

```
<Directory /var/www/perl>
    SetHandler perl-script
    PerlResponseHandler ModPerl::Registry
    Options +ExecCGI
</Directory>
```

La maggior parte dei moduli per mod_perl 1.x deve funzionare senza alcuna modifica con mod_perl 2.x. I moduli XS richiedono la ricompilazione e possono richiedere modifiche Makefile minori.

10.2.4.7. Il modulo mod_python

La configurazione per mod_python; è stata spostata da httpd.conf nel file /etc/httpd/conf.d/python.conf. Perchè questo file venga caricato e perchè mod_python; funzioni, dovete disporre dell'istruzione Include conf.d/*.conf nel file httpd.conf come descritto nella Sezione 10.2.1.3.

10.2.4.8. PHP

La configurazione per PHP è stata spostata da httpd.conf nel file /etc/httpd/conf.d/php.conf. Perchè questo file venga caricato, dovete disporre dell'istruzione Include conf.d/*.conf nel file httpd.conf come descritto nella Sezione 10.2.1.3.

Nota Bene

Quando si esegue una migrazione su Server HTTP Apache 2.0 su Red Hat Enterprise Linux 4, qualsiasi direttiva di configurazione PHP usata nel Server HTTP Apache 1.3, è completamente compatibile.

In PHP versione 4.2.0 e successive, la serie di variabili predefinite di defaultdisponibili nell'ambito globale è stata modificata. Il singolo input e le variabili del server non sono più, per default, collocate direttamente in questo punto. Questa modifica può fare in modo che gli script si interrompano. Potete tornare al comportamento precedente impostando register_globals su On nel file /etc/php.ini.

Per ulteriori informazioni su questo argomento, consultate l'URL indicato di seguito per dettagli relativi alle modifiche:

- http://www.php.net/release_4_1_0.php

10.2.4.9. Il modulo `mod_authz_ldap`

Red Hat Enterprise Linux contiene il modulo `mod_authz_ldap` per il Server HTTP Apache. Questo modulo usa la forma abbreviata del distinguished name per il soggetto, e l'emittente del certificato SSL del client per determinare il distinguished name dell'utente all'interno della directory LDAP. È altresì in grado di abilitare gli utenti in base agli attributi della entry della directory LDAP dell'utente stesso, determinando un accesso alle risorse in base ai privilegi dell'utente o del gruppo, negando tale accesso agli utenti che possiedono una password scaduta. È necessario il modulo `mod_ssl`, quando si usa il modulo `mod_authz_ldap`.

Importante

Il modulo `mod_authz_ldap` non esegue l'autenticazione dell'utente su di una directory LDAP che usa una password cifrata. Questa funzionalità viene fornita dal modulo sperimentale `mod_auth_ldap`. Consultate la documentazione del modulo `mod_auth_ldap` disponibile su http://httpd.apache.org/docs-2.0/mod/mod_auth_ldap.html per ottenere maggiori informazioni.

Il file `/etc/httpd/conf.d/authz_ldap.conf` configura il modulo `mod_authz_ldap`.

Per maggiori informazioni su come configurare il modulo `mod_authz_ldap`, consultare `/usr/share/doc/mod_authz_ldap-`*<version>*`/index.html` (sostituendo *<version>* con il numero della versione del pacchetto) o http://authzldap.othello.ch/.

10.3. Dopo l'installazione

Dopo aver installato il pacchetto `httpd`, rivedere la documentazione del Server HTTP Apache disponibile online su http://httpd.apache.org/docs-2.0/.

La documentazione relativa al Server HTTP Apache contiene un elenco e descrizioni complete di tutte le opzioni di configurazione. Per vostra praticità, questo capitolo fornisce brevi descrizioni delle direttive di configurazione utilizzate dal Server HTTP Apache 2.0.

La versione del Server HTTP Apache 2.0 comprende la possibilità d'impostare i Web server sicuri utilizzando la potente cifratura SSL fornita dai pacchetti `mod_ssl` e `openssl`. Mentre esaminate i file di configurazione, fate attenzione che sia incluso sia un Web server non sicuro che sicuro. Quest'ultimo può essere eseguito come un host virtuale che viene configurato nel file `/etc/httpd/conf.d/ssl.conf`. Per ulteriori informazioni sugli host virtuali, consultate la Sezione 10.8. Per informazioni sulla configurazione di un host virtuale del server sicuro, consultate la Sezione 10.8.1. Per informazioni sulla configurazione del server sicuro HTTP di Apache, consultate il capitolo relativo alla *Configurazione del server sicuro HTTP Apache* nella *Red Hat Enterprise Linux System Administration Guide*.

Nota Bene

Red Hat, Inc. non include le estensioni di FrontPage, poichè la licenza Microsoft™ vieta l'inserimento delle estensioni in prodotti di terzi. Per maggiori informazioni sulle estensioni di FrontPage e Server HTTP Apache, consultate: http://www.rtr.com/fpsupport/.

10.4. Avvio e arresto di `httpd`

L'RPM `httpd` installa lo script `/etc/init.d/httpd` il quale è accessibile tramite il comando `sbin/service`.

Per avviare il server, digitate il comando come root:

```
/sbin/service httpd start
```

Per fermare il server, digitate il comando:

```
/sbin/service httpd stop
```

Il comando `restart` è un modo veloce per fermare e riavviare il Server HTTP Apache.

Per avviare il server, digitate il comando come root:

```
/sbin/service httpd restart
```

Nota Bene

Se state eseguendo Server HTTP Apache come server sicuro, sarà forse necessario digitare la password del server quando si utilizzano le opzioni `start` o `restart`.

Dopo aver modificato il file `httpd.conf`, non é necessario fermare e avviare il server. Invece, usare l'opzione `reload`.

Per ricaricare il file di configurazione del server, digitare come root:

```
/sbin/service httpd reload
```

Nota Bene

Se state eseguendo Server HTTP Apache come server sicuro, la password del server *non* é necessaria quando si usa l'opzione `reload`.

Per default, il servizio `httpd` *non* verrà avviato automaticamente al momento dell'avvio del computer. Per configurare il servizio `httpd` in modo tale da iniziare al momento dell'avvio, usare una utility initscript, come `/sbin/chkconfig`, **/sbin/ntsysv**, o il programma **Strumento di configurazione dei servizi**. Per ulteriori informazioni relative a questi tool, consultate il capitolo relativo al *Controllo dell'accesso ai servizi* in *Red Hat Enterprise Linux System Administration Guide*.

Nota Bene

Se state eseguendo Server HTTP Apache come server sicuro, quando usate una chiave SSL privata cifrata, vi viene richiesta la password del server sicuro dopo l'avvio della macchina.

Per informazioni sulla configurazione di un server sicuro HTTP Apache, consultate il capitolo relativo alla *Configurazione di un server sicuro HTTP Apache* nella *Red Hat Enterprise Linux System Administration Guide*.

10.5. Direttive di configurazione in `httpd.conf`

Il file di configurazione del Server HTTP Apache è `/etc/httpd/conf/httpd.conf`. Il file `httpd.conf` é ben commentato e facile da capire.La sua configurazione di default si adatta bene a molteplici situazioni, anche se è comunque necessario acquisire familiarità con alcune delle più importanti opzioni di configurazione.

Avvertenza

Con la versione 2.0 del Server HTTP Apache, molte opzioni di configurazione sono state modificate. Se dovete migrare un file di configurazione della versione 1.3 al nuovo formato, consultate la Sezione 10.2.

10.5.1. Suggerimenti generali di configurazione

Se avete necessità di configurare il Server HTTP Apache, modificate `/etc/httpd/conf/httpd.conf` e ricaricate, riavviate oppure spegnete e riavviate, il processo `httpd`. Per informazioni su come ricaricare, arrestare e avviare il Server HTTP Apache, consultate la Sezione 10.4.

Prima di modificare `httpd.conf` si consiglia di fare una copia del file originale. Creando un backup, infatti, è possibile rimediare a eventuali errori commessi durante la modifica del file di configurazione.

Se viene commesso un errore e il Web server non funziona correttamente, rivisionare prima i precedenti passaggi in `httpd.conf` in modo tale da verificare che non ci siano errori di battitura.

Successivamente controllare il log d'errore del server, `/var/log/httpd/error_log`. Il log d'errore puó essere non semplice da interpretare, dipende dal vostro livello di esperienza. Se avete dei problemi, le ultime entry nel log d'errore, dovrebbero fornire informazioni utili inerenti a ció che é accaduto.

Nelle sottosezioni che seguono, troverete una breve descrizione delle direttive incluse in `httpd.conf`. Tali descrizioni non sono approfondite. Per reperire maggiori informazioni potete consultare la relativa documentazione, disponibile online su http://httpd.apache.org/docs-2.0/.

Per ulteriori dettagli sulle direttive `mod_ssl`, consultate la documentazione disponibile online su http://httpd.apache.org/docs-2.0/mod/mod_ssl.html.

10.5.2. `ServerRoot`

`ServerRoot` è la directory di livello superiore che contiene i file del server. Entrambi i server (sicuro e non sicuro) sono impostati per utilizzare `ServerRoot` di `"/etc/httpd"`.

10.5.3. `PidFile`

`PidFile` nomina il file nel quale è memorizzato il PID (ID del processo). Per default il PID viene memorizzato nella directory `/var/run/httpd.pid`.

10.5.4. `Timeout`

`Timeout` definisce, tempo necessario al server per la ricezione e la trasmissione durante la comunicazione. `Timeout` è impostato per un'attesa di `300` secondi, ossia il tempo adeguato per la maggior parte delle situazioni.

10.5.5. KeepAlive

KeepAlive stabilisce se il server permetterà più di una richiesta per connessione e puó essere usato per evitare che un client utilizzi troppe risorse del server.

Per default, Keepalive è impostato su off. Se viene impostato su on e il server è particolarmente occupato, il server è in grado di produrre rapidamente il numero più elevato di processi figli. In tal caso, il server diventa piuttosto lento. Se abilitate Keepalive, è buona idea avere una impostazione su valori bassi di KeepAliveTimeout (consultate la Sezione 10.5.7 per maggiori informazioni sulla direttiva KeepAliveTimeout) e controllate i file di log /var/log/httpd/error_log sul server. Questo log vi consente di sapere se il server presenta una carenza di processi figli.

10.5.6. MaxKeepAliveRequests

La direttiva imposta il numero massimo di richieste accettate su ogni connessione persistente. Il team di sviluppo di Apache consiglia di impostare un valore alto, al fine di migliorare le prestazioni del server. MaxKeepAliveRequests è impostato per default su 100, un valore che si adatta alla maggior parte delle possibili situazioni.

10.5.7. KeepAliveTimeout

KeepAliveTimeout imposta il numero di secondi durante il quale il server attende una nuova richiesta prima di chiudere la connessione. Una volta ricevuta la richiesta, si applica invece la direttiva Timeout. KeepAliveTimeout é impostato per default su 15 secondi.

10.5.8. IfModule

I tag <IfModule> e </IfModule> creano una sezione attivata solo se il modulo specificato é montato. Le direttive presenti all'interno della sezioneIfModule vengono elaborate solo tramite una di queste due condizioni. Il modulo specificato all'interno del tag di inizio <IfModule> è stato caricato, oppure se un punto esclamativo [!] appare prima del nome del modulo, le direttive sono elaborate solo se il modulo specificato nel tag <IfModule>, *non* è caricato.

Per maggiori informazioni inerenti i moduli Server HTTP Apache, consultare la Sezione 10.7.

10.5.9. Direttive MPM specifiche del pool di server

Come spiegato nella Sezione 10.2.1.2, con il Server HTTP Apache 2.0 la responsabilità per la gestione delle caratteristiche del gruppo del server, ricade su di un gruppo di moduli chiamato MPM. Le caratteristiche del gruppo del server differisce a seconda di quale MPM viene usato. Per questa ragione, è necessario una sezione IfModule per definire il gruppo di server per l'MPM in uso.

Per default, Server HTTP Apache 2.0 definisce il pool di server per gli MPM prefork e worker.

Il seguente è un elenco di direttive trovate all'interno delle sezioni MPM specifiche del gruppo di server.

10.5.9.1. StartServers

La direttiva StartServers imposta il numero di processi server che devono essere creati all'avvio. Poichè il Web server elimina o crea dinamicamente i processi server in funzione del carico del traffico, non è necessario cambiare questo parametro. Il vostro Web server è impostato per far partire all'avvio 8 processi server, per l'MPM prefork e 2 per l'MPM worker.

10.5.9.2. `MaxRequestsPerChild`

`MaxRequestsPerChild` imposta il numero massimo di richieste che ogni processo figlio può gestire prima di essere eliminato. Lo scopo principale di `MaxRequestsPerChild` è quello di evitare che un processo rimanga in esecuzione troppo a lungo, occupando un'eccessiva quantità di memoria. Il default `MaxRequestsPerChild` per l'MPM `prefork` è `4000` e per l'MPM `worker` è `0`.

10.5.9.3. `MaxClients`

`MaxClients` imposta un limite per il numero totale di processi server, di client connessi contemporaneamente, in esecuzione allo stesso momento. Lo scopo principale per questa direttiva è di prevenire un crash del sistema operativo da parte di Server HTTP Apache. Si consiglia di mantenere alto questo valore, per server molto occupati. Il default del server è impostato su 150, questo senza tener conto dell'MPM in uso. Tuttavia é consigliato che il valore di `MaxClients` ecceda `256` quando si usa l'MPM `prefork`.

10.5.9.4. `MinSpareServers` e `MaxSpareServers`

Questi valori vengono usati con l'MPM `prefork`. Essi determinano come il Server HTTP Apache si adatti dinamicamente al carico di lavoro mantenendo un numero appropriato di processi di riserva del server a seconda del traffico. Viene eseguita la verifica del numero di server in attesa di richiesta che vengono eliminati se superano il valore di `MaxSpareServers` oppure vengono creati se sono inferiori al valore di `MinSpareServers`.

Il valore di default di `MinSpareServers` è `5`, mentre quello di `MaxSpareServers` è `20`. Queste impostazioni di default dovrebbero essere adatte alla maggior parte delle situazioni possibili. Si consiglia di non aumentare troppo il valore di `MinSpareServers`, poichè si rischia di sovraccaricare il server quando il traffico non è eccessivo.

10.5.9.5. `MinSpareThreads` e `MaxSpareThreads`

Questi valori vengono usati con l'MPM `worker`. Essi determinano come il Server HTTP Apache si adatti dinamicamente al carico di lavoro mantenendo un numero appropriato di processi di riserva del server a seconda del traffico. Viene eseguita la verifica del numero dei thread del server in attesa di una richiesta, ed elimina alcuni di essi se il loro numero è maggiore del valore di `MaxSpareThreads`, alternativamente vengono creati altri thread se il loro numero risulta essere inferiore a `MinSpareThreads`.

Il valore di default di `MinSpareThreads` è `25`, mentre quello di `MaxSpareThreads` è `75`. Queste impostazioni di default sono adatte alla maggior parte delle situazioni possibili. Il valore per `MaxSpareThreads` deve essere maggiore o uguale alla somma di `MinSpareThreads` e `ThreadsPerChild` altrimenti il Server HTTP Apache lo corregge automaticamente.

10.5.9.6. `ThreadsPerChild`

Questo valore viene usato solo con l'MPM `worker`. Esso imposta il numero di trhead all'interno di ogni processo figlio. Il valore di default per questa direttiva è `25`.

10.5.10. `Listen`

Il comando `Listen` specifica su quale porta il Web server accetta le richieste in entrata. Per default il Server HTTP Apache attende le richieste sulla porta 80 per la comunicazione Web non sicura e (nel

/etc/httpd/conf.d/ssl.conf che definiscono i server sicuri) sulla porta 443 per la comunicazione Web sicura.

Se impostate il Server HTTP Apache in ascolto su una porta inferiore alla 1024, solo l'utente root è in grado di iniziarlo. Per le porte superiori alla 1024, httpd può essere iniziato come un utente normale.

La direttiva Listen può inoltre essere usata per specificare particolari indirizzi IP dai quali il server accetta le connessioni.

10.5.11. Include

Include consente ad altri file di configurazione di essere inclusi in fase di runtime.

Il percorso di questi file di configurazione può essere assoluto o relativo rispetto a ServerRoot.

Importante

Perchè il server utilizzi moduli in singoli pacchetti, come mod_ssl, mod_perl e php, la direttiva riportata di seguito deve trovarsi in Section 1: Global Environment di http.conf:

```
Include conf.d/*.conf
```

10.5.12. LoadModule

LoadModule è utilizzata per caricare i moduli Dynamic Shared Object (DSO). Maggiori informazioni sul supporto DSO di Server HTTP Apache e sull'esatto modo di impiego della direttiva LoadModule sono disponibili sulla Sezione 10.7. L'ordine di caricamento dei moduli *non è più importante* con Server HTTP Apache 2.0. Per ulteriori informazioni sul supporto del Server HTTP Apache 2.0 per il DSO, consultate la Sezione 10.2.1.3.

10.5.13. ExtendedStatus

La direttiva ExtendedStatus controlla se Apache genera informazioni di base (off) sullo stato del server oppure informazioni dettagliate (on), quando viene chiamato server-status. Il gestore Server-status viene chiamato usando i tag Location. Maggiori informazioni sulla chiamata server-status sono incluse nella Sezione 10.5.60.

10.5.14. IfDefine

I tag IfDefine utilizzano le direttive di configurazione specificate al loro interno se nel primo tag la definizione "test" presente nel tag IfDefine risulta essere vera. Le direttive vengono ignorate se il test è falso.

Il test nei tag IfDefine è il nome di un parametro (per esempio, HAVE_PERL). Se il parametro è definito, ossia viene fornito come argomento del comando d'avvio del server, allora il test è vero. In questo caso, quando il Web server viene attivato, il test è vero e le direttive contenute nei tag IfDefine vengono applicate.

10.5.15. SuexecUserGroup

La direttiva SuexecUserGroup, la quale viene originata dal modulo mod_suexec, permette la specificazione dei privilegi di esecuzione dell'utente e del gruppo per i programmi CGI. La richieste non-CGI vengono processate con l'utente ed il gruppo specificato nelle direttive User e Group.

Nota Bene

La direttiva SuexecUserGroup sostituisce la configurazione Server HTTP Apache 1.3 nell'uso delle direttive User e Group, all'interno della configurazione delle sezioni di VirtualHosts.

10.5.16. User

La direttiva User imposta il nome utente del processo server e determina quale file il server é in grado di accedere. Qualsiasi file non accessibile per questo utente, risultano inaccessibili anche per i client che si collegano al Server HTTP Apache.

L'utente di default per User è apache.

Questa direttiva è sconsigliata per la configurazione degli host virtuali.

Nota Bene

Per ragioni di sicurezza, l'Server HTTP Apache non funzionerá come utente root.

10.5.17. Group

Specifica il nome del gruppo dei processi del Server HTTP Apache.

Questa direttiva è sconsigliata per la configurazione degli host virtuali.

Per default Group è impostato su apache.

10.5.18. ServerAdmin

Imposta la direttiva ServerAdmin per l'indirizzo di posta elettronica dell'amministratore del Web server. Questo indirizzo di posta elettronica appare nei messaggi di errore delle pagine Web generate dal server, in modo che gli utenti possano riferire eventuali problemi inviando un messaggio all'amministratore del server.

Per default, ServerAdmin é impostato su root@localhost.

Un modo comune per impostare ServerAdmin è di impostarlo su webmaster@your_domain.com. Una volta impostato, assegnate dunque l'alias webmaster alla persona responsabile del Web server nel file /etc/aliases, ed eseguire /usr/bin/newaliases.

10.5.19. ServerName

ServerName specifica un hostname e un numero di porta (corrispondenti alla direttiva Listen) per il server. Il ServerName non deve necessariamente corrispondere al nome reale dell'hostname. Per esempio, il Web server puó essere www.example.com ma l'hostname del server è foo.example.com. Il valore specificato in ServerName deve essere un Domain Name Service (DNS) valido, che può essere risolto dal sistema — evitate di inserire nomi inventati.

Di seguito viene riportato un esempio di direttiva ServerName:

```
ServerName www.example.com:80
```

Se specificate un ServerName, accertatevi che nel file /etc/hosts esista una corrispondenza tra indirizzo IP e nome del server.

10.5.20. UseCanonicalName

Quando impostato su on, questa direttiva configura il Server HTTP Apache in modo tale da essere usato come riferimento usando il valore specificato nelle direttive ServerName e Port. Quando UseCanonicalName é impostato su off, il server userá invece il valore usato dal client richiedente.

UseCanonicalName é impostato per default su off.

10.5.21. DocumentRoot

DocumentRoot è la directory che contiene la maggior parte dei file HTML in risposta alle richieste. La directory DocumentRoot di default, per entrambi i Web server, sicuro e non sicuro, è la directory /var/www/html. Per esempio, il server può ricevere una richiesta per il documento seguente:

```
http://example.com/foo.html
```

Il server cercherà il file riportato di seguito nella directory di default:

```
/var/www/html/foo.html
```

Se desiderate modificare DocumentRoot in modo che non sia condivisa dal Web server non sicuro e da quello sicuro, consultate la Sezione 10.8.

10.5.22. Directory

I tag <Directory /path/to/directory> e </Directory> creano ció che viene riferito come una sezione, usata per raggruppare un insieme di direttive di configurazione da applicare solo a una particolare directory e a tutte le sue sottodirectory. Tutte le direttive applicabili a una directory possono essere usate all'interno dei tag Directory.

Per default, alla directory root (/), vengono applicati i parametri più restrittivi, tramite le direttive Options (consultate la Sezione 10.5.23) e AllowOverride (consultate la Sezione 10.5.24). Sotto questa configurazione, alle directory che necessitano di impostazioni meno restrittive devono essere assegnate in modo esplicito quelle impostazioni.

Nella configurazione predefinita, un'altra Directory é configurata per il DocumentRoot la quale assegna un minor numero di parametri rigidi all'albero della directory in modo tale che ilServer HTTP Apache possa accedere ai file presenti.

La sezione Directory puó essere usata per configurare delle directory cgi-bin aggiuntive per applicazioni di tipo server-side, al di fuori della directory specificata nella direttiva ScriptAlias (consultate la Sezione 10.5.41 per maggiori informazioni).

Per fare questo, la sezione `Directory` deve impostare l'opzione `ExecCGI` per quella directory.

Per esempio, se gli script sono posizionati in `/home/my_cgi_directory`, aggiungere `Directory` al file `httpd.conf`:

```
<Directory /home/my_cgi_directory>
    Options +ExecCGI
</Directory>
```

Successivamente, la direttiva `AddHandler` non deve essere commentata per identificare i file con l'estensione `.cgi` come script CGI. Consultare la Sezione 10.5.56 per istruzioni su come impostare `AddHandler`.

Per fare ció, i permessi per gli script CGI, e l'intero percorso per gli script, deve essere impostato su 0755.

10.5.23. `Options`

La direttiva `Options` controlla le caratteristiche dei server disponibili in una particolare directory. Per esempio, con i parametri restrittivi specificati per la directory root, la direttiva `Options` è impostata solo per `FollowSymLinks`. Non sono abilitate altre caratteristiche, ad eccezione di quella che consente al server di seguire i link simbolici nella directory root.

Per default, nella directory `DocumentRoot`, la direttiva `Options` è configurata per contenere `Indexes`, `Includes` e `FollowSymLinks`. `Indexes` permette al server di generare un elenco di directory per una directory, se non è specificata alcuna direttiva `DirectoryIndex` (per esempio: `index.html`). `FollowSymLinks` consente al server di seguire i link simbolici in questa directory.

Nota Bene

Le istruzioni `Options` della sezione di configurazione del server principale, devono essere replicate individualmente su ogni sezione del`VirtualHost`. Consultate la Sezione 10.5.65 per maggiori informazioni.

10.5.24. `AllowOverride`

La direttiva `AllowOverride` consente di stabilire se `Options` più essere ridefinito dalle dichiarazioni presenti in un file `.htaccess`. Per default, sia la directory root, sia la directory `DocumentRoot` sono impostate per non permettere di sovrascrivere `.htaccess`.

10.5.25. `Order`

La direttiva `Order` controlla l'ordine con il quale le direttive `allow` e `deny` sono valutate. Il server viene configurato per valutare le direttive `Allow` prima delle direttive `Deny` per la direttiva `DocumentRoot`.

10.5.26. `Allow`

`Allow` specifica quale client può accedere a una determinata directory. Il client può essere `all`, un nome di dominio, un indirizzo IP, una parte dell'indirizzo IP, una coppia rete/maschera di rete e così

via. La directory `DocumentRoot` è configurata per `Allow` o permettere l'accesso da `all` ossia da tutti i client.

10.5.27. `Deny`

`Deny` funziona esattamente come `allow`, ma specifica quali accessi negare. Per default `DocumentRoot` non è configurata per `Deny` o negare alcuna richiesta.

10.5.28. `UserDir`

`UserDir` è la sottodirectory all'interno di ogni home directory dell'utente, in cui vanno collocati i file HTML personali che il Web server utilizza. Questa direttiva é impostata per default su `disable`.

Per default, la sottodirectory è `public_html`. Per esempio, il server può ricevere la richiesta seguente:

`http://`*`example.com`*`/~`*`username`*`/foo.html`

Il server cerca il file:

`/home/username/public_html/foo.html`

Nell'esempio precedente `/home/username` è la home directory dell'utente (ovviamente il percorso di default della directory home può essere diverso sul vostro sistema).

Assicuratevi che i permessi della home directory dell'utente siano corretti. L'impostazione esatta è 0711. I bit di lettura (r) e di esecuzione (x) devono essere impostati nelle directory `public_html` dell'utente (anche 0755 funziona correttamente). I file presenti nelle directory `public_html` devono essere impostati almeno su 0644.

10.5.29. `DirectoryIndex`

La direttiva `DirectoryIndex` è la pagina predefinita che viene restituita al client quando un utente richiede l'indice di una directory, specificando uno slash (/) dopo il nome della directory.

Quando un utente richiede la pagina http://*`esempio`*/*`questa_directory`*/, riceve la pagina `DirectoryIndex`, se presente, o un elenco di directory generato dal server. Il default per `DirectoryIndex` è `index.html` ed il tipo di mappa `index.html.var`. Il server cerca di individuare uno di questi file, restituendo il primo file trovato. Se non trova alcun file, e per questa directory è impostata la direttiva `Options Indexes`, il server genera e restituisce un elenco delle subdirectory e dei file contenuti nella directory in formato HTML, a meno che il contenuto elencato della directory, non viene impostato su off.

10.5.30. `AccessFileName`

`AccessFileName` attribuisce un nome al file che il server utilizza per accedere alle informazioni di controllo in ogni directory. Il default é `.htaccess`.

Immediatamente dopo la direttiva `AccessFileName`, una serie di tag `Files` controllano l'accesso ai file che iniziano con `.ht`. Per ragioni di sicurezza queste direttive negano l'accesso Web a qualunque file `.htaccess` (o a qualunque altro file che inizi con `.ht`).

10.5.31. `CacheNegotiatedDocs`

Per default, il Web server chiede ai server proxy di non conservare nella cache i documenti trasmessi in base al contenuto (ovvero quei documenti che potrebbero essere modificati col tempo o mediante l'inserimento del richiedente). Se `CacheNegotiatedDocs` é impostato su `on`, questa funzione viene disabilitata e i server proxy sono autorizzati a conservare i documenti nella cache.

10.5.32. `TypesConfig`

`TypesConfig` definisce il nome del file che imposta le mappature dell'elenco predefinito dei tipi MIME (le estensioni dei file per i tipi di contenuto). Il file `TypesConfig` di default è `/etc/mime.types`. Invece di modificare questo file, si consiglia di aggiungere i tipi MIME tramite la direttiva `AddType`.

Per maggiori informazioni su questa direttiva, consultate la Sezione 10.5.55.

10.5.33. `DefaultType`

`DefaultType` definisce il tipo MIME di default per i documenti non riconosciuti. Il default é `text/plain`.

10.5.34. `HostnameLookups`

`HostnameLookups` puó essere impostato su `on`, `off` o `double`. Se `HostnameLookups` é impostato su `on`, il server automaticamente resolve l'indirizzo IP per ogni collegamento. Risolvere l'indirizzo IP significa che il server effettua uno o piú collegamenti ad un server DNS, aggiungendo l'elaborazione overhead. Se `HostnameLookups` é impostato su `double`, il server effettua un look up DNS inverso doppio, aggiungendo una maggiore elaborazione overhead.

Per conservare risorse sul server, per default impostate `HostnameLookups` su `off`.

Se desiderate vedere gli hostname nei vostri file di log, dovreste eseguire uno dei tanti tool di analisi dei log in grado di effettuare lookup DNS in modo più efficiente e su scala più ampia nel momento in cui ruotate i file di log.

10.5.35. `ErrorLog`

`ErrorLog` specifica il nome del file dove vengono registrati tutti gli errori del server. Per default, il file di log degli errori è `/var/log/httpd/error_log`.

10.5.36. `LogLevel`

`LogLevel` definisce il livello di dettaglio dei messaggi d'errore registrati nel file di registrazione. `LogLevel` può essere impostato (dal più dettagliato al meno dettagliato) su`emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` o `debug`. Il `LogLevel` di default è `warn`.

10.5.37. `LogFormat`

La direttiva `LogFormat` configura il formato dei diversi file log del Web server. L'attuale `LogFormat` che verrà utilizzata dipende dalle impostazioni attribuite nella direttiva `CustomLog` (consultate la Sezione 10.5.38).

Le seguenti, sono delle opzioni del formato se la direttiva `CustomLog` é impostata su `combined`:

`%h` (indirizzo IP dell'host remoto oppure hostname)

Elenca l'indirizzo IP remoto del client richiedente. Se `HostnameLookups` é impostato su `on`, l'hostname del client, se disponibile dal DNS, viene registrato.

`%l` (rfc931)

Non usato. Un trattino [-] viene visualizzato nel file log per questo campo.

`%u` (utente autenticato)

Elenca il nome utente dell'utente memorizzato se è necessario eseguire l'autenticazione. Generalmente non é usato, quindi viene visualizzato un trattino [-] nel file log per questo campo.

`%t` (data)

Elenca la data e l'orario della richiesta.

`%r` (riga di richiesta)

Elenca la riga di richiesta esattamente come arriva dal browser o dal client.

`%s` (stato)

Elenca il codice dello stato HTTP ritornato all'host del client.

`%b` (byte)

Elenca la misura del documento.

`%\"%{Referer}i\"` (referenza)

Elenca l'URL della pagina web riferita all'host del client per il Web server.

`%\"%{User-Agent}i\"` (utente-agent)

Elenca il tipo di browser web che effettua la richiesta.

10.5.38. `CustomLog`

`CustomLog` indica il file di log e il suo formato. Nella configurazione di default, il file di log é registrato sul file `/var/log/httpd/access_log`.

Il formato `CustomLog` di default é il formato del file log `combined` come di seguito riportato:

```
remotehost rfc931 user date "request" status bytes referrer user-agent
```

10.5.39. `ServerSignature`

La direttiva `ServerSignature` aggiunge una linea contenente la versione del Server HTTP Apache e il `ServerName` del server host a qualsiasi documento generato dal server stesso (per esempio, i messaggi di errore rispediti ai client). Per default, `ServerSignature` è impostato su `on`.

Potete impostarlo anche su `off` o su `EMail`. `EMail`, aggiunge un tag HTML `mailto:ServerAdmin` alla linea della firma delle risposte generate automaticamente.

10.5.40. `Alias`

L'impostazione `Alias` consente alle directory che si trovano al di fuori di `DocumentRoot` di essere accessibili. Qualunque URL che termina con l'alias viene automaticamente risolto all'interno del percorso dell'alias. Per default, é giá impostata un alias per la directory `icons/`. Un Web server puó accedere alla directory `icons/`, ma la suddetta directory non é presente nel `DocumentRoot`.

10.5.41. `ScriptAlias`

La direttiva `ScriptAlias` definisce dove sono localizzati gli script CGI. Normalmente è meglio non lasciare gli script CGI all'interno di `DocumentRoot`, poiché potrebbero essere visualizzati come documenti di testo.Per questa ragione, una directory speciale, esterna alla directory `DocumentRoot` contenente gli eseguibili e gli script del server, é ideata dalla direttiva `ScriptAlias`. Questa directory é conosciuta come `cgi-bin` ed è impostata per default su `/var/www/cgi-bin/`.

É possibile creare delle directory per conservare gli eseguibili esternamente alla directory `cgi-bin`. Per informazioni su quanto sopra, consultare la Sezione 10.5.56 e la Sezione 10.5.22.

10.5.42. `Redirect`

Quando una pagina Web viene spostata, la direttiva `Redirect` può essere utilizzata per rimappare il vecchio URL con quello nuovo. Il formato è il seguente:

```
Redirect /<old-path>/<file-name> http://<current-domain>/<current-path>/<file-name>
```

In questo esempio, sostituire *<percorso-vecchio>* con le informazioni del percorso vecchio per *<nome-file>* e *<dominio-corrente>* e *<percorso-corrente>* con le informazioni correnti del dominio e percorso per *<nome-file>*.

In questo esempio, qualsiasi richiesta per *<nome-file>* nella vecchia posizione, é automaticamente ridiretta nella nuova posizione.

Per tecniche piú avanzate di ridirezione, usare il modulo `mod_rewrite` incluso con il Server HTTP Apache. Per maggiori informazioni inerenti la configurazione del modulo `mod_rewrite`, consultare la documentazione online di Apache Software Foundation http://httpd.apache.org/docs-2.0/mod/mod_rewrite.html.

10.5.43. `IndexOptions`

`IndexOptions` controlla l'aspetto degli elenchi delle directory generate dal server, aggiungendo icone e descrizioni dei file e così via. Se è impostata la direttiva `Options Indexes` (consultate la Sezione 10.5.23), il Web server genera un elenco delle directory quando lo stesso riceve una richiesta HTTP per una directory senza un indice.

Innanzitutto, il Web server cerca nella directory uno dei file specificati con la direttiva `DirectoryIndex` (di solito, `index.html`). Se non viene trovato un file `index.html`, Server HTTP Apache crea una directory HTML che elenca le directory richieste. L'aspetto di questa directory é controllato, in parte, dalla direttiva `IndexOptions`.

La configurazione di default imposta su on `FancyIndexing`. Questo significa che un utente puó riordinare un elenco della directory, facendo clic sulle intestazioni della colonna. Con un altro clic sulla stessa intestazione si inverte l'ordine da ascendente a discendente. `FancyIndexing` visualizza icone diverse per file diversi, a seconda dell'estensione.

Se utilizzate la direttiva `AddDescription` e attivate `FancyIndexing`, viene visualizzata una breve descrizione dei file nell'elenco delle directory generato dal server.

IndexOptions presenta diversi parametri che possono essere impostati per controllare l'aspetto delle directory generate dal server. I parametri IconHeight e IconWidth, necessitano l'inclusione HTML delle tag HEIGHT e WIDTH da parte del server, per le icone delle pagine Web generate dal server stesso.Il parametro IconsAreLinks combina l'icona grafica con il link HTML, il quale contiene il target del link URL.

10.5.44. AddIconByEncoding

Questa direttiva associa un'icona a un particolare tipo di file secondo la codifica MIME negli elenchi di directory generati dal server. Per esempio, il Web server mostra, per default, l'icona compressed.gif accanto ai file di tipo x-compress e x-gzip negli elenchi della directory generati dal server.

10.5.45. AddIconByType

Questa direttiva specifica il nome dell'icona da visualizzare accanto al file con il tipo MIME negli elenchi delle directory generati dal server. Per esempio, il vostro server è impostato per visualizzare l'icona text.gif accanto al file con il tipo MIME di testo text, negli elenchi della directory generati dal server.

10.5.46. AddIcon

AddIcon specifica l'icona da visualizzare negli elenchi delle directory generati dal server per certi tipi di file o per i file che hanno determinate estensioni. Per esempio, il vostro Web server è impostato in modo da mostrare l'icona binary.gif per i file con estensione .bin o .exe.

10.5.47. DefaultIcon

DefaultIcon specifica l'icona da visualizzare negli elenchi delle directory generati dal server per i file che non hanno altre icone specificate. Il file d'immagine unknown.gif é il default.

10.5.48. AddDescription

Quando utilizzate FancyIndexing come parametro IndexOptions, la direttiva AddDescription puó essere utilizzata per visualizzare le descrizioni specificate dall'utente, per certi file o tipi di file, negli elenchi della directory generati dal server. La direttiva AddDescription supporta l'elenco di file specifici, espressioni della wildcard, oppure estensioni del file.

10.5.49. ReadmeName

ReadmeName definisce il nome del file che viene aggiunto alla fine degli elenchi delle directory generati dal server. Il Web server cercherà prima di includere il file come documento HTML, poi come file di testo. Nella configurazione di default, ReadmeName è impostato su README.html.

10.5.50. HeaderName

HeaderName specifica il nome del file (se presente nella directory) che viene inserito all'inizio degli elenchi delle directory generati dal server. Come per ReadmeName, il server cerca, se possibile, di includere il file in formato HTML o altrimenti in formato di testo.

10.5.51. IndexIgnore

`IndexIgnore` elenca le estensioni del file, parti di nomi di file, espressioni wildcard o nomi di file completi. Il Web server non include alcun file che corrisponda a quei parametri negli elenchi delle directory generati dal server.

10.5.52. AddEncoding

`AddEncoding` definisce le estensioni dei file che hanno una particolare codifica. `AddEncoding` può essere utilizzato anche per indicare ai browser di decomprimere alcuni file mentre vengono scaricati.

10.5.53. AddLanguage

`AddLanguage` associa l'estensione di un file a una particolare lingua. Questa direttiva è particolarmente utile per Server HTTP Apache, quando il server restituisce un documento in base alla lingua di preferenza del client specificata nel browser.

10.5.54. LanguagePriority

`LanguagePriority` vi permette di stabilire una lingua prioritaria in caso il browser WEb del client non ha impostato alcuna lingua di preferenza.

10.5.55. AddType

Usare la direttiva `AddType` per definire o sovrascrivere un tipo MIME di default e coppie di estensione del file. Nell'esempio seguente la direttiva indica a Server HTTP Apache di riconoscere l'estensione del file `.tgz`.

```
AddType application/x-tar .tgz
```

10.5.56. AddHandler

`AddHandler` mappa l'estensione di un file per handler specifici. Per esempio, l'handler `cgi-script` può essere utilizzato in associazione con l'estensione `.cgi` per trattare un file che termina con `.cgi` automaticamente come script CGI. Il seguente é un esempio di direttiva `AddHandler` per l'estensione `.cgi`.

```
AddHandler cgi-script .cgi
```

Questa direttiva abilita CGI a funzionare esternamente `cgi-bin`, in qualsiasi altra directory sul server che possiede l'opzione `ExecCGI` all'interno del "cotainer" delle directory. Consultate la Sezione 10.5.22 per maggiori informazioni sull'impostazione dell'opzione `ExecCGI` per una directory.

Oltre agli script CGI, il vostro Web server utilizza anche `AddHandler` per elaborare gli HTML e i file imagemap analizzati dal server.

10.5.57. Action

`Action` specifica un tipo di contenuto MIME e una coppia di script CGI, in questo modo, quando viene richiesto un file di questo tipo, viene eseguito un particolare script CGI.

10.5.58. `ErrorDocument`

La direttiva `ErrorDocument` associa un codice di risposta HTTP con un messaggio o un URL da ritornare al client. Per default, il Web server emette un output di un messaggio di errore quando si verifica un errore. La direttiva `ErrorDocument` forza il Web server ad emettere un messaggio personalizzato o una pagina.

Importante

Per essere valido, il messaggio *deve* deve essere racchiuso in un paio di virgolette ["].

10.5.59. `BrowserMatch`

La direttiva `BrowserMatch` consente al server di definire le variabili di ambiente e/o le azioni sulla base del campo dell'intestazione HTTP User-Agent, che identifica il browser del client. Per default, il vostro server Web utilizza `BrowserMatch` per negare le connessioni a determinati browser con problemi noti e anche per disabilitare i keepalive e i comandi di annullamento delle intestazioni HTTP per i browser che hanno problemi con queste azioni.

10.5.60. `Location`

I tag `<Location>` e `</Location>` vi consentono di specificare il controllo dell'accesso in base all'URL.

Per esempio, per abilitare gli utenti al collegamento dall'interno del dominio del server, per vedere lo stato dei riport, usare le seguenti direttive:

```
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from <.example.com>
</Location>
```

Dovete sostituire *<.example.com>* con il nome del dominio di secondo livello.

Se desiderate fornire report sulla configurazione del server (inclusi i moduli installati e le direttive di configurazione) da richiedere all'interno del vostro dominio, usare le seguenti direttive:

```
<Location /server-info>
    SetHandler server-info
    Order deny,allow
    Deny from all
    Allow from <.example.com>
</Location>
```

Ed ancora, sostituite *<.example.com>* con il nome del dominio di secondo livello per il Web server.

10.5.61. `ProxyRequests`

Per configurare il Server HTTP Apache in modo da comportarsi come un server proxy, rimuovere (`#`) dall'inizio della riga `<IfModule mod_proxy.c>`, le ProxyRequests, e ogni riga nella sezione `<Proxy>`. Impostare la direttiva `ProxyRequests` su `On`, e impostare quale dominio è abilitato all'accesso del server, nella direttiva `Allow from` della sezione `<Proxy>`.

10.5.62. `Proxy`

I tag `<Proxy *> </Proxy>` creano un "cotainer" il quale racchiude un gruppo di direttive di configurazione che vengono applicate solo al server proxy. Molte direttive applicabili ad una directory possono essere usate all;interno dei tag `<Proxy>`.

10.5.63. Direttive della cache

Un numero di direttive commentate della cache, sono fornite dal file di configurazione di default del Server HTTP Apache. In molti casi non commentare queste righe, per fare ció é sufficiente rimuovere semplicemente il carattere (`#`) dall'inizio della riga. Quanto segue, rappresenta un elenco di alcune delle direttive piú importanti relative alla cache.

- 5`CacheEnable` — Specifica se la cache è un disco, una memoria, o un file descriptor cache. Per default `CacheEnable` configura una cache a disco per le URL su o al di sotto di `/`.
- `CacheRoot` — configura il nome della directory che conterrà i file memorizzati nella cache. La direttiva `CacheRoot` di default è la directory `/var/cache/httpd`.
- `CacheSize` — Specifica quanto spazio in kilobyte, puó essere usato dalla cache. Il default `CacheSize` é `5` KB.

Il seguente è un elenco di alcune delle direttive comuni inerenti alla cache.

- `CacheMaxExpire` — Specifica per quanto tempo i documenti HTML vengono trattenuti (senza un ricaricamento dal web server originario) nella cache. Il default é `24` ore `86400` secondi).
- `CacheLastModifiedFactor` — si occupa della creazione di una data di scadenza per un documento che non ne possieda una propria. Il valore di default per `CacheLastModifiedFactor` è `0.1`. Questo significa che la data di scadenza per questi documenti è pari a 1/10 della quantità di tempo trascorso dall'ultima modifica.
- `CacheDefaultExpire` — Specifica in ore la scadenza di un documento ricevuto tramite un protocollo che non supporta la data di scadenza. La configurazione di default è `1` ora (`3600` seconds).
- `NoProxy` — Specifica un elenco separato da uno spazio di sottoreti, indirizzi IP, domini, o di host i quali contenuti non sono stati conservati nella cache. Questa impostazione è molto utile per siti Intranet.

10.5.64. `NameVirtualHost`

La direttiva `NameVirtualHost` associa un indirizzo IP e un numero della porta, se necessario, per ogni host virtuale basato sul nome. La configurazione degli host virtuali basati sul nome, abilita un Server HTTP Apache a servire diversi domini senza usare indirizzi IP multipli.

Nota Bene

Ogni host virtuale basato sul nome funzionerà *solo* con connessioni HTTP non sicure, poichè non potete utilizzare host virtuali basati sui nomi con un server sicuro. In questo secondo caso, dovreste utilizzare host virtuali basati su indirizzi IP.

Per abilitare un host virtuale basato sul nome, decommentate la direttiva `NameVirtualHost` e aggiungete l'indirizzo IP corretto. Successivamente inserite delle sezioni `VirtualHost` aggiuntive per ogni host virtuale come richiesto dalla vostra configurazione..

10.5.65. `VirtualHost`

I tag `<VirtualHost>` e `</VirtualHost>` creano una sezione riportando le caratteristiche dell'host virtuale. La sezione `<VirtualHost>` accetta molte direttive di configurazione.

Una sezione `VirtualHost` commentata è presente in `httpd.conf`, il quale mostra il set minimo di direttive di configurazione necessario per ogni host virtuale. Consultare la Sezione 10.8 per maggiori informazioni inerenti gli host virtuali.

Nota Bene

La sezione dell'host virtuale SSL di default è stata spostata nel file `/etc/httpd/conf.d/ssl.conf`.

10.5.66. Direttive di configurazione per SSL

Le direttive nel file `/etc/httpd/conf.d/ssl.conf` possono essere configurate per abilitare comunicazioni Web sicure utilizzando SSL e TLS.

10.5.66.1. `SetEnvIf`

`SetEnvIf` imposta le variabili dell'ambiente basate sulle intestazioni di collegamenti in entrata. *Non* è solamente una direttiva SSL, anche se presente nel file `/etc/httpd/conf.d/ssl.conf`. Il suo scopo è quello di disabilitare i keepalive HTTP e di permettere al protocollo SSL di chiudere la connessione senza un messaggio di avvertimento da parte del browser client. Questa impostazione è necessaria per alcuni browser che non chiudono in modo affidabile la connessione SSL.

Per maggiori informazioni su altre direttive all'interno del file di configurazione SSL, consultate i seguenti URL:

- http://localhost/manual/mod/mod_ssl.html
- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html

Per informazioni sulla configurazione di un server sicuro HTTP Apache, consultate il capitolo relativo alla *configurazione di un server sicuro HTTP Apache* nella *Red Hat Enterprise Linux System Administration Guide*.

Nota Bene

In molti casi, le direttive SSL sono configurate in modo appropriato durante l'installazione di Red Hat Enterprise Linux. Fate attenzione nell'alterare le direttive del server sicuro HTTP di Apache, in quanto configurarlo in modo non corretto puó compromettere la sicurezza del vostro sistema.

10.6. Moduli predefiniti

Nel Server HTTP Apache sono disponibili alcuni moduli. Per default i moduli indicati qui di seguito sono installati e abilitati con il pacchetto `httpd` in Red Hat Enterprise Linux4:

```
mod_access
mod_actions
mod_alias
mod_asis
mod_auth
mod_auth_anon
mod_auth_dbm
mod_auth_digest
mod_auth_ldap
mod_autoindex
mod_cache
mod_cern_meta
mod_cgi
mod_dav
mod_dav_fs
mod_deflate
mod_dir
mod_disk_cache
mod_env
mod_expires
mod_ext_filter
mod_file_cache
mod_headers
mod_imap
mod_include
mod_info
mod_ldap
mod_log_config
mod_logio
mod_mem_cache
mod_mime
mod_mime_magic
mod_negotiation
mod_proxy
mod_proxy_connect
mod_proxy_ftp
mod_proxy_http
mod_rewrite
mod_setenvif
mod_speling
mod_status
mod_suexec
mod_unique_id
mod_userdir
mod_usertrack
```

```
mod_vhost_alias
```

Sono inoltre disponibili i moduli seguenti installando pacchetti aggiuntivi:

```
mod_auth_kerb
mod_auth_mysql
mod_auth_pgsql
mod_authz_ldap
mod_dav_svn
mod_jkz
mod_perl
mod_python
mod_ssl
php
```

10.7. Aggiunta di moduli

Il Server HTTP Apache supporta *Dynamically Shared Objects* (*DSO*s) o moduli, i quali possono essere facilmente caricati se necessario al momento dell'esecuzione.

Il progetto Apache fornisce una documentazione DSO completa all'indirizzo http://httpd.apache.org/docs-2.0/dso.html. Oppure, se il pacchetto `http-manual` è installato, potete anche reperire la documentazione sui DSO all'indirizzo http://localhost/manual/mod/.

Affinchè il Server HTTP Apache utilizzi un DSO, esso deve essere specificato in una direttiva`LoadModule` all'interno di `/etc/httpd/conf/httpd.conf`. Se il modulo viene fornito da un pacchetto separato, la riga deve apparire all'interno del file di configurazione dei moduli nella directory `/etc/httpd/conf.d/`. Consultate la Sezione 10.5.12 per maggiori informazioni.

Se aggiungete o eliminate dei moduli dal file `http.conf`, dovete ricaricare o riavviare il Server HTTP Apache, come descritto nella Sezione 10.4.

Se create un nuovo modulo, installate prima il pacchetto `httpd-devel` in quanto contiene i file include, i file d'intestazione e l'applicazione *APache eXtenSion* (`/usr/sbin/apxs`), la quale utilizza i file include e quelli d'intestazione per compilare i DSO.

Dopo aver scritto un modulo, usare `/usr/sbin/apxs` per compilare le sorgenti del modulo esterne all'albero della sorgente di Apache. Per maggiori informazioni sul comando `/usr/sbin/apxs`, consultate la documentazione di Apache all'indirizzo http://httpd.apache.org/docs-2.0/dso.html e la pagina man `apxs`.

Dopo aver compilato il vostro modulo, inseritelo nella directory `//usr/lib/httpd/modules/`. Inserite poi una linea `LoadModule` nel file `httpd.conf`, usando la seguente struttura:

```
LoadModule <module-name> <path/to/module.so>
```

Dove *<module-name>* è il nome del modulo e *<path/to/module.so>* è il percorso per il DSO.

10.8. Host virtuali

Il virtual hosting interno del Server HTTP Apache permette ai server di fornire diverse informazioni basate sulla richiesta degli indirizzi IP, hostname, o delle porte. Una guida completa sull'utilizzo di host virtuali è disponibile su http://httpd.apache.org/docs-2.0/vhosts/.

10.8.1. Configurazione degli host virtuali

Per creare un host virtuale basato sul nome, é meglio usare il container dell'host virtuale presente con `httpd.conf` come esempio.

Il suddetto esempio di host virtuale viene letto in modo seguente:

```
#NameVirtualHost *:80
#
#<VirtualHost  *:80>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
```

Per attivare un host virtuale basato sul nome, eliminate il commento dalla riga `NameVirtualHost`, per fare ció rimuovere il carattere (`#`) e sostituire l'asterisco (`*`) con l'indirizzo IP assegnato alla macchina.

Successivamente, configurate un host virtuale decommentando e personalizzando la sezione `<VirtualHost>`.

Sulla riga `<VirtualHost>`, cambiare l'asterisco (`*`) nell'indirizzo IP del server. Cambiare il `ServerName` con un nome del DNS *valido* assegnato alla macchina, e configurare le altre direttive come necessario.

Il "container" `<VirtualHost>` é altamente personalizzabile e accetta quasi ogni direttiva disponibile all'interno della configurazione del server principale.

Suggerimento

Se state configurando un host virtuale in ascolto su di una porta che non sia quella di default, la stessa porta deve essere aggiunta alla direttiva `Listen` nella sezione delle impostazioni globali del file `/etc/httpd/conf/http.conf`.

Per attivare un host virtuale appena creato, il Server HTTP Apache deve essere ricaricato e riavviato. Consultate la Sezione 10.4 per maggiori informazioni.

Informazioni complete sulla creazione e configurazione degli host virtuali basati sul nome e sull'indirizzo IP, vengono fornite online su http://httpd.apache.org/docs-2.0/vhosts/.

10.8.2. Host virtuali del Web server sicuro

Per default, il Server HTTP Apache è configurato sia come server non sicuro che come server sicuro. Entrambi i server utilizzano lo stesso indirizzo IP e lo stesso hostname, ma sono in ascolto su porte diverse: rispettivamente 80 e 443. Questo abilita le comunicazioni sicure e non sicure simultaneamente.

Un aspetto del miglioramento SSL delle trasmissioni HTTP, è quello di usare molte più risorse rispetto ai protocolli HTTP standard, in questo modo un server sicuro non è in grado di servire un numero elevato di pagine al secondo. Per questa ragione è sempre buona idea minimizzare le informazioni disponibili dal server sicuro, soprattutto su di un sito web molto trafficato.

Importante

Non usare gli host virtuali basati sul nome insieme con un server Web sicuro in quanto l'"handshake SSL" avviene prima che la richiesta HTTP identifica l'appropriato host virtuale basato sul nome. Gli host virtuali basati sul nome funzionano solo con server Web non sicuri.

Le direttive di configurazione per il server sicuro, sono contenuti all'interno dei tag dell'host virtuale nel file `/etc/httpd/conf.d/ssl.conf`.

Per default, i Web server sicuri e non sicuri condividono la stessa `DocumentRoot`. É consigliato che `DocumentRoot` sia diverso per il Web server sicuro.

Per far sì che il Web server non sicuro non accetti il collegamento, commentare la riga in `httpd.conf`, la quale legge `Listen 80`, posizionando il carattere (`#`) all'inizio della riga stessa. Fatto ciò, la riga sarà simile al seguente esempio:

```
#Listen 80
```

Per maggiori informazioni sulla configurazione di un Web server con maggiore SSL, consultare il capitolo intitolato *Configurazione del server sicuro HTTP di Apache* nella *Red Hat Enterprise Linux System Administration Guide*. Per suggerimenti inerenti una configurazione avanzata, fare riferimento alla documentazione Apache Software Foundation, disponibile sui seguenti URL:

- http://httpd.apache.org/docs-2.0/ssl/
- http://httpd.apache.org/docs-2.0/vhosts/

10.9. Risorse aggiuntive

Per saperne di più su Server HTTP Apache, consultate le fonti seguenti.

10.9.1. Siti Web utili

- http://httpd.apache.org/ — Il sito Web ufficiale per il Server HTTP Apache con tutta la documentazione relativa alle direttive e ai moduli di default.
- http://www.modssl.org/ — Il sito Web ufficiale di `mod_ssl`.
- http://www.apacheweek.com/ — Una newsletter settimanale online completa su tutto ciò che riguarda Apache.

10.9.2. Libri correlati

- *Apache Desktop Reference* di Ralf S. Engelschall; Addison Wesley — Scritto da Ralf EngelSchall, membro dell'ASF e autore di mod_ssl, *Apache Desktop Reference* rappresenta una guida di riferimento concisa ma esauriente su come usare Apache durante le fasi di compilazione, configurazione ed esecuzione. È possibile scaricare la versione online di questo libro all'indirizzo http://www.apacheref.com/.
- *Professional Apache* di Peter Wainwright; Wrox Press Ltd — *Professional Apache* uno dei numerosi libri della collana Wrox Press Ltd's "Programmer to Programmer" e si rivolge agli utenti esperti e agli amministratori dei server Web che si apprestano a utilizzare Apache per la prima volta.

- *Administering Apache* di Mark Allan Arnold; Osborne Media Group — Questo libro si rivolge a quei provider di servizi Internet che desiderano fornire servizi più sicuri.
- *Apache Server Unleashed* di Richard Bowen, et al; SAMS BOOKS — Una risorsa enciclopedica per Server HTTP Apache.
- *Apache Pocket Reference* di Andrew Ford, Gigi Estabrook; O'Reilly — L'ultimo aggiornamento della collana O'Reilly Pocket.
- *Red Hat Enterprise Linux System Administration Guide*; Red Hat, Inc. — Contiene un capitolo su come configurare Server HTTP Apache usando **Strumento di configurazione di HTTP**, e un capitolo su come configurare il server sicuro Server HTTP Apache.
- *Red Hat Enterprise Linux Security Guide*; Red Hat, Inc. — Il capitolo *Sicurezza del server*, spiega come rendere sicuro Server HTTP Apache e altri servizi.

Capitolo 11.

E-mail

La nascita della posta elettronica (*email*) risale al 1960. Il mailbox era un file nella home directory dell'utente ed era leggibile solo dall'utente in questione. Le prime applicazioni di posta allegavano nuovi messaggi di testo nella parte inferiore del file, e l'utente doveva ricercare all'interno del file quel particolare messaggio. Questo sistema era solo in grado di inviare messaggi agli utenti sullo stesso sistema.

Il primo vero trasferimento di rete di un messaggio di posta elettronica, è avvenuto nel 1971, quando un ingegnere di computer chiamato Ray Tomlinson inviò un messaggio prova tra due macchine tramite ARPANET — il precursore a Internet. La comunicazione tramite email, diventò presto molto popolare, raggiungendo il 75 per cento del traffico di ARPANET in meno di 2 anni.

Oggi, il sistema email basati su protocolli di rete standardizzati si sono evoluti in uno dei servizi piú diffusi di Internet. Red Hat Enterprise Linux offre molte applicazioni avanzate per servire ed accedere alle email.

Questo capitolo tratta i protocolli e-mail attualmente più diffusi e alcuni programmi ideati per le operazioni di posta elettronica.

11.1. Protocolli Email

Oggi, l'email viene consegnata usando una architettura client/server. Un messaggio email é creato usando un programma client di posta. Questo programma poi, invia il messaggio a un server. Il server a sua volta inoltra il messaggio al server email del ricevente, dove il messaggio viene fornito al client email dello stesso.

Per abilitare questo processo, vi sono un certo numero di protocolli di rete standard che permettono a macchine diverse, che spesso eseguono sistemi operativi diversi e usano diversi programmi email, di inviare e ricevere email.

I seguenti protocolli sono fra i più comunemente utilizzati per il trasferimento di e-mail da un sistema all'altro.

11.1.1. Protocolli di trasporto posta

La consegna della posta da una applicazione client al server, e da un server originatore al server destinatario, è gestita dal *Simple Mail Transfer Protocol* (*SMTP*).

11.1.1.1. SMTP

Lo scopo primario di SMTP è quello di trasferire le email tra i server di posta. Tuttavia, è una fase critica anche per i client email. Per poter inviare le email, il client invia il messaggio ad un server di posta in uscita, il quale contatta il server di posta destinatario per la consegna. Per questa ragione, è necessario specificare un server SMTP quando si configura un client email.

Con Red Hat Enterprise Linux, un utente può configurare un server SMTP sulla macchina locale per gestire la consegna della posta. Tuttavia, è possibile anche configurare server SMTP remoti per la posta in uscita.

É inoltre importante puntualizzare che il protocollo SMTP non richiede una autenticazione. Questo permette a chiunque su Internet, di inviare email ad chiunque oppure a un gruppo molto grande di persone. É questa caratteristica di SMTP che rende possibile la cosí detta posta indesiderata o *spam*. I server SMTP moderni cercano di minimizzare questo comportamento, abilitando all'accesso solo host conosciuti. Questi server che non abilitano una tale restrizione vengono chiamati server *open relay*.

Per default, Sendmail (`/usr/sbin/sendmail`) è il programma SMTP di default sotto Red Hat Enterprise Linux. Tuttavia è anche disponibile un'applicazione piú semplice di server mail chiamata Postfix (`/usr/sbin/postfix`).

11.1.2. Mail Access Protocols

Sono presenti due protocolli primari usati dalle applicazioni client email per riprendere le email dai server di posta: il *Post Office Protocol* (*POP*) e *Internet Message Access Protocol* (*IMAP*).

Diversamente da SMTP, entrambi questi protocolli richiedono ai client collegati una autenticazione usando il nome utente e una password. Per default, le password per entrambi i protocolli sono passete attraverso la rete in chiaro.

11.1.2.1. POP

Il server POP di default con Red Hat Enterprise Linux è `/usr/sbin/ipop3d` ed è fornito dal pacchetto `imap`. Quando si usa un server POP, i messaggi email sono scaricati dalle applicazioni client email. Per default, la maggior parte dei client POP è configurata per l'eliminazione del messaggio sul server eameil dopo che questo è stato trasferito con successo, tuttavia questa impostazione può essere modificata.

POP é completamente compatibile con importante messaggistica Internet standard, come ad esempio *Multipurpose Internet Mail Extensions* (*MIME*), che permette di inserire gli allegati.

Il POP funziona meglio per utenti che hanno un sistema sul quale leggere la email. Lavora bene anche per utenti che non hanno una connessione persistente a Internet oppure una rete contenente il server posta. Sfortunatamente per quelli che hanno una connessione di rete lenta, POP richiede programmi client previa autenticazione, per scaricare l'intero contenuto di ogni messaggio. Questo puó richiedere molto tempo se un messaggio ha un allegato molto grande.

La versione piú recente del protocollo POP standard é POP3.

Ci sono tuttavia diverse varianti riguardanti i protocolli POP, usate meno frequentemente:

- *APOP* — POP3 con autenticazione MDS, in cui il client e-mail invia al server la password criptata e non in chiaro.
- *KPOP* — POP3 con l'autenticazione di Kerberos. Per ulteriori informazioni, consultate il Capitolo 19.
- *RPOP* — POP3 con autenticazione RPOP, utilizza un'ID per ogni utente, simile a una password, per autenticare le richieste del POP. L'ID non è tuttavia criptato, quindi RPOP non è più sicuro di un POP standard.

Per aumentare la sicurezza, é possibile usare il metodo di cifratura *Secure Socket Layer* (*SSL*) per autenticazione del client e per le sessioni di trasferimento dati. Questo può essere abilitato usando il servizio `ipop3s`, oppure usando il programma `/usr/sbin/stunnel`. Consultare la Sezione 11.5.1 per maggiori informazioni.

11.1.2.2. IMAP

Il server IMAP di default con Red Hat Enterprise Linux è `/usr/sbin/imapd` e viene fornito dal pacchetto `imap`. Quando si utilizza un server mail IMAP, i messaggi di posta elettronica rimangono sul server, dove l'utente può leggerli o cancellarli, e creare, rinominare o eliminare le directory mail presenti sul server, in modo da organizzare e conservare le email.

L'IMAP è utilizzato principalmente da utenti che possono accedere alle e-mail mediante più computer. Gli utenti connessi a Internet o a una rete privata mediante connessione a banda bassa utilizzano spesso

questo protocollo, poiché inizialmente visualizza le informazioni di testo del messaggio. Allo stesso modo, l'utente può cancellare i messaggi e-mail indesiderati senza visualizzare il corpo del messaggio, evitando addirittura di scaricarlo durante la connessione.

Per convenienza, le applicazioni client IMAP sono capaci di ottenere delle copie di messaggi in modo locale, in modo tale da permettere all'utente di controllare i messaggi letti precedentemente, anche non essendo collegato direttamente al server IMAP.

IMAP, come POP, é compatibile con importanti messaggi standard, come ad esempio MIME, il quale permette la creazione di allegati.

Per aumentare la sicurezza, é possibile usare il metodo di cifratura *Secure Socket Layer* (*SSL*) per autenticazione del client e per le sessioni di trasferimento dati. Questo puó essere abilitato usando il servizio `imaps`, oppure usando il programma `/usr/sbin/stunnel`. Consultare la Sezione 11.5.1 per maggiori informazioni.

Altri client e server IMAP sono disponibili sia gratis che a pagamento, molti dedi quali estendono il protocollo IMAP e forniscono delle funzioni aggiuntive. Un elenco completo puó essere trovato su http://www.imap.org/products/longlist.htm.

11.2. Tipi di programmi e-mail

In generale, esistono tre tipi di programmi e-mail, ciascuno dei quali svolge un ruolo specifico nel processo di trasferimento e gestione dei messaggi di posta elettronica. La maggior parte degli utenti conosce solo il programma e-mail usato specificatamente per ricevere e inviare i messaggi, ma perché il messaggio arrivi al corretto destinatario sono fondamentali tutti e tre.

11.2.1. Mail Transfer Agent

Un *Mail Transfer Agent* (*MTA*) rende possibile il trasferimento dei messaggi email tra host usando SMTP. Un messaggio puó interessare diversi MTA mentre si sposta verso la destinazione desiderata.

Anche se la consegna dei messaggi tra computer sembra molto semplice, in realtà l'intero processo necessario per decidere se un particolare MTA può o dovrebbe accettare un messaggio per la consegna, è piuttosto complicato. Inoltre, a causa di problemi dovuti allo spam, l'uso di un MTA specifico è in genere limitato dalla sua stessa configurazione o dalla configurazione di accesso per la rete sulla quale risiede.

Molti programmi client email moderni possono essere usati come un MTA durante l'invio di email. Tuttavia, la suddetta azione non deve essere confusa con i compiti di un MTA vero e proprio. La sola ragione per la quale i programmi client email sono capaci di inviare email come un MTA, é dovuto dal fatto che l'host che esegue l'applicazione non presenta il proprio MTA. Questo é particolarmente vero per programmi client email su sistemi operativi non-Unix. Tuttavia, questi programmi client possono inviare solo messaggi in uscita ad un MTA che essi hanno autorizzato ad usare e non consegnano direttamente il messaggio al server email ricevente desiderato.

Piochè Red Hat Enterprise Linux installa due MTA, Sendmail e Postfix, i programmi client email non vengono spesso chiamati a comportarsi come un MTA. Red Hat Enterprise Linux include anche un MTA con compiti speciali chiamato Fetchmail.

Per maggiori informazioni su Sendmail, Postfix e Fetchmail, consultate la Sezione 11.3.

11.2.2. Mail Delivery Agent

Il *Mail Delivery Agent (MDA)* è utilizzato dall'MTA per consegnare le e-mail a una mailbox specifica di un utente. In molti casi, l'MDA è di fatto un *Local Delivery Agent (LDA)*, come ad esempio `mail` o Procmail.

Tutti i programmi che gestiscono un messaggio da consegnare fino al punto in cui può essere letto da un MUA possono essere considerati MDA. Per questa ragione, alcuni MTA (come ad esempio Sendmail e Postfix) possono ricoprire il ruolo di un MDA quando aggiungono nuovi messaggi email ad un file spool di posta dell'utente locale. In generale, é importante ricordare che gli MDA non trasportano messaggi tra sistemi o interfacce; MDA distribuisce messaggi sulla macchina locale per far accedere una applicazione client email.

11.2.3. Mail User Agent

Un *Mail User Agent* (*MUA*) é sinonimo di applicazione client email. É un programma che consente all'utente di leggere e scrivere messaggi e-mail. Molti MUA permettono all'utente di svolgere altri compiti, fra cui il reperimento di messaggi attraverso i protocolli POP o IMAP, l'impostazione di mailbox per archiviare i messaggi e il passaggio delle nuove e-mail a un programma Mail Transfer Agent.

I programmi MUA possono essere grafici, come **Mozilla Mail**, oppure possono avere una interfaccia semplice, basata sul testo, come ad esempio `mutt`.

11.3. Mail Transport Agents

Red Hat Enterprise Linux include due MTA primari, Sendmail e Postfix. Il primo é configurato come il default di MTA, anche se è facile cambiare l'MTA di default su Postfix.

Suggerimento

Per informazioni su come impostare Postfix invece di Sendmail per l'MTA di default, consultate il capitolo relativo alla *configurazione dell'MTA (Mail Transport Agent)* nella *Red Hat Enterprise Linux System Administration Guide*.

11.3.1. Sendmail

Lo scopo di Sendmail, come gli altri MTA, é di trasferire in sicurezza le email tra gli host, generalmente usando il protocollo SMTP. Tuttavia, Sendmail é altamente configurabile, permettendo il controllo su quasi tutti gli aspetti di come viene gestita la email, incluso il protocollo usato. Molti amministratori di sistema scelgono di usare Sendmail come il loro MTA a causa della sua potenza e scalabilitá.

11.3.1.1. Scopi e limiti

Conoscere Sendmail e i suoi possibili usi diventa molto importante per gli utenti. Al giorno d'oggi, per via della preponderanza di applicazioni monolitiche che svolgono molteplici compiti, l'utente potrebbe erroneamente pensare a Sendmail come l'unica applicazione necessaria per un server mail all'interno della propria organizzazione. Tecnicamente, ciò corrisponde a verità, poiché Sendmail esegue la distribuzione della posta alle directory dei diversi utenti, eseguendo anche la consegna dei messaggi in uscita agli utenti stessi. Tuttavia la maggior parte degli utenti necessita qualcosa di più che la semplice consegna di posta. Vuole interagire con il servizio di posta elettronica usando un MUA

che utilizza POP o IMAP per scaricare i messaggi sul computer locale o preferire una interfaccia Web per accedere alla propria mailbox. Queste applicazioni aggiuntive funzionano insieme a Sendmail e SMTP, ma il loro scopo è differente e possono operare separatamente le une dalle altre.

Questa sezione non prevede l'approfondimento di Sendmail e di come potrebbe o dovrebbe essere configurato. Vi sono centinaia di opzioni e regole differenti e interi volumi che illustrano le potenzialità di Sendmail e le soluzioni ai suoi problemi. Consultare la Sezione 11.6 per un elenco delle risorse di Sendmail.

È comunque importante capire quali file vengono installati per default con Sendmail sul vostro sistema, come effettuare modifiche di base alla sua configurazione o come bloccare la posta indesiderata (spam) e ampliare Sendmail mediante il protocollo *Lightweight Directory Access Protocol (LDAP)*.

11.3.1.2. Installazione predefinita di Sendmail

L'eseguibile di Sendmail é `/usr/sbin/sendmail`.

Il lungo e dettagliato file di configurazione di Sendmail é `/etc/mail/sendmail.cf`. Evitate di modificare direttamente il file `sendmail.cf`. Invece, per apportare delle modifiche a Sendmail è preferibile modificare il file `/etc/mail/sendmail.mc`, eseguire un backup del file originale `/etc/mail/sendmail.cf`, e usare il macro processore `m4` per creare un nuovo `/etc/sendmail.cf`. Ulteriori informazioni sulla configurazione di Sendmail sono disponibili nella Sezione 11.3.1.3.

Diversi file di configurazione di Sendmail sono installati in `/etc/mail`,

- `access` — Specifica quali sistemi possono utilizzare Sendmail per la posta in uscita.
- `domaintable` — Consente di fornire la mappatura del nome del dominio.
- `local-host-names` — Il punto in cui si indicano tutti gli alias per gli host.
- `mailertable` — specifica le istruzioni per superare il routing per particolari domini.
- `virtusertable` — Consente di eseguire una forma di aliasing specifica per dominio e quindi posizionare domini virtuali multipli su un computer.

Diversi file di configurazione in `/etc/mail`, fra cui `access`, `domaintable`, `mailertable` e `virtusertable`, devono archiviare le informazioni nei file del database prima che Sendmail possa adottare qualsiasi modifica della configurazione. Per includere tali modifiche nei file del database, è necessario eseguire il comando:

```
makemap hash /etc/mail/<name> < /etc/mail/<name>
```

dove *<name>* viene sostituito con il nome del file di configurazione da convertire.

Se, per esempio, volete indirizzare tutte le e-mail a un account `example.com` perché siano consegnate a <`bob@other-example.com`>, sarà necessario aggiungere una riga simile a quella riportata di seguito al file `virtusertable`:

```
@example.com      bob@other-example.com
```

Per finalizzare il cambiamento, il file `virtusertable.db` deve essere aggiornato usando il seguente comando come root:

```
makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable
```

In questo modo creerete un nuovo `virtusertable.db` contenente la nuova configurazione.

11.3.1.3. Modifiche comuni alla configurazione di Sendmail

Quando modificate il file di configurazione di Sendmail, è meglio non modificare un file esistente, ma creare un nuovo file `/etc/mail/sendmail.cf`.

Attenzione

Prima di effettuare modifiche al file `sendmail.cf`, è consigliabile eseguire una copia di backup.

Per aggiungere la funzionalità desiderata a Sendmail, modificate il file `/etc/mail/sendmail.mc` come utente root. Fatto ciò, utilizzate il macro processore `m4` per generare un nuovo file `sendmail.cf`, eseguendo il seguente comando:

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

Per default, il macro processore `m4` viene installato con Sendmail ed è incluso nel pacchetto `m4`.

Dopo la creazione di un nuovo `/etc/mail/sendmail.cf`, riavviate Sendmail affinché le modifiche siano effettive. Il modo più semplice per fare ciò è quello di digitare il seguente comando:

```
/sbin/service sendmail restart
```

Importante

La versione di default di `sendmail.cf` non consente a sendmail di accettare collegamenti di rete da host diversi da quelli del computer locale. Se desiderate configurare sendmail come server per altri client, dovete modificare `/etc/mail/sendmail.mc` e cambiare l'indirizzo specificato nell'opzione `Addr=` della direttiva `DAEMON_OPTIONS` da `127.0.0.1` all'indirizzo IP di un dispositivo attivo della rete, o decommentare la direttiva `DAEMON_OPTIONS` posizionando `dnl` all'inizio della riga. Una volta terminato, rigenerare `/etc/mail/sendmail.cf` eseguendo il comando di seguito riportato:

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

La configurazione di default presente con Red Hat Enterprise Linux funziona per la maggior parte dei siti SMTP. Tuttavia non funziona per siti UUCP (UNIX ad una copia UNIX). Se si utilizzano i trasferimenti mail UUCP, il file `/etc/mail/sendmail.mc` deve essere riconfigurato, generando anche un nuovo `/etc/mail/sendmail.cf`.

Si consiglia di consultare il file `/usr/share/sendmail-cf/README` prima di modificare i file contenuti nelle sottodirectory di `/usr/share/sendmail-cf`, poiché possono influire sulle future configurazioni dei file `/etc/mail/sendmail.cf`.

11.3.1.4. Masquerading

Una configurazione comune di Sendmail è rappresentata da un singolo computer che si comporta da gateway mail per tutte le macchine sulla rete. Per esempio, un'azienda potrebbe chiamare una macchina `mail.example.com` che si occupa della gestione della posta elettronica e dell'assegnazione di un indirizzo del mittente per tutta la posta in uscita.

In questa situazione il server Sendmail deve mascherare i nomi del computer sulla rete della compagnia per fare in modo che l'indirizzo del mittente sia `user@example.com` invece di `user@host.example.com`.

Per effettuare questa operazione, aggiungete le righe riportate di seguito al file `/etc/mail/sendmail.mc`.

```
FEATURE(always_add_domain)dnl
FEATURE('masquerade_entire_domain')
FEATURE('masquerade_envelope')
FEATURE('allmasquerade')
MASQUERADE_AS('bigcorp.com.')
MASQUERADE_DOMAIN('bigcorp.com.')
MASQUERADE_AS(bigcorp.com)
```

Dopo avere generato un nuovo file `sendmail.cf` mediante `m4`, questa configurazione consentirà a tutta la posta presente all'interno della rete, di essere visualizzata come se fosse inviata da `bigcorp.com`.

11.3.1.5. Neutralizzazione dei massaggi indesiderati

Email spam puó essere definito come una email non necessaria e non voluta dall'utente che non ha mai richiesto una comunicazione. Esso rappresenta il modo errato di utilizzare le comunicazioni standard di Internet.

Sendmail facilita il blocco delle nuove tecniche spamming usate per inviare la posta indesiderata. É capace di bloccare, per default, molti metodi spamming.

Per esempio, l'inoltro dei messaggi SMTP, definito anche relaying, è stato disabilitato per default a partire dalla versione 8.9 di Sendmail. Prima che si verificasse questa modifica, Sendmail indicava al mail host (`x.edu`) di accettare i messaggi provenienti da un gruppo (`y.com`) e a inviarli ad un altro gruppo (`z.net`). Oggi, tuttavia, Sandmail deve essere configurato in modo da permettere a qualsiasi dominio di trasmettere posta attraverso il server. Per configurare i domini di trasmissione, modificate il file `/etc/mail/relay-domains` e riavviate Sendmail.

Accade spesso, tuttavia, che i vostri utenti siano bombardati da spam provenienti da altri server su Internet, i quali sfuggono al vostro controllo. In questi casi, utilizzate le caratteristiche di controllo agli accessi di Sendmail disponibili mediante il file `/etc/mail/access`. Il seguente esempio mostra come puó essere usato questo file sia per bloccare e sia per abilitare specificamente l'accesso al server Sendmail:

```
badspammer.com        ERROR:550 "Go away and do not spam us anymore"
tux.badspammer.com    OK
10.0                  RELAY
```

Questo esempio mostra che qualsiasi e-mail inviata da `badspammer.com` sarà bloccata con un codice d'errore 550 RFC-821e rimandata allo spammer. Le email inviate dal sottodominio `tux.badspammer.com` vengono accettate. L'ultima riga indica che qualsiasi e-mail inviata dalla rete 10.0.*.* può essere trasmessa dal mail server.

Poiché `/etc/mail/access.db` é un database, usare `makemap` per attivare qualsiasi cambiamento. Fate questo usando il seguente comando come un utente root:

```
makemap hash /etc/mail/access < /etc/mail/access
```

Questo esempio si limita a rappresentare solo una parte di quello che Sendmail è in grado di fare in termini di concessione o blocco dell'accesso. Consultate `/usr/share/sendmail-cf/README` per informazioni dettagliate ed alcuni esempi.

Poichè Sendmail chiama il Procmail MDA quando consegna la posta, é anche possibile usare un programma di filtro spam, come ad esempio SpamAssassin, in modo da identificare ed eseguire un file spam, per gli utenti in questione. Consultate la Sezione 11.4.2.6 per maggiori informazioni sull'uso di SpamAssassin.

11.3.1.6. Utilizzo di Sendmail con LDAP

Il protocollo *Lightweight Directory Access Protocol (LDAP)* fornisce un metodo veloce e potente per trovare informazioni su un utente specifico proveniente da un gruppo più ampio. È possibile, per esempio, utilizzare un server LDAP per cercare un indirizzo e-mail specifico in una directory comune aziendale partendo dal cognome dell'utente. In questo tipo d'implementazione il protocollo LDAP, ampiamente separato da Sendmail, archivia le informazioni gerarchiche sull'utente mentre Sendmail riceve solo il risultato delle query LDAP in messaggi e-mail pre-indirizzati.

Sendmail supporta un'integrazione maggiore con LDAP, in cui utilizza il protocollo per sostituire file mantenuti separatamente, fra cui `aliases` e `virtusertables`, su mail server differenti che funzionano insieme per supportare una azienda che opera a livello medio-grande. In breve, il protocollo LDAP può essere utilizzato per analizzare il livello di routing della posta di Sendmail e i file di configurazione separati in un potente cluster LDAP, potenziato da differenti applicazioni.

La versione attuale di Sendmail include il supporto per LDAP. Per ampliare il server Sendmail usando LDAP, procurarsi prima un server LDAP, come **OpenLDAP**, funzionante e correttamente configurato. Modificate quindi `/etc/mail/sendmail.mc` per includere:

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

Nota Bene

La presente è valida solo per una configurazione elementare di Sendmail con LDAP. La configurazione può differire in modo sostanziale a seconda del tipo d'implementazione di LDAP, soprattutto se desiderate configurare diverse macchine Sendmail per usare un server LDAP comune.

Consultate `/usr/share/sendmail-cf/README` per istruzioni dettagliate riguardo alla configurazione del routing LDAP ed esempi connessi.

Successivamente, ricreate il file `/etc/mail/sendmail.cf` eseguendo il comando `m4` e riavviando Sendmail. Per informazioni, consultate la Sezione 11.3.1.3.

Per ulteriori informazioni sul protocollo LDAP, consultate il Capitolo 13.

11.3.2. Postfix

Sviluppato originariamente da IBM da esperti e programmatori Wietse Venema, Postfix è un MTA compatibile con Sendmail creato per essere sicuro, veloce, e facile da configurare.

Per migliorare la sicurezza Postfix utilizza un design modulare, dove vengono lanciati, da un demone *master*, piccoli processi con privilegi limitati. I processi più piccoli e meno privilegiati, eseguono compiti specifici inerenti alle varie fasi di consegna della posta, e vengono eseguiti in un ambiente 'rooted', per limitare gli effetti dovuti agli attacchi.

Per configurare Postfix in modo da accettare i collegamenti di rete da host diversi da quelli del computer locale, bisogna eseguire solo alcuni piccoli cambiamenti sul prorpio file di configurazione. Per quelli che hanno delle esigenze particolari, Postfix fornisce una varietà di opzioni per la configurazione, insieme con delle opzioni di terzi, che rendono MTA molto versatile e pieno di contenuti.

I file di configurazione per Postfix, sono leggibili dagli utenti e supportano più di 250 direttive. A differenza di Sendmail, non è richiesta alcuna processazione macro per confermare i cambiamenti, e la maggior parte delle opzioni più comunemente usate, sono descritte nei file ampiamentecommentati.

Importante

Prima di usare Postfix, l'MTA di default deve essere smistato da Sandmail a Postfix. Consultate il capitolo relativo alla *configurazione di Mail Transport Agent (MTA)* nella *Red Hat Enterprise Linux System Administration Guide* per maggiori informazioni.

11.3.2.1. Installazione di default di Postfix

L'eseguibile di Postfix è `/usr/sbin/postfix`. Questo demone lancia tutti i processi relativi, necessari per gestire la consegna della posta.

Postfix conserva i propri file di configurazione nella directory `/etc/postfix/`. Il seguente è un elenco dei file più comunemente usati:

- `access` — Usato per controllare l'accesso, questo file specifica gli host autorizzati al collegamento a Postfix.
- `aliases` — Un elenco configurabile necessario per il protocollo di posta.
- `main.cf` — Il file di configurazione Postfix globale. La maggior parte delle opzioni di configurazione sono specificate in questo file.
- `master.cf` — Specifica come Postfix interagisce con i diversi processi per portare a termine la consegna della posta.
- `transport` — Mappa gli indirizzi email agli host di trasmissione.

Importante

Il file `/etc/postfix/main.cf` di default, non permette a Postfix di accettare i collegamenti di rete da un host diverso dal computer locale. Per istruzioni su come configurare Postfix come server per altri client, consultare la Sezione 11.3.2.2.

Quando si cambiano altre opzioni all'interno dei file presenti nella directory `/etc/postfix/`, per poter confermare i suddetti cambiamenti potrebbe essere necessario riavviare il servizio `postfix`. Il modo più semplice per fare ciò, è quello di digitare il seguente comando:

```
/sbin/service postfix restart
```

11.3.2.2. Configurazione Postfix di base

Per default, Postfix non accetta i collegamenti di rete da un host diverso da quello locale. Eseguire le seguenti fasi come utente root, per poter abilitare la consegna della posta per altri host presenti sulla rete:

- Modificare il file `/etc/postfix/main.cf` con un editor di testo, come ad esempio `vi`.
- Decommentare la riga `mydomain`, rimuovendo il carattere (`#`), e sostituire *`domain.tld`* con il dominio che il server mail stà servendo, come ad esempio `example.com`.
- Decommentare la riga `myorigin = $mydomain`.
- Decommentare la riga `myhostname`, e sostituire *`host.domain.tld`* con l'hostname per la macchina.
- Decommentare la riga `mydestination = $myhostname, localhost.$mydomain`.

- Decommentare la riga `mynetworks`, e sostituire *`168.100.189.0/28`* con una impostazione di rete valida per gli host che possono eseguire un collegamento al server.
- Decommentare la riga `inet_interfaces = all`.
- Riavviare il servizio `postfix`.

Una volta completate queste fasi, l'host accetta di consegnare le email esterne.

Postfix possiede una vasta gamma di opzioni di configurazione. Uno dei modi migliori per come configurare Postfix, è leggere i commenti all'interno di `/etc/postfix/main.cf`. Risorse aggiuntive, incluso le informazioni inerenti LDAP e l'integrazione SpamAssassin, sono disponibili online su http://www.postfix.org/.

11.3.3. Fetchmail

Fetchmail è un MTA che riprende le email da server remoti e le consegna all'MTA locale. Molti utenti apprezzano la capacità di separare il processo di download dei messaggi sul server remoto da quello di lettura e di organizzazione dei messaggi in un MUA. Ideato specificamente per gli utenti dial-up, Fetchmail è in grado di collegarsi e scaricare velocemente tutti i messaggi e-mail nel file spool di posta, utilizzando un numero indefinito di protocolli, incluso POP3 e IMAP. Questo programma, può anche inoltrare i vostri messaggi a un server SMTP, qualora fosse necessario.

Fetchmail viene configurato per ogni utente, attraverso l'uso di un file `.fetchmailrc` nella home directory dell'utente.

Le preferenze contenute nel file `.fetchmailrc` consentono a Fetchmail di controllare la posta su un server remoto e di rinviarla nel tentativo di consegnarla alla porta 25 sul computer locale, utilizzando l'MTA locale per posizionare le e-mail nel corretto file spool dell'utente. Se Procmail è disponibile, può essere lanciato per filtrare i messaggi e archiviarli in una mailbox affinché siano letti da un MUA.

11.3.3.1. Opzioni di configurazione per Fetchmail

Anche se è possibile passare tutte le opzioni sulla linea di comando necessaria a controllare la posta su di un server remoto durante l'esecuzione di Fetchmail, tuttavia si consiglia di semplificare l'operazione usando il file `.fetchmailrc`. Posizionate le opzioni di configurazione desiderate nel file `.fetchmailrc`, le suddette opzioni vengono usate ogni volta il comando `fetchmail` viene emesso. È possibile altresì annullare queste opzioni ogni qualvolta che si esegue Fetchmail, specificando l'opzione sulla linea di comando.

Il file `.fetchmailrc` di un utente si divide in tre classi:

- *opzioni globali* — fornisce a Fetchmail le istruzioni che controllano l'esecuzione del programma o le impostazioni per le connessioni di controllo dei messaggi.
- *opzioni del server* — Specifica le informazioni necessarie per il polling del server, come ad esempio l'hostname o le preferenze per server email specifici, per esempio la porta da controllare oppure i secondi d'attesa prima del time out. Queste opzioni riguardano ogni utente che utilizzata quel server specifico.
- *opzioni utente* — Contiene informazioni, quali nome utente e password, necessarie per l'autenticazione e il controllo delle email mediante un server email particolare.

Le opzioni globali sono in cima al file `.fetchmailrc`, seguite da una o più opzioni server, ciascuna delle quali designa un server di posta differente che sarà controllato da Fetchmail. Le opzioni utente sono successive alle opzioni server e servono per gli account utente che si desidera controllare un server di posta. Come le opzioni server, quelle multiple utente possono essere specifiche per un server particolare, e si usano, per esempio, per controllare account e-mail multipli sullo stesso server.

Le opzioni del server nel file `.fetchmailrc` vengono attivate da una opzione verbale speciale, `poll`oppure `skip`, che precede ogni informazione del server. L'azione di `poll` indica a Fetchmail di usare l'opzione del server quando è in esecuzione, in pratica si tratta del controllo delle email che utilizzano le opzioni dell'utente. Ogni opzione del server dopo un'azione di `skip`, tuttavia, non viene controllata a meno che l'hostname del server non viene specificato quando Fetchmail viene invocato. L'opzione `skip` è utile quando si esegue una prova delle configurazioni in `.fetchmailrc` poichè esegue un controllo solo se indicato, senza interferire sulle configurazioni correnti.

Un file di esempio `.fetchmailrc` è simile al seguente esempio:

```
set postmaster "user1"
set bouncemail

poll pop.domain.com proto pop3
     user 'user1' there with password 'secret' is user1 here

poll mail.domain2.com
     user 'user5' there with password 'secret2' is user1 here
     user 'user7' there with password 'secret3' is user1 here
```

In questo esempio le impostazioni globali sono impostate in modo tale che l'utente riceva la posta come ultima risorsa (opzione `postmaster`) e tutti gli errori e-mail siano inviati al postmaster invece che al mittente (opzione `bouncemail`). L'azione `set` indica a Fetchmail che questa linea contiene un'opzione globale. Vengono quindi specificati due server di posta, uno impostato per rilevare la posta usando POP3 e l'altro per utilizzare diversi protocolli e consentire al primo di eseguire le proprie funzioni. I due utenti vengono controllati mediante l'opzione relativa al secondo server, ma tutte le email trovate per ogni utente vengono inviate allo spool mail dello `user1`. Ciò consente il controllo delle mailbox multiple su server multipli, mentre compaiono in un unico inbox MUA. Le informazioni specifiche per ogni utente iniziano con l'azione `user`.

Nota Bene

Non è necessario inserire la password personale nel file `.fetchmailrc`. Potete pertanto tralasciare la sezione `with password '`*`password`*`'`. Fetchmail vi chiederà la password dopo l'avvio.

Fetchmail contiene una varietà di opzioni globali, server e locali. Molte di queste opzioni sono usate di rado oppure si applicano solo in situazioni molto specifiche. La pagina man di `fetchmail` spiega in dettaglio queste opzioni, ma troverete qui di seguito un elenco delle opzioni più comuni.

11.3.3.2. Opzioni globali

Ogni opzione globale dovrebbe essere posizionata su di una singola riga dopo un'azione di `set`.

- `daemon` <*`seconds`*> — Specifica la modalità del demone, dove Fetchmail resta nel background. Sostituire <*`seconds`*> con il numero di secondi che Fetchmail deve attendereprima di richiamare il server.
- `postmaster` — Specifica un utente locale al quale inviare la posta in caso di problemi di consegna.
- `syslog` — Specifica il file di log per gli errori e per i messaggi sullo stato. Per default, esso è `/var/log/maillog`.

11.3.3.3. Opzioni del server

Le opzioni del server devono essere posizionate sulle proprie righe in `.fetchmailrc` dopo un'azione `poll` o `skip`.

- `auth` <*auth-type*> — Sostituire <*auth-type*> con il tipo di autenticazione da utilizzare. Per default, viene utilizzata l'autenticazione `password`, ma alcuni protocolli supportano altri tipi di autenticazione, fra cui `kerberos_v5`, `kerberos_v4`, e `ssh`. Quando viene usata l'autenticazione di tipo `any`, Fetchmail tenterà prima i metodi che non richiedono una password, quindi quelli che usano il masquerading e infine cercherà di inviare la vostra password in chiaro per l'autenticazione presso il server.
- `interval` <*number*> — Interroga il server specificato ogni <*number*> di volte che controlla per una email sui server configurati. Questa opzione può essere usata con i server di posta che ricevono i messaggi solo occasionalmente.
- `port` <*port-number*> — Sostituire <*port-number*> con il numero della porta. Questo valore annulla il numero della porta di default per il protocollo specificato.
- `proto` <*protocol*> — Sostituire <*protocol*> con il protocollo, come ad esempio `pop3` o `imap`, da usare quando si esegue un controllo dei messaggi sul server
- `timeout` <*seconds*> — Sostituisce <*seconds*> con il numero di secondi di inattività del server dopo i quali Fetchmail non prova più ad eseguire un collegamento. Se questo valore non viene impostato, si presuppone il valore predefinito di `300`.

11.3.3.4. Opzioni utente

Le opzioni dell'utente possono essere posizionate sulle righe al di sotto di una opzione del server, o sulla stessa riga dell'opzione del server. In entrambi i casi le opzioni definite, devono seguire l'opzione `user` (definita qui sotto).

- `fetchall` — Ordina a Fetchmail di scaricare tutti i messaggi in coda, compresi quelli che sono già stati visualizzati. Per default, Fetchmail scarica solo i messaggi nuovi.
- `fetchlimit` <*number*> — Sostituire <*number*> con il numero dei messaggi da riprendere prima di eseguire un arresto.
- `flush` — Cancellare tutti i messaggi precedentemente visualizzati nella coda, prima di scaricare quelli nuovi.
- `limit` <*max-number-bytes*> — Sostituisce <*max-number-bytes*> con la misura massima, in byte, dei messaggi quando gli stessi vengono ripresi da Fetchmail. Questa opzione risulta utile in caso di connessioni di rete lente, quando l'intervallo di tempo necessario a scaricare il messaggio risulta essere lungo.
- `password '`<*password*>`'` — Sostituire <*password*> con la password dell'utente.
- `preconnect "`<*command*>`"` — Sostituire <*command*> con un comando da eseguire prima di riprendere i messaggi per un utente specifico.
- `postconnect "`<*command*>`"` — Sostituire <*command*> con un comando da eseguire dopo aver ripreso i messaggi per un utente specifico.
- `ssl` — Attiva la cifratura SSL.
- `user "`<*username*>`"` — Sostituire <*username*> con il nome utente usato da Fetchmail per riprendere i messaggi. *Questa opzione dovrebbe figurare in elenco prima di qualsiasi altra opzione utente.*

11.3.3.5. Opzioni di comando di Fetchmail

La maggior parte delle opzioni Fetchmail utilizzate sulla riga di comando, quando si esegue il comando `fetchmail`, rispecchia le opzioni di configurazione `.fetchmailrc`. In questo modo, Fetchmail può essere utilizzato con o senza un file di configurazione. Queste opzioni sono usate sulla riga di comando, poiché è più semplice lasciarle nel file `.fetchmailrc`.

A volte, tuttavia, è possibile voler eseguire il comando `fetchmail`, con altre opzioni per scopi particolari. Poiché ogni opzione specificata sulla linea di comando elimina le opzioni del file di configurazione, è possibile attivare le opzioni di comando per escludere temporaneamente l'impostazione `.fetchmailrc` che sta provocando un errore.

11.3.3.6. Opzioni informative o di debugging

Certe opzioni usate dopo il comando `fetchmail` possono fornire informazioni importanti.

- `--configdump` — Visualizza ogni possibile opzione basata su informazioni provenienti da `.fetchmailrc` e dai valori di default di Fetchmail. Quando si usa questa opzione, non vi è la possibilità di recuperare le email per gli utenti.
- `-s` — Esegue Fetchmail in modalità 'silent', impedendo la visualizzazione di qualsiasi messaggio che non sia di errore dopo il comando `fetchmail`.
- `-v` — Esegue Fetchmail in modalità 'verbose', visualizzando ogni comunicazione tra Fetchmail e i server email remoti.
- `-V` — Fa sì che Fetchmail visualizzi informazioni dettagliate sulla versione, elenca le opzioni globali e mostra le impostazioni da usare per ogni utente, compreso il protocollo e-mail e il metodo di autenticazione. Quando questa opzione è attiva, la posta non viene rilevata per alcun utente.

11.3.3.7. Opzioni speciali

Queste opzioni vengono usate occasionalmente per escludere i valori di default spesso inclusi nel file `.fetchmailrc`.

- `-a` — Indica a Fetchmail di scaricare tutti i messaggi, sia nuovi che precedentemente visualizzati, presenti sul server remoto. Per default, Fetchmail scarica solo i messaggi nuovi.
- `-k` — Fa sì che Fetchmail lasci i messaggi sul server remoto dopo averli scaricati. Questa opzione esclude la cancellazione di default dei messaggi dopo il download.
- `-l <max-number-bytes>` — Indica a Fetchmail di non scaricare i messaggi che superano determinate dimensioni lasciandoli sul server email remoto.
- `--quit` — Abbandona il processo demone di Fetchmail.

Ulteriori comandi e opzioni `.fetchmailrc` sono disponibili sulla pagina man `fetchmail`.

11.4. Mail Delivery Agents

Red Hat Enterprise Linux include due MDA primari, Procmail e `mail`. Entrambe le applicazioni sono considerate LDA, ed entrambe muovono le email dal file spool dell'MTA nella mailbox dell'utente. Tuttavia, Procmail fornisce un sistema robusto di filtraggio.

Questa sezione affronta in modo dettagliato solo Procmail. Per informazioni sul comando `mail`, consultare la propria pagina man.

Procmail consegna e filtra email nel vostro file spool dell'host locale. É potente, ampiamente utilizzato e non intrusivo. Procmail puó giocare un ruolo importante nella consegna di posta elettronica letta dalle applicazioni client.

Procmail può essere richiamato in svariati modi. Ogni volta che un MTA posiziona una email nel file spool di posta, Procmail viene lanciato. Procmail, quindi, filtra e archivia per l'MUA e successivamente abbandona l'applicazione. In alternativa, l'MUA potrebbe essere configurato per richiamare Procmail ogni volta che si riceve un messaggio, in modo tale da archiviare i messaggi nelle corrette mailbox. Per default, la presenza di `/etc/procmailrc` o di un `.procmailrc` (anche chiamato file *rc*) nella home directory dell'utente, richiamerà Procmail, nel caso in cui un MTA riceve un nuovo messaggio.

Le azioni eseguite da Procmail con i messaggi e-mail dipendono dalla corrispondenza del messaggio rispetto ad un insieme di condizioni o *requisiti* nel file `rc`. Se un messaggio soddisfa i requisiti necessari, allora la email verrà posizionata in un file specifico, viene cancellato oppure processato.

Una volta avviato, Procmail legge il messaggio e-mail e separa la parte principale dall'informazione di testo. Successivamente Procmail và alla ricerca, per default, del file `/etc/procmailrc` e dei file `rc` nella directory `/etc/procmailrcs`, per le regole e le variabili del sistema dell'ambiente Procmail. Procmail va alla ricerca quindi di un file `.procmailrc` nella home directory dell'utente. Molti utenti creano anche dei file `rc` aggiuntivi per Procmail, per un riferimento all'interno del file `.procmailrc` nella loro home directory.

Per default, non esiste alcun file `rc` nella directory `/etc/` e non vi sono nemmeno file `.procmailrc` nella directory home dell'untente. Per utilizzare Procmail, ogni utente deve creare un file `.procmailrc` con particolari variabili e regole per l'ambiente.

11.4.1. Configurazione di Procmail

I file di configurazione di Procmail contengono molte variabili importanti per l'ambiente. Tali variabili indicano i messaggi da smistare, e come comportarsi nei confronti dei messaggi che non soddisfano alcuna regola.

Queste variabili di ambiente compaiono in genere all'inizio del file `.procmailrc`, nel seguente formato:

<env-variable>="*<value>*"

In questo esempio, *<env-variable>* è il nome della variabile e *<value>* definisce la variabile.

La maggior parte degli utenti Procmail non utilizza molte variabili, anche se molte delle più importanti variabili sono già definite come valore di default. Spesso vi troverete di fronte alle seguenti variabili:

- `DEFAULT` — Imposta il mailbox di default in cui saranno posizionati i messaggi che non soddisfano le regole.

  Il valore di default `DEFAULT` è uguale a `$ORGMAIL`.

- `INCLUDERC` — Specifica i file `rc` aggiuntivi che contengono ulteriori regole per i messaggi da controllare. Ciò consente di separare gli elenchi delle regole in due singoli file che svolgono funzioni differenti, per esempio il blocco degli spam o la gestione delle mailing list, le quali sono attivabili o disattivabili utilizzando i caratteri commento nel file utente `.procmailrc`.

  Il seguente potrebbe essere un esempio di righe in un file utente `.procmailrc`:

  ```
  MAILDIR=$HOME/Msgs
  INCLUDERC=$MAILDIR/lists.rc
  INCLUDERC=$MAILDIR/spam.rc
  ```

  Se l'utente desidera disabilitare il filtro Procmail sugli elenchi di posta ma lasciare attivo il controllo degli spam, può semplicemente inserire il carattere [#] nella riga `INCLUDERC`.

- `LOCKSLEEP` — Imposta l'intervallo di tempo, in secondi, che intercorre tra un tentativo e l'altro di Procmail, di utilizzare un particolare file di blocco. Il tempo predefinito è di otto secondi.
- `LOCKTIMEOUT` — Imposta l'intervallo di tempo, in secondi, che deve trascorrere dopo l'ultima modifica di un file di blocco perché Procmail assume che tale file sia vecchio e possa essere eliminato. Il tempo predefinito è di 1024 secondi.
- `LOGFILE` — Posizione e file che contengono i messaggi informativi e di errore di Procmail.
- `MAILDIR` — Imposta la directory correntemente in uso per Procmail. Se impostata, tutti gli altri percorsi di Procmail sono legati a questa directory.
- `ORGMAIL` — Specifica il mailbox originale o qualsiasi altro luogo dove posizionare i messaggi qualora non fosse possibile usare la posizione di default o quella richiesta dalle regole.

  Per default, viene usato un valore di `/var/spool/mail/$LOGNAME`.
- `SUSPEND` — Imposta l'intervallo, in secondi, che Procmail utilizzerà come pausa se una risorsa necessaria, come per esempio lo spazio swap, non è disponibile.
- `SWITCHRC` — Consente all'utente di specificare un file esterno contenente regole Procmail aggiuntive, molto simile all'opzione `INCLUDERC`, tranne per la verifica delle regole, che di fatto termina sul file di configurazione di riferimento, causando l'utilizzazione delle regole sul file `SWITCHRC` specificato.
- `VERBOSE` — Consente a Procmail di registrare una maggiore quantità d'informazioni. Questa opzione si rivela utile per il debugging.

Altre variabili importanti di ambiente sono prelevate dalla shell, fra queste `LOGNAME`, che corrisponde al vostro nome di login, `HOME`, ovvero la posizione della vostra home directory e `SHELL`, la shell di default.

Spiegazioni esaurienti su tutte le variabili di ambiente e sui valori di default sono disponibili nella pagina man `procmailrc`.

11.4.2. Regole Procmail

Per molti nuovi utenti, la creazione delle regole rappresenta la parte più complicata per l'uso di Procmail. In un certo senso, questo è comprensibile, poiché le regole utilizzano *espressioni regolari* per far sì che i messaggi soddisfino i requisiti richiesti. Queste espressioni regolari identificano un particolare formato utilizzato per specificare gli attributi delle stringhe corrispondenti. Il costrutto delle espressioni regolari non è, tuttavia, complicato e la loro lettura ne rende ancora più semplice la comprensione. Inoltre, la consistenza del modo in cui le regole sono scritte, indipendentemente dalle espressioni regolari, facilita la comprensione del processo in corso. Per avere degli esempi, consultare la Sezione 11.4.2.5.

Le regole Procmail hanno le seguenti forme:

```
:0<flags>: <lockfile-name>

* <special-condition-character> <condition-1>
* <special-condition-character> <condition-2>
* <special-condition-character> <condition-N>

<special-action-character><action-to-perform>
```

I primi due caratteri di una regola Procmail sono i due punti e lo zero. Dopo lo zero possono anche esserci diverse flag per il controllo dell'attività di Procmail durante l'elaborazione di quella regola. La presenza dei due punti dopo la sezione <*flags*> indica che per quel messaggio sarà creato un file di blocco. L'utente dovrà specificare il nome del file nello spazio <*lockfile-name*>.

Per corrispondere un messaggio, una regola puó contenere diverse condizioni. Se non vi sono condizioni, ogni messaggio sarà conforme alla regola. Le espressioni regolari sono comprese in alcune condizioni al fine di facilitare una corrispondenza con il messaggio. Se vengono utilizzate delle condizioni multiple, queste devono corrispondere tutte affinché sia possibile eseguire un'azione. Le condizioni sono controllate in base ai flag impostati nella prima riga delle regole. Speciali caratteri opzionali posizionati dopo il carattere `*` aggiungono un ulteriore controllo sulla condizione.

L'*<action-to-perform>*specifica l'azione intrapresa quando un messaggio soddisfa una delle condizioni. È consentita una sola azione per regola. In molti casi, qui viene utilizzato il nome di una mailbox per dirigere i messaggi conformi in quel file, smistando efficacemente la emal. Prima di specificare l'azione, possono essere utilizzati alcuni caratteri per azioni speciali. Consultare la Sezione 11.4.2.4 per maggiori informazioni.

11.4.2.1. Regole di distribuzione

L'azione eseguita nel caso in cui la regola corrisponda ad un messaggio particolare, determina se la regola stessa può essere considerata per un'azione di *consegna* o di *rifiuto della consegna*. Una regola di consegna, contiene un'azione in grado di scrivere un messaggio su di un file, lo invia ad un altro programma oppure lo inoltra ad un altro indirizzo e-mail. Una regola per il rifiuto della consegna copre qualsiasi altra azione, come ad esempio il *nesting block*. Il nesting block rappresenta un insieme di azioni contenute tra parentesi graffe `{ }`, eseguite sui messaggi che soddisfano le condizioni della regola. I nesting block possono essere nidificati al loro interno, garantendo così un maggiore controllo per l'identificazione e l'esecuzione delle azioni sui messaggi.

Quando i messaggi corrispondono ad una regola di consegna o di 'delivering', Procmail esegue l'azione specifica e interrompe l'azione di confronto con le altre regole. I messaggi che corrispondono alle regole per il rifiuto della consegna, continueranno ad essere confrontati con altre regole.

11.4.2.2. Flag

I flag sono molto importanti per determinare se e come le condizioni della regola sono confrontate ad un messaggio. I seguenti esempi mostrano alcuni flag comunemente usati:

- `A` — Specifica che la regola sarà usata solo se anche l'ultima regola applicata senza un flag `A` o `a` è stata applicata al messaggio.
- `a` — Specifica che la regola sarà usata solo se anche l'ultima regola applicata senza un flag `A` o `a` è stata applicata al messaggio *ed* è stata completata con successo.
- `B` — Analizza il corpo del messaggio e cerca il soddisfacimento delle condizioni.
- `b` — Utilizza il corpo in ogni azione risultante, come la scrittura del messaggio su un file o il suo inoltro. Tale comportamento viene eseguito per default.
- `c` — Genera una copia carbone della email. Ciò risulta utile con le regole di distribuzione, poiché l'azione richiesta può essere eseguita sul messaggio e la copia dello stesso può continuare a essere elaborata nei file `rc`.
- `D` — Fa in modo che il confronto `egrep` preveda il riconoscimento dei caratteri maiuscoli. Per default, il processo di confronto non lo prevede.
- `E` — Simile al flag `A`, tranne per il fatto che le condizioni in questa regola sono confrontate con il messaggio solo se la regola immediatamente precedente senza un flag `E` non soddisfa le condizioni. Ciò è paragonabile a un'azione *else*.
- `e` — La regola viene confrontata con il messaggio, solo se l'azione specificata nella regola immediatamente precedente fallisce.
- `f` — Utilizza pipe come filtro.

- `H` — Analizza l'intestazione del messaggio e va alla ricerca del soddisfacimento delle condizioni. Ciò viene eseguito per default.
- `h` — Utilizza l'intestazione in un'azione risultante. Ciò viene eseguito per default.
- `w` — Indica a Procmail di aspettare il filtro specificato o il programma per terminare, ed eseguire il reporto sull'esito dell'operazione prima di considerare il messaggio già filtrato.
- `W` — È identico a `w` ad eccezione che i messaggi "Program failure" sono soppressi.

Per un elenco dettagliato di flag aggiuntive, consultare la pagina man `procmailrc`.

11.4.2.3. Specificare un file di lock locale

I Lockfile sono molto utili perché evitano il verificarsi in contemporanea di processi di alterazione su alcuni messaggi. È possibile specificare un lockfile locale, posizionando un carattere `:` dopo ogni flag sulla prima linea della regola. In questo modo verrà creato un lockfile locale basato sul filename di destinazione che comprende tutto ciò che è stato impostato nella variabile globale dell'ambiente `LOCKEXT`.

In alternativa, è possibile specificare il nome del file di lock locale da utilizzare con la regola dopo i due punti.

11.4.2.4. Condizioni e azioni speciali

Caratteri speciali utilizzati prima delle condizioni delle regole e delle azioni di Procmail cambiano la loro interpretazione.

I seguenti caratteri possono essere utilizzati dopo il carattere `*` all'inizio di una linea di condizione delle regole:

- `!` — Inverte le condizioni, provocando un controllo solo se le condizioni non sono applicabili al messaggio.
- `<` — Controlla se il messaggio è al di sotto di un determinato numero di byte.
- `>` — Controlla se il messaggio superi un determinato numero di byte.

I seguenti caratteri sono utilizzati per eseguire azioni speciali:

- `!` — Nella riga d'azione, questo carattere indica a Procmail di inoltrare il messaggio all'indirizzo e-mail specificato.
- `$` — Si riferisce a una variabile precedentemente impostata nel file `rc`. Questo carattere è utilizzato per impostare un comune mailbox cui faranno riferimento varie regole.
- `|` — Avvia un programma specificato in modo da processare il messaggio.
- `{` and `}` — Crea un blocco di nesting, usato per contenere regole aggiuntive da applicare ai messaggi che soddisfano le condizioni.

Se non sono utilizzati caratteri speciali all'inizio della linea d'azione, Procmail assume che quest'ultima stia specificando il mailbox sul quale scrivere il messaggio.

11.4.2.5. Esempi di regole

Procmail è un programma estremamente flessibile. Come conseguenza di questa flessibilità, tuttavia, vi è il fatto che comporre una regola per raggiungere un determinato scopo può risultare difficile per i non esperti.

Il modo migliore per sviluppare l'abilità di creare le condizioni della regola di Procmail è quello di comprendere delle espressioni regolari combinate con il controllo degli esempi creati da altri. La spiegazione approfondita delle espressioni regolari va oltre gli obbiettivi di questa sezione. La struttura delle regole di Procmail è molto più importante. Su internet sono disponibili esempi utili di regole Procmail (come ad esempio http://www.iki.fi/era/procmail/links.html). L'uso appropriato e l'adattamento delle espressioni regolari trovate negli esempi dipendono dalla comprensione della struttura delle regole Procmail. Specifiche informazioni introduttive alle espressioni regolari di base sono disponibili nella pagina man `grep`.

I seguenti esempi mostrano la struttura di base delle regole Procmail, e possono fornire la base per la creazione di regole più complesse.

Le regole più elementari non contengono nemmeno le condizioni, come illustrato nell'esempio riportato di seguito.

```
:0:
new-mail.spool
```

La prima linea indica che deve essere creato un lockfile locale senza però indicare il nome, in modo che Procmail possa utilizzare il file name di destinazione, indicando altresì il valore specificato nella variabile dell'ambiente `LOCKEXT`. Poiché non viene specificata alcuna condizione, ogni messaggio potrà soddisfare questa regola e, pertanto, sarà posizionato in un unico spool file chiamato `new-mail.spool`, che si trova all'interno della directory indicata dalla variabile di ambiente `MAILDIR`. I messaggi presenti in questo file possono quindi essere visualizzati da un MUA.

Una regola di base, come questa, può essere posizionata alla fine di ogni file `rc`, in modo da dirigere i messaggi in una posizione di default.

Il seguente esempio corrisponde a messaggi provenienti da un indirizzo email specifico, che successivamente vengono eliminati.

```
:0
* ^From: spammer@domain.com
/dev/null
```

In questo esempio, ogni messaggio inviato da `spammer@domain.com` viene immediatamente inviato nel dispositivo `/dev/null`, con una conseguente eliminazione.

Attenzione

Assicurarsi che una regola funzioni correttamente prima di spostare i messaggi che la soddisfano in `/dev/null`, poiché la cancellazione è definitiva. Se le condizioni della vostra regola trovano inavvertitamente dei messaggi da non sottoporre al controllo, e i suddetti messaggi vengono eliminati, diventerà difficile risolvere la regola.

La soluzione migliore è indirizzare l'azione verso un mailbox speciale che potrete controllare di volta in volta per cercare falsi positivi. Una volta certi che non vi siano messaggi controllati inavvertitamente, potete cancellare il mailbox e dirigere l'azione in modo da inviare i messaggi a `/dev/null`.

La seguente regola riceve i messaggi inviati da una mailing list particolare e li posiziona in una cartella particolare.

```
:0:
* ^(From|CC|To).*tux-lug
tuxlug
```

Qualsiasi messaggio inviato dalla mailing list `tux-lug@domain.com` sarà posizionato automaticamente nel mailbox `tuxlug` per il MUA. La condizione in questo esempio controllerà il messaggio se l'indirizzo e-mail della mailing list si trova sulle linee `From`, `CC` oppure `To`.

Consultate le risorse online di Procmail, disponibili su la Sezione 11.6 per regole più specifiche e potenti.

11.4.2.6. Filtri Spam

Poichè viene chiamato da Sendmail, Postfix, e Fetchmail quando si ricevono nuove email, Procmail puó essere usato come potente strumento contro lo spam.

Questo é particolarmente vero quando Procmail é usato in combinazione con SpamAssassin. Quando usati insieme, queste due applicazioni possono identificare velocemente email spam, separandole oppure eliminandole.

SpamAssassin usa l'analisi d'intestazione, di testo, blacklist, un database spam-tracking, e un'analisi spam self-learning Bayesian per identificare accuratamente e velocemente ed etichettare le email spam.

Il modo piú facile per un utente locale di usare SpamAssassin, é di posizionare la seguente riga vicino al limite superiore del file `~/.procmailrc`:

```
INCLUDERC=/etc/mail/spamassassin/spamassassin-default.rc
```

Il `/etc/mail/spamassassin/spamassassin-default.rc` contiene una regola Procmail semplice in grado di attivare SpamAssassin per tutte le email in arrivo. Se una email viene determinata essere spam, viene etichettata nell'intestazione, e il titolo viene mostrato in questo modo:

```
*****SPAM*****
```

Il messaggio della email viene presentato con un riscontro corrente dell'elemento che ha causato il motivo per il quale la email é stata considerata spam.

Per archiviare una email etichettata come spam, puó essere usata una regola simile alla seguente:

```
:0 Hw
* ^X-Spam-Status: Yes
spam
```

Questa regola archivia tutte le email etichettate nell'intestazione, come spam in un mailbox chiamato `spam`.

Poichè SpamAssassin é uno script Perl, puó essere necessario su server molto occupati, di usare il demone SpamAssassin binario (`spamd`) e l'applicazione client (`spamc`). Configurando SpamAssassin in questo modo, tuttavia, richiede un accesso root per la host.

Per avviare il demone `spamd`, digitare il seguente comando come un utente root:

```
/sbin/service spamassassin start
```

Per avviare il demone SpamAssassin quando il sistema viene avviato, usare una utility initscript, come ad esempio il **Strumento di configurazione dei servizi** (`redhat-config-services`), per abilitare il servizio `spamassassin`. Consultate la Sezione 1.4.2 per maggiori informazioni sulle utility initscript.

Per configurare Procmail in modo da usare l'applicazione client SpamAssassin invece dello script Perl, posizionare le seguenti righe vicino alla parte superiore del file `~/.procmailrc`. Per una configurazione dell'intero sistema, posizionarlo in `/etc/procmailrc`:

```
INCLUDERC=/etc/mail/spamassassin/spamassassin-spamc.rc
```

11.5. Mail User Agents

Sono presenti alcuni programmi di posta con Red Hat Enterprise Linux. Sono paltresì disponibili programmi client email grafici, con molti contenuti come ad esempio **Mozilla Mail** o **Ximian Evolution**, oppure programmi email basati sul testo, come ad esempio **Mutt**.

Per istruzioni sull'uso di queste applicazioni, consultare il capitolo intitolato *Applicazioni email* in *Red Hat Enterprise Linux Guida passo dopo passo*.

Il resto di questa sezione presta particolare attenzione sulla sicurezza delle comunicazioni tra il client ed il server.

11.5.1. Securezza delle comunicazioni

I MUA più diffusi forniti con Red Hat Enterprise Linux, quali **Mozilla Mail**, **mutt** e **Ximian Evolution**, dispongono di sessioni di posta criptata mediante SSL.

Come qualsiasi altro servizio che si muove in chiaro in una rete, con informazioni email importanti, come ad esempio il nome utente, le password e interi messaggi, possono essere intercettate e lette da altri utenti sulla rete. In aggiunta, poichè il POP standard e i protocolli IMAP inviano le informazioni di autenticazione in chiaro, é possibile per un intruso, ottenere l'accesso agli account, raccogliendo i nomi utente e le password, quando questi vengono inviati sulla rete.

11.5.1.1. Client e-mail sicuri

Molti Linux MUA, sono stati ideati per controllare le email con supporto SSL di cifratura su server remoti. Per poter usare SSL quando si riprende una email, ricordarsi di abilitarlo su entrambe le email client e del server.

Dalla parte del client, SSL è facile da abilitare, viene spesso fatto semplicemente facendo clic su di un pulsante nella finestra di configurazione MUA o attraverso una opzione nel file di configurazione MUA. IMAP sicuro e POP, sono a conoscenza dei numeri delle porte (rispettivamente 993 e 995) usate da MUA per autenticare e scaricare i messaggi.

11.5.1.2. Securezza nelle comunicazioni client email

Offrire il metodo di cifratura SSL a utenti IMAP e POP sul server email, é una cosa molto facile.

Innanzitutto, create un certificato SSL. Questo puó essere effettuato in due modi: applicando un *Certificate Authority* (*CA*) per un certificato SSL oppure creando un certificato firmato da voi stessi "self-signed"

Attenzione

I certificati "self-signed" dovrebbero essere usati solo a scopo di test. Ogni server usato in un ambiente di produttivitá, deve usare un certificato SSL garantito da un CA.

Per creare un certificato SSL 'self-signed' per IMAP, andare nella directory `/usr/share/ssl/certs/` e digitare i seguenti comandi come utente root:

```
rm -f imapd.pem
make imapd.pem
```

Rispondere a tutte le domende per completare il processo.

Per creare un certificato SSL 'self-signed' per POP, andare nella directory `/usr/share/ssl/certs/` e digitare i seguenti comandi come utente root:

```
rm -f ipop3d.pem
make ipop3d.pem
```

Ancora, rispondere a tutte le domande per procedere.

Importante

Assicuratevi di rimuovere i file di default `imapd.pem` e `ipop3d.pem`, prima di emettere il comando `make`.

Una volta terminato, eseguire il comando `/sbin/service xinetd restart` per riavviare il demone `xinetd`, il quale controlla `imapd` e `ipop3d`.

Alternativamente, il comando `stunnel` puó essere usato come un wrapper di cifratura SSL con i demoni standard non-sicuri, `imapd` o `pop3d`.

Il programma `stunnel` utilizza delle librerie OpenSSL esterne incluse con Red Hat Enterprise Linux, in modo da fornire una codifica forte e per proteggere i collegamenti. È consigliabile applicare il suddetto programma ad un CA, in modo da ottenere un certificato SSL, ma è anche possibile creare un certificato così detto 'self-signed'.

Per creare un certificato SSL "self-signed", andare nella directory `/usr/share/ssl/certs/`, e digitare il seguente comando:

```
make stunnel.pem
```

Ancora, rispondere a tutte le domande per procedere.

Una volta generato il certificato, é possibile usare il comando `stunnel` per iniziare il demone di posta `imapd`, usando il seguente comando:

```
/usr/sbin/stunnel -d 993 -l /usr/sbin/imapd imapd
```

Una volta emesso questo comando, é possibile aprire un client email IMAP e connettersi al server email usando la cifratura SSL.

Per avviare il `pop3d` usando il comando `stunnel`, digitare il seguente comando:

```
/usr/sbin/stunnel -d 995 -l /usr/sbin/pop3d pop3d
```

Per maggiori informazioni su come usare `stunnel`, leggere la pagina man `stunnel` o consultare i documenti nella directory `/usr/share/doc/stunnel-<version-number>/`, dove *<version-number>* è il numero della versione di `stunnel`.

11.6. Risorse aggiuntive

Di seguito vi proponiamo un elenco di documenti aggiuntivi sulle applicazioni email.

11.6.1. Documentazione installata

- I pacchetti `sendmail` e `sendmail-cf` comprendono informazioni sulle modalità di configurazione di Sendmail.

- `/usr/share/sendmail-cf/README.cf` — Contiene informazioni sui file `m4`, i percorsi dei file per Sendmail, i mailer supportati, l'accesso alle caratteristiche potenziate e altro ancora.

Inoltre, le pagine man `sendmail` e `aliases` contengono, rispettivamente, informazioni utili riguardanti varie opzioni di Sendmail e la corretta configurazione del file `/etc/mail/aliases`.

- `/usr/share/doc/postfix-<version-number>` — Contiene una grande quantitá di informazioni sui diversi modi di configurazione di Postfix. Sostituire *<numero-versione>* con il numero della versione di Postfix.
- `/usr/share/doc/fetchmail-<numero-versione>` — Contiene un elenco completo delle caratteristiche Fetchmail contenute nel file `FEATURES` e un documento introduttivo `FAQ`. Sostituite *<numero-versione>* con il numero della versione di Fetchmail.
- `/usr/share/doc/procmail-<numero-versione>` — Contiene un file `README` che fornisce una panoramica su Procmail, un file `FEATURES` che esplora le caratteristiche di ciascun programma, e un file `FAQ` con le risposte alle domande più frequenti riguardanti la configurazione. Sostituite *<numero-versione>* con il numero della versione di Procmail.

  Quando si familiarizza con il funzionamento di Procmail e la creazione di nuove regole, queste pagine man di Procmail assumono un valore notevole:

  - `procmail` — fornisce una panoramica sul funzionamento di Procmail e le fasi di filtraggio della posta elettronica.
  - `procmailrc` — affronta il formato del file usato per creare le regole.
  - `procmailex` — fornisce vari esempi utili e già applicati delle regole Procmail.
  - `procmailsc` — Spiega la tecnica di scoring utilizzata da Procmail per verificare che una particolare regola è applicabile a un certo messaggio.
  - `/usr/share/doc/spamassassin-<numero-versione>/` — Contiene una grande quantitá di informazioni inerenti SpamAssassin. Sostituire *<numero-versione>* con il numero della versione del pacchetto `spamassassin`.

11.6.2. Siti Web utili

- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-Administrator-HOWTO.html — Fornisce una panoramica sul funzionamento delle e-mail ed esamina possibili soluzioni di posta e la configurazione lato client e server.
- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-User-HOWTO/ — Considera la posta elettronica dal punto di vista dell'utente, interroga varie applicazioni client e dispone di un'introduzione ad argomenti specifici come alias, inoltro, auto-replying, mailing list, filtri di posta
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Secure-POP+SSH.html — Mostra come rilevare la posta POP usando SSH con il port forwarding, in modo che le password e i messaggi possano essere trasferiti in modo sicuro.
- http://www.sendmail.net/ — Contiene novità, interviste e articoli su Sendmail, oltre a un ampia panoramica sulle opzioni disponibili.
- http://www.sendmail.org/ — Offre un'approfondita analisi delle caratteristiche di Sendmail ed esempi di configurazione.
- http://www.postfix.org/ — La home page del progetto Postfix contiene informazioni utili su Postfix. La mailing list rappresenta un luogo particolarmente utile per la ricerca di informazioni.
- http://catb.org/~esr/fetchmail/ — La home page di Fetchmail, con un manuale online, e delle domande frequanti 'FAQ' approfondite.

- http://www.procmail.org/ — La home page di Procmail, con link a diverse mailing list dedicate a Procmail e FAQ.
- http://www.ling.helsinki.fi/users/reriksso/procmail/mini-faq.html — Un eccellente documento FAQ su Procmail, con suggerimenti per la risoluzione dei problemi e dettagli sul blocco dei file e l'uso di caratteri jolly.
- http://www.uwasa.fi/~ts/info/proctips.html — Fornisce numerosi suggerimenti che, in molti casi, facilitano l'uso di Procmail, incluso il metodo per verificare i file `.procmailrc` e l'utilizzo dello scoring Procmail per decidere se eseguire una particolare azione.
- http://www.spamassassin.org/ — Il sito ufficiale del progetto SpamAssassin.

11.6.3. Libri correlati

- *Sendmail* di Bryan Costales ed Eric Allman e al; O'Reilly & Associates — un valido riferimento su Sendmail scritto con l'assistenza dell'autore originale di Delivermail e Sendmail.
- *Removing the Spam: Email Processing and Filtering* di Geoff Mulligan; Addison-Wesley Publishing Company — un volume che illustra diversi metodi usati dagli amministratori di posta elettronica che utilizzano tool affermati, quali Sendmail e Procmail, per gestire i problemi di spam.
- *Internet Email Protocols: A Developer's Guide* di Kevin Johnson; Addison-Wesley Publishing Company — fornisce una rivisitazione approfondita dei principali protocolli di posta elettronica e la sicurezza che garantiscono.
- *Managing IMAP* di Dianna Mullet e Kevin Mullet; O'Reilly & Associates — illustra in modo dettagliato le fasi necessarie per la configurazione di un server IMAP.
- *Red Hat Enterprise Linux Security Guide*; Red Hat, Inc. — Il capitolo *Sicurezza del server*, spiega i diversi modi per rendere sicuro Sendmail e altri servizi.

Capitolo 12.

BIND (Berkeley Internet Name Domain)

Nella maggior parte di reti moderne, incluso Internet, gli utenti identificano gli altri computer dal nome. Ció consente all'utente di non ricordare l'indirizzo di rete numerico delle risorse della rete. Il modo migliore per configurare una rete in modo da abilitare i collegamenti basati sul nome, è quello di impostare un *Domain Name Service* (*DNS*) o un *nameserver*, che converte gli hostname sulla rete in indirizzi numerici e viceversa.

In questo capitolo verrà trattato il nameserver presente in Red Hat Enterprise Linux, il server DNS *Berkeley Internet Name Domain* (*BIND*), con risalto alla struttura dei suoi file di configurazione e il modo in cui può essere amministrato in modo locale o remoto.

Per istruzioni sulla configurazione di BIND tramite il **Tool di configurazione del servizio del nome del dominio**, `redhat-config-bind`, consultate il capitolo *Configurazione di BIND* nella *Red Hat Enterprise Linux System Administration Guide*.

Avvertenza

Se usate il **Tool di configurazione del servizio del nome del dominio**, ricordatevi di non modificare manualmente i file di configurazione BIND, poichè qualsiasi modifica manuale verrá sovrascritta la volta successiva che userete il **Tool di configurazione del servizio del nome del dominio**.

12.1. Introduzione a DNS

Quando gli host su di una rete, si collegano ad un'altra tramite un hostname, chiamato anche *fully qualified domain name (FQDN)*, viene usato un DNS per associare i nomi delle macchine all'indirizzo IP per l'host.

L'uso dei nomi FQDN e DNS, è vantaggioso per gli amministratori di sistema, perché consente una certa flessibilità nella modifica degli indirizzi IP per un host, senza influire sulle interrogazioni basate sui nomi dei computer stessi. Gli amministratori inoltre possono stabilire quale computer gestisce una interrogazione basata sui nomi.

Il DNS, viene normalmente implementato utilizzando server centrali che risultano "autorevoli" per alcuni domini e si rivolgono ad altri server DNS per ottenere le informazioni di cui non dispongono.

Quando un'applicazione client richiede informazioni al server dei nomi, di solito essa si collega tramite la porta 53 del server. Il server dei nomi cerca di risolvere l'FQDN in base alla sua libreria di conversione, che può contenere informazioni "autorevoli" per l'FQDN in questione oppure dati memorizzati in seguito a una precedente query. Se la libreria di conversione del server dei nomi non contiene già la risposta, esso si rivolgerà ad altri server di nomi, chiamati *server dei nomi root* per determinare quali sono i server di nomi autorevoli per l'FQDN in questione. Poi, con queste informazioni, chiede ai server dei nomi autorevoli il nome per determinare l'indirizzo IP. Se invece si esegue una ricerca inversa, viene utilizzata la stessa procedura, ma la richiesta è inoltrata con un indirizzo IP sconosciuto anziché un nome.

12.1.1. Zone del server dei nomi

Su internet, l'FQDN di un host può essere suddiviso in sezioni diverse, organizzate in una gerarchia (ad albero) con un tronco, dei rami principali, dei rami secondari e così via. Considerate il seguente FQDN:

```
bob.sales.example.com
```

Per capire come l'FQDN venga convertito per trovare l'indirizzo IP che si riferisce a un determinato sistema, è necessario leggere il nome da destra a sinistra, con ogni livello della gerarchia separato da punti (`.`). In questo esempio, `com` indica il *dominio del livello superiore* per questo FQDN. Il nome `example` indica un sottodominio di `com` e a sua volta, `sales` è un sottodominio di `example`. L'ultimo nome a sinistra in un FQDN, `bob`, è l'hostname della macchina specifica.

A eccezione dell'hostname, ogni sezione è definita *zona*, e contraddistingue un particolare *spazio dei nomi*. Tale *spazio* controlla la denominazione dei sottodomini alla propria sinistra. Mentre in questo esempio sono contenuti solo due sottodomini, un FQDN deve contenerne almeno uno, ma può comprenderne molti di più, a seconda di come sono organizzati gli spazi dei nomi.

Le zone sono definite nei server dei nomi autorevoli mediante l'uso di *file zone*, che descrivono lo spazio dei nomi di quella zona e i server di posta da usare per un dominio o sottodominio particolare. I file zone sono memorizzati in *server dei nomi primari* (chiamati anche *server master*) che sono autorevoli e consentono la modifica dei file e nei *server dei nomi secondari* (chiamati anche *server slave*), che ricevono i propri file zone dai server dei nomi primari. Ogni server dei nomi può essere allo stesso tempo primario o secondario per zone diverse e può essere riconosciuto autorevole per più zone. Dipende tutto dalla configurazione del server dei nomi.

12.1.2. Tipi di server dei nomi

Esistono quattro tipi principali di configurazione per i server dei nomi:

- *master* — Memorizza la zona originale e autorevole, registra un namespace, e risponde alle richieste inerenti al namespace provenienti da altri server dei nomi.
- *slave* — risponde a richieste di altri server dei nomi relative agli spazi dei nomi sui quali ha autorità. Comunque i server slave ottengono le informazioni sugli spazi dei nomi dai server master.
- *caching-only* — offre il nome ai servizi di risoluzione IP ma non è autorevole per tutte le zone. Di norma, le risposte a tutte le risoluzioni vengono memorizzate in un database archiviato in memoria per un determinato periodo di tempo, solitamente specificato dal record di zona recuperato.
- *forwarding* — inoltra richieste a un elenco specifico di server dei nomi da convertire. Se nessuno dei server specificati può eseguire la risoluzione, il processo si interrompe e la risoluzione non viene completata.

Un server dei nomi può essere di uno o più tipi tra quelli descritti. Per esempio può essere un master per alcune zone e uno slave per altre e può offrire solo una risoluzione forwarding.

12.1.3. BIND come un server dei nomi

BIND effettua dei servizi di risoluzione del nome, attraverso il demone `/usr/sbin/named`. BIND include anche una utility di gestione chiamata `/usr/sbin/rndc`. Maggiori informazioni su `rndc` sono disponibili nella Sezione 12.4.

BIND conserva i propri file di configurazione nelle seguenti posizioni:

- `/etc/named.conf` — Il file di configurazione per il demone `named`.
- `/var/named/` directory — La directory `named` dove si trovano i file zone, statistici, ecc.

Le sezioni successive descrivono in dettaglio i file di configurazione BIND.

12.2. /etc/named.conf

Il file named.conf è un insieme di istruzioni che utilizza opzioni nidificate tra parentesi graffe { }. Gli amministratori devono prestare attenzione nel modificare named.conf, in quanto piccoli errori di sintassi impediscono la partenza del servizio named.

Avvertenza

Non modificate manualmente il file /etc/named.conf o qualsiasi file nella directory /var/named/, se state utilizzando l'applicazione **Tool di configurazione del servizio del nome del dominio**. Tutte le modifiche manuali apportate a questi file, verranno sovrascritte al successivo utilizzo di **Tool di configurazione del servizio del nome del dominio**.

Un file tipico named.conf é organizzato in modo del tutto simile al seguente esempio:

```
<statement-1> ["<statement-1-name>"] [<statement-1-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};

<statement-2> ["<statement-2-name>"] [<statement-2-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};

<statement-N> ["<statement-N-name>"] [<statement-N-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};
```

12.2.1. Tipo di istruzioni comuni

Le seguenti istruzioni vengono utilizzate comunemente in /etc/named.conf:

12.2.1.1. Istruzioni acl

L'istruzione acl (o commento di controllo di accesso) definisce il gruppo o gli host permessi o meno all'accesso al server dei nomi.

Una istruzione acl ha la seguente forma:

```
acl <acl-name> {
    <match-element>;
    [<match-element>; ...]
};
```

In questa istruzione, sostituire *<acl-nome>* con il nome della lista di controllo accesso e sostituire *<elemento-corrispondente>* con una serie di indirizzi IP separati da un punto e virgola. La maggior parte delle volte vengono utilizzati gli indirizzi IP individuali o le notazioni di rete IP (come 10.0.1.0/24) per identificare gli indirizzi IP all'interno del commento acl.

Le seguenti liste di controllo per gli accessi sono giá definite come parole chiavi per semplificare la configurazione:

- `any` — corrisponde a ogni indirizzo IP.
- `localhost` — corrisponde a qualsiasi indirizzo IP in uso nel sistema locale.
- `localnets` — corrisponde a qualsiasi indirizzo IP in qualsiasi rete a cui il sistema locale è connesso.
- `none` — non corrisponde a nessun indirizzo IP.

Se utilizzato con altre istruzioni (come ad esempio `options`), i commenti `acl` possono essere molto utili nel prevenire l'uso improprio di un server dei nomi BIND.

Il seguente esempio definisce due liste di controllo di accesso e usa una istruzione `options` per definire come vengono trattate dal server:

```
 acl black-hats {
    10.0.2.0/24;
    192.168.0.0/24;
 };

acl red-hats {
    10.0.1.0/24;
 };

options {
    blackhole { black-hats; };
    allow-query { red-hats; };
    allow-recursion { red-hats; };
 }
```

Questo esempio contiene due elenchi di controllo per l'accesso, `black-hats` e `red-hats`. Gli host nell'elenco `black-hats` non vengono accettati nel server dei nomi, mentre vengono accettati nell'elenco `red-hats`.

12.2.1.2. L'istruzione `include`

L'istruzione `include` permette ai file di essere inclusi in un file `named.conf`. In questo modo i dati importanti di configurazione (come ad esempio `keys`), possono essere posizionati in un file separato con permessi restrittivi.

Una istruzione `include` assume la seguente forma:

```
include  "<file-name>"
```

In questa istruzione, *<nome-file>* viene sostituito con un path assoluto per un file.

12.2.1.3. Istruzione `options`

L'istruzione `options` definisce le opzioni di configurazione globale del server e imposta i default per altri commenti. Puó essere usato per specificare la posizione della directory di lavoro `named` i tipi di interrogazione permessi e molto altro.

L'istruzione `options` assume la seguente forma:

```
options {
        <option>;
 [<option>; ...]
};
```

In questa istruzione, le direttive *<option>* sono sostituite con una opzione valida.

Le seguenti sono opzioni usate comunemente:

- `allow-query` — specifica gli host autorizzati a interrogare questo server. Per default, tutti gli host sono autorizzati. Un elenco di controllo dell'accesso o un insieme degli indirizzi o reti IP può essere utilizzato, in questo caso, solo per autorizzare degli host particolari a interrogare il server dei nomi.
- `allow-recursion` — simile a `allow-query`, tranne per il fatto che viene utilizzato per richieste ricorsive. Per default, tutti gli host sono autorizzati ad effettuare richieste ricorsive ai server dei nomi.
- `blackhole` — Specifica quali host non possono interrogare i server.
- `directory` — Specifica la directory di lavoro `named` se diversa dal valore di default `/var/named/`.
- `forward` — Specifica il modo in cui avviene l'inoltro da parte di una direttiva `forwarders`.

  Sono accettate le seguenti opzioni:

  - `first` — Specifica che i nameserver elencati nella direttiva `forwarders` vengano interrogati prima che `named` tenti di risolvere il nome da solo.
  - `only` — Specifica che `named` non cerchi di eseguire la risoluzione del nome da solo, nel caso in cui le interrogazioni ai nameserver specificati nella direttiva `forwarders` falliscano.

- `forwarders` — Specifica un elenco di indirizzi IP validi per i server dei nomi a cui inviare le richieste di risoluzione.
- `listen-on` — specifica l'interfaccia di rete che `named` utilizza per ricevere le interrogazioni. Per default, vengono utilizzate tutte le interfacce.

  Usando questa direttiva su di un server DNS, il quale funge da gateway, BIND puó essere configurato in modo da rispondere solo alle domande originate da una delle reti.

  Una direttiva `listen-on` somiglia al seguente esempio:

```
options {
   listen-on { 10.0.1.1; };
};
```

  In questo esempio, vengono accettate solo le richieste che provengono dall'interfaccia di rete che serve la rete privata (`10.0.1.1`).
- `notify` — Controlla se `named` notifica i server slave quando si aggiorna una zona. Accetta le seguenti opzioni:

  - `yes` — Notifica i server slave.
  - `no` — Non notifica i server slave.
  - `explicit` — Notifica solo i server slave specificati in un elenco `also-notify` all'interno di una istruzione di zona.

- `pid-file` — vi consente di specificare la posizione del file di processo ID creato da `named`.
- `root-delegation-only` — Abilita la forzatura delle proprietà di delega nei top-level domains (TLD), e nelle zone root con un elenco di esclusione opzionale. *Delega* è quel processo di separazione di una singola zona in sottozone multiple. Per poter creare una zona delegata, vengono usati gli oggetti conosciuti come *record NS*. I record NameServer (record di delega) annunciano i nameserver principali per una zona particolare.

  L'esempio `root-delegation-only` seguente, specifica un elenco di esclusione di TLD, dai quali si prevedono delle risposte non delegate fidate:

```
options {
   root-delegation-only exclude { "ad"; "ar"; "biz"; "cr"; "cu"; "de"; "dm"; "id";
      "lu"; "lv"; "md"; "ms"; "museum"; "name"; "no"; "pa";
      "pf"; "se"; "sr"; "to"; "tw"; "us"; "uy"; };
};
```

- `statistics-file` — Vi consente di specificare la posizione in cui è stato salvato il file delle statistiche. Per default, le statistiche di `named` vengono salvate in `/var/named/named.stats`.

Sono inoltre disponibili decine di altre opzioni, molte delle quali dipendono l'una dall'altra per poter funzionare correttamente. Per maggiori informazioni, consultate il *Manuale BIND 9 di riferimento per l'amministratore* nella Sezione 12.7.1 e la pagina man per `bind.conf` per maggiori informazioni.

12.2.1.4. Istruzione `zone`

Una istruzione `zone` definisce le caratteristiche di una zona come ad esempio la posizione dei propri file di configurazione e le opzioni specifiche di zona. Questo commento puó essere usato per sovrascrivere i commenti globali `options`.

Una istruzione `zone` assume la seguente forma:

```
zone <zone-name> <zone-class> {
     <zone-options>;
     [<zone-options>; ...]
};
```

In questa istruzione, *<nome-zona>* é il nome della zona, *<classe-zona>* é la zona facoltativa della zona, e *<opzioni-zona>* é un elenco di opzioni che caratterizzano la zona.

L'attributo *<nome-zona>* per l'istruzione della zona, é particolarmente importante. Esso è il valore di default assegnato per la direttiva `$ORIGIN`, usata all'interno delfile zone corrispondente posizionato nella directory `/var/named/`. Il demone `named` conferisce il nome della zona a qualsiasi nome del dominio non qualificato elencato nel file zone.

Per esempio, se una istruzione `zone` definisce lo spazio del nome per `example.com`, usare `example.com` come *<zone-name>* cosí da posizionarlo alla fine dell'hostname all'interno del file zone `example.com`.

Per maggiori informazioni sui file zone, consultare la Sezione 12.3.

Le opzioni piú comuni della `zone` include quanto segue:

- `allow-query` — Specifica i client abilitati a richiedere informazioni inerenti questa zona. Per default tutte le richieste vengono permesse.
- `allow-transfer` — Specifica i server slave abilitati a richiedere un trasferimento delle informazioni della zona. Il default é di permettere tutte le richieste di trasferimento.
- `allow-update` — Specifica gli host che sono permessi ad aggiornare dinamicamente le informazioni nella loro zona. Il default é di negare tutte le richieste di aggiornamento dinamico.

  Fare attenzione a permettere agli host di aggiornare le informazioni inerenti le loro zone. Non abilitare questa funzione se l'utente non é fidato. In generale, é meglio avere un amministratore che aggiorni manualmente le informazioni e ricaricare il servizio `named`.
- `file` — Specifica il nome del file nella directory di lavoro che contiene i dati di configurazione della zona. Il default é la directory `/var/named/`.
- `masters` — Specifica gli indirizzi IP dai quali si effettua la richiesta di informazioni della zona autoritaria, usatosolo se la zona é definita come `type eslave`.
- `notify` — Specifica se `named` effettua la notifica ai server slave quando si aggiorna una zona. Questa direttiva accetta le seguenti opzioni:

- `yes` — Notifica i server slave.
- `no` — Non notifica i server slave.
- `explicit` — Notifica solo i server slave specificati in un elenco `also-notify` all'interno di una istruzione di zona.

- `type` — Definisce il tipo di zona.

  Di seguito viene riportata una lista di opzioni valide:

  - `delegation-only` — Forza lo stato di delega delle zone dell'infrastruttura, come ad esempio COM, NET oppure ORG. Qualsiasi risposta ricevuta senza una delega implicita o esplicita, viene trattata come `NXDOMAIN`. Questa opzione viene applicata solo in TLD, o nelle zone root utilizzate con implementazioni caching o ricorsive.
  - `forward` — Inoltra tutte le richieste di informazioni di una zona in particolare ad altri server dei nomi.
  - `hint` — tipo speciale di zona usato per fare riferimento ai server dei nomi root, utilizzati per risolvere richieste quando una zona è sconosciuta. In genere non è necessario configurare una zona del tipo `hint`.
  - `master` — Definisce il server dei nomi autorevole per questa zona. Occorre impostare una zona del tipo `master` se nel vostro sistema vi sono i file di configurazione della zona.
  - `slave` — Definisce il server come slave per questa zona. Specifica anche l'indirizzo IP del server dei nomi per la zona.

- `zone-statistics` — Configura `named` in modo da conservare le statistiche relative a questa zona, scrivendole nella posizione di default (`/var/named/named.stats`), o nel file elencato nell'opzione `statistics-file` nell'istruzione `server`. Consultate la Sezione 12.2.2 per maggiori informazioni riguardanti l'istruzione `server`.

12.2.1.5. Istruzione `zone`: esempi

La maggior parte delle modifiche al file `/etc/named.conf` di un server dei nomi master o slave riguarda l'aggiunta, la modifica o la cancellazione di istruzioni `zone`. Sebbene queste istruzioni possano contenere molte opzioni, quasi tutti i server dei nomi ne usano solo alcune. I commenti `zone` che seguono sono alcuni esempi di base da utilizzare in una relazione master/slave.

Quello riportato di seguito è un esempio di istruzione`zone` per il server dei nomi primario con dominio `example.com` (`192.168.0.1`):

```
zone "example.com" IN {
  type master;
  file "example.com.zone";
  allow-update { none; };
};
```

All'interno dell'istruzione la zona è identificata come `example.com`, il tipo è impostato su `master` e il servizio `named` legge il file `/var/named/example.com.zone`. Indica inoltre a `named` di non consentire l'aggiornamento da parte di nessun altro host.

Una istruzione `zone` di un server slave per `example.com` è leggermente diverso dall'esempio precedente. Per un server slave il tipo è impostato su `slave` e invece della riga `allow-update` è presente una direttiva che indica a `named` l'indirizzo IP del server master.

Quello riportato di seguito è un esempio di istruzione `zone`del server slave, per la zona `example.com`:

```
zone "example.com" {
  type slave;
  file "example.com.zone";
  masters { 192.168.0.1; };
};
```

Questa istruzione `zone` configura`named` sul server slave, in modo da interrogare il server master all'indirizzo IP `192.168.0.1`, per informazioni inerenti la zona `example.com`. Le informazioni che il server slave riceve dal server master vengono salvate in `/var/named/domain.com.zone`.

12.2.2. Altri tipi di istruzione

Ecco riportata una lista di istruzioni meno usate, disponibili in `named.conf`

- `controls` — Configura vari requisiti di sicurezza necessari all'uso del comando `rndc` per amministrare il servizion `named`.

  Consultate la Sezione 12.4.1 per saperne di più su come è strutturata l'istruzione `controls`, incluso le opzioni disponibili.

- `key "<key-name>"` — definisce una chiave particolare per il nome. Le chiavi sono usate per autenticare azioni varie, come ad esempio aggiornamenti sicuri o l'uso del comando `rndc`. Con `key` vengono utilizzate due opzioni:

  - `algorithm <algorithm-name>` — Il tipo di algoritmo usato, come ad esempio `dsa` o `hmac-md5`.
  - `secret "<key-value>"` — La chive cifrata.

  Consultate la Sezione 12.4.2 per informazioni su come scrivere una istruzione `key`.

- `logging` — Permette l'uso di tipi di log multipli chiamati *canali*. Usando l'opzione `channel` all'interno dell'istruzione `logging`, un tipo di log personalizzato, con il proprio nome del file (`file`), misura limite (`size`), versione (`version`), e livello d'importanza (`severity`), puó essere costruito. Una volta definito un canale personalizzato, una opzione `category` viene usata per categorizzare il canale e iniziare il logging quando si avvia `named`.

  Per default, `named` effettua una registrazione di messaggi standard per il demone `syslog`, inviandoli in `/var/log/messages`. Ció accade perché diversi canali standard sono stati costruiti in BIND con diversi livelli di severitá, come ad esempio il supporto di messaggi di logging (`default_syslog`), oppure il supporto specifico dei messaggi di debug (`default_debug`). Una categoria di default, chiamata `default`, usa i canali (del tipo built-in) per effettuare un logging normale senza alcuna configurazione speciale.

  Personalizzare un processo di log in, puó rappresentare un una fase molto articolata, e va oltre lo scopo di questo capitolo. Per maggiori informazioni sulla creazione dei log BIND personali, consultare *BIND 9 Administrator Reference Manual* nella Sezione 12.7.1.

- `server` — Specifica le opzioni che influenzano il comportamento di `named` rispetto ai server dei nomi remoti, in particolar modo nei confronti delle notifiche e dei trasferimenti di zona.

  L'opzione `transfer-format` controlla se una risorsa record viene inviata con ogni messaggio (`one-answer`) oppure se vengono inviate risorse record multiple sono inviate con ogni messaggio (`many-answers`). Mentre `many-answers` é piú efficiete, solo i server dei nomi BIND piú recenti lo possono comprendere.

- `trusted-keys` — Contiene diverse chiavi pubbliche usate per rendere sicuro DNS (DNSSEC). Consultare la Sezione 12.5.3 per maggiori informazioni sulla sicurezza di BIND.

- `view "<view-name>"` — Crea una visuale speciale a seconda della rete sulla quale viene effettuata l'interrogazione da parte dell'host al server dei nomi.Questo permette ad alcuni host di

ricevere una risposta riguardante una zona particolare, mentre altri host riceveranno delle informazioni totalmente diverse. Alternativamente, alcune zone vengono rese disponibili ad alcuni host sicuri mentre quelli non sicuri possono solo effettuare delle richieste ad altre zone.

Visuali multiple possono essere usate fino a quando i nomi sono unici. L'opzione `match-clients` specifica gli indirizzi IP idonei ad una visuale particolare. Qualsiasi istruzione `options` puó essere usato all'interno di una visuale, sovrascrivendo le opzioni globali giá configurate per `named`. Molti commenti `view` contengono commenti multipli `zone` idonei all'elenco `match-clients`. L'ordine con il quale i commenti `view` vengono elencati é molto importante, poichè viene usato il primo commento `view` idoneo ad un particolare indirizzo IP del client.

Consultate la Sezione 12.5.2 per maggiori informazioni sull'istruzione `view`.

12.2.3. Tag di commento

Il seguente é un elenco di tag di commento validi usati all'interno di `named.conf`:

- `//` — Quando posizionato all'inizio di una riga, la stessa viene ignorata da `named`.
- `#` — Quando posizionato all'inizio di una riga, la stessa viene ignorata da `named`.
- `/*` e `*/` — Quando il testo viene contenuto in queste etichette, lo stesso viene ignorato da `named`.

12.3. File zone

I *file zone*, contenenti le informazioni relative a un determinato namespace, sono memorizzati nella directory operativa di `named`, `/var/named` per default. Ogni file zone viene nominato a seconda dei dati indicati nell'opzione `file` contenuta nell'istruzione `zone`. In genere si riferisce al dominio in questione e identifica il file in quanto contiene dati sulla zona, come per esempio `example.com.zone`.

Ogni file zone può contenere *direttive* e dei *record della risorsa*. Le *direttive* indicano al server dei nomi di eseguire una certa azione o di eseguire delle impostazioni speciali per la zona. I record della risorsa definiscono i parametri della zona attribuendo una identità a host individuali. Le direttive sono facoltative, mentre i record della risorsa sono necessari per fornire il servizio dei nomi a quella zona.

Tutte le direttive ed i record dovrebbero essere inseriti su righe diverse.

Nei file zone è possibile aggiungere dei commenti dopo il carattere punto e virgola (`;`).

12.3.1. Direttive dei file zone

Le direttive sono contraddistinte dal carattere `$` che precede il nome della direttiva e che di solito si trova all'inizio del file zone.

Le direttive più usate sono le seguenti:

- `$INCLUDE` — indica a `named` di includere un file zone in un altro file nel punto in cui viene usata la direttiva. Ciò consente di memorizzare impostazioni di zona aggiuntive separatamente dal file zone principale.
- `$ORIGIN` — imposta il nome del dominio da accodare a qualsiasi record non qualificato, come quelli che specificano solo l'host e nient'altro.

  Per esempio, un file zone potrebbe contenere una riga seguente:
  `$ORIGIN example.com.`

  Qualsiasi nome utilizzato nei record della risorsa, che non terminacon un punto (`.`), presenterá `example.com`.

Nota bene

Non è necessario usare la direttiva `$ORIGIN` se alla zona si assegna un nome nel file `/etc/named.conf` identico al valore che assegnereste a `$ORIGIN`. Il nome della zona viene utilizzato, per default, come valore della direttiva `$ORIGIN`.

- `$TTL` — imposta il valore predefinito *Time to Live (TTL)* per la zona. Si tratta di un valore, in secondi, assegnato ai server dei nomi che indica il periodo di validità dei record di risorsa della zona. Un record di risorsa può avere un valore TTL proprio, che annulla quindi quello impostato da questa direttiva.

  Impostando un valore più alto si indica ai server dei nomi di conservare in memoria queste informazioni di zona per un periodo di tempo maggiore. Ciò riduce il numero di richieste relative a questa zona, ma allunga anche il tempo necessario per modificare il record di risorse.

12.3.2. Informazioni sulla risorsa del file zone

Il componente primario di un file zone risulta essere il proprio record di risorsa.

Sono disponibili diversi record della risorsa del file zone. I seguenti tipi sono tra i più usati:

- `A` — informazioni sull'indirizzo che specifica un indirizzo IP da assegnare al nome, come in questo esempio:

  ```
  <host>      IN      A      <IP-address>
  ```

  Se non viene indicato il valore <*host*>, il record `A` fa riferimento a un indirizzo IP predefinito per l'inizio dello spazio dei nomi. Questo sistema è utilizzato per tutte le richieste non FQDN.

  Prendete in considerazione i seguenti esempi di record `A` per il file zone `example.com`:

  ```
                IN      A       10.0.1.3
  server1       IN      A       10.0.1.5
  ```

  Le richieste per `example.com` vengono indirizzate a 10.0.1.3, mentre quelle per `server1.example.com` a 10.0.1.5.

- `CNAME` — record di nome tipico che mappa un nome all'altro, conosciuto anche come un alias.

  L'esempio successivo indica a `named` che le richieste inviate a <*nome-alias*> dovrebbero indicare l'host <*nome-reale*>. I record `CNAME` sono utilizzati più comunemente per indicare i servizi che utilizzano uno schema di assegnazione dei nomi comune,come ad esempio `www` per i Web server.

  ```
  <alias-name>      IN      CNAME        <real-name>
  ```

  Considerate l'esempio riportato di seguito, in cui il record `A` lega un indirizzo IP con un hostname, mentre il record `CNAME` indica l'hostname `www` più usato.

  ```
  server1       IN      A       10.0.1.5
  www           IN      CNAME   server1
  ```

- `MX` — si tratta del record "Mail eXchange", che indica dove va inoltrata la posta inviata a un particolare spazio dei nomi controllato da questa zona.

  ```
        IN      MX      <preference-value>   <email-server-name>
  ```

  In questo esempio il <*valore-preferenza*> vi consente di classificare numericamente i server e-mail su cui preferite ricevere la posta elettronica per questo spazio dei nomi, dando la precedenza ad alcuni sistemi e-mail rispetto ad altri. Il record di risorsa `MX` con il <*valore-preferenza*> più basso ha la precedenza sugli altri, ma potete comunque impostare vari server di posta elettronica con lo stesso valore e distribuire quindi il traffico di posta.

  Il <*nome-server-email*> può essere un nome host o un FQDN.

  ```
        IN      MX      10      mail.example.com.
  ```

```
        IN      MX      20      mail2.example.com.
```

In questo esempio il primo server di posta `mail.example.com` ha la precedenza sul server `mail2.example.com` al momento della ricezione di posta per il dominio `example.com`.

- `NS` — record NameServer che annuncia i server dei nomi autorevoli per una determinata zona.

  Ecco un esempio di record `NS`:

```
        IN      NS      <nameserver-name>
```

  Il *<nome-nameserver>* dovrebbe essere un FQDN.

  Di seguito sono elencati due nomi di server come autorevoli per un dominio. Non importa se questi server dei nomi sono slave o master, poiché entrambi sono considerati autorevoli.

```
        IN      NS      dns1.example.com.
        IN      NS      dns2.example.com.
```

- `PTR` — record "PoinTeR" che serve per fare riferimento a un'altra "porzione" dello spazio dei nomi.

  I record `PTR` vengono usati principalmente per invertire la risoluzione del nome, in quanto essi riferiscono gli indirizzi IP ad un particolare nome. Per maggiori esempi sull'opzione `PTR` in uso, consultate la Sezione 12.3.4.

- `SOA` — Start Of Authority, indica al nameserver le informazioni autorevoli importanti inerenti al namespace per il nameserver.

  Posizionato dopo le direttive, `SOA` è il primo record di risorsa in un file zone.

  L'esempio riportato mostra la struttura di base di un record di risorsa`SOA`:

```
@       IN      SOA     <primary-name-server>       <hostmaster-email> (
                        <serial-number>
                        <time-to-refresh>
                        <time-to-retry>
                        <time-to-expire>
                        <minimum-TTL> )
```

  Il simbolo `@` serve a posizionare la direttiva `$ORIGIN` (o il nome della zona, se la direttiva non è impostata) come il namespace definito da questo record di risorsa `SOA`. L'hostname del server dei nomi primario il quale è autoritario per questo dominio, è la direttiva *<primary-name-server>* e l'email della persona da contattare per questo namespace, è la direttiva *<hostmaster-email>*.

  La direttiva *<numero-seriale>* è un valore numerico incrementato ogni volta il file zone viene modificato, affinche `named` riceva l'informazione di ricaricare la zona. La direttiva *<tempo-di-aggiornamento>* è un server slave del valore numerico usato per determinare il tempo necessario prima di chiedere al server dei nomi master se sono state effettuate delle modifiche alla zona. La direttiva *<numero-seriale>* è un valore numerico utilizzato dai server slave per determinare se sta usando dati di zona obsoleti e deve dunque aggiornarli.

  La direttiva *<time-to-retry>* è un valore numerico usato dai server slave per determinare il periodo di tempo di attesa prima di formulare una richiesta di aggiornamento, se il server dei nominon risponde. Se il master non ha risposto alla richiesta di aggiornamento entro il periodo di tempo specificato in *<time-to- expire>*, i server slave cessano di fungere come autorità per quanto riguarda quel nameserver.

  La direttiva *<TTL-minimo>* è l'ammontare di tempo utilizzato dagli altri server dei nomi per memorizzare le informazioni della zona.

  Quando si configura BIND, il tempo viene riportato in secondi. Comunque potete utilizzare anche delle abbreviazioni per altre unità di tempo, come minuti (`M`), ore (`H`), giorni (`D`) e settimane (`W`). La Tabella 12-1 mostra la quantità di tempo in secondi e l'equivalente in un altro formato.

Secondi	Altre unità di tempo
Secondi	Altre unità di tempo
60	1M
1800	30M
3600	1H
10800	3H
21600	6H
43200	12H
86400	1D
259200	3D
604800	1W
31536000	365D

Tabella 12-1. Secondi paragonati ad altre unità di tempo

L'esempio seguente mostra la struttura che un record di risorsa `SOA` potrebbe avere quando popolato con valori reali.

```
@     IN     SOA    dns1.example.com.     hostmaster.example.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expire after 1 week
                    86400 )    ; minimum TTL of 1 day
```

12.3.3. Esempi di file zone

Le direttive e i record di risorsa, visti individualmente, possono essere difficili da comprendere. Comunque, tutto ha molto più senso se riunito in un unico file.

Il seguente esempio mostra un file zone di base.

```
$ORIGIN example.com.
$TTL 86400
@     IN     SOA    dns1.example.com.     hostmaster.example.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expire after 1 week
                    86400 )    ; minimum TTL of 1 day

      IN     NS     dns1.example.com.
      IN     NS     dns2.example.com.

      IN     MX     10     mail.example.com.
      IN     MX     20     mail2.example.com.

             IN     A       10.0.1.5

server1      IN     A       10.0.1.5
server2      IN     A       10.0.1.7
dns1         IN     A       10.0.1.2
dns2         IN     A       10.0.1.3
```

```
ftp             IN      CNAME   server1
mail            IN      CNAME   server1
mail2           IN      CNAME   server2
www             IN      CNAME   server2
```

In questo esempio vengono utilizzate le direttive standard e i valori `SOA`. I server dei nomi autorevoli impostati sono `dns1.example.com` e `dns2.example.com` con il record `A` che li lega rispettivamente a `10.0.1.2` e `10.0.1.3`.

Il server di posta configurato con i record `MX` fa riferimento a `server1` e `server2` tramite `CNAME`. Poiché i nomi del `server1` e del `server2` non terminano con un punto (`.`), il dominio `$ORIGIN` viene collocato dopo tali nomi, diventando `server1.example.com` e `server2.example.com`. È possibile determinarne gli indirizzi IP tramite i relativi record di risorsa `A`.

I servizi FTP e Web, disponibili con i nomi standard `ftp.example.com` e `www.example.com` vengono indirizzati a macchine che forniscono i servizi adeguati per questi nomi usando i record `CNAME`.

12.3.4. File zone per la risoluzione inversa dei nomi

Un file zone per la risoluzione inversa dei nomi viene utilizzato per tradurre un indirizzo IP in uno spazio particolare in un FQDN. Somiglia molto a un file zone standard, tranne per il fatto che i record di risorsa `PTR`, vengono utilizzati per collegare gli indirizzi IP a un nome del dominio qualificato.

Un record `PTR` è simile a quanto riportato di seguito:

```
<last-IP-digit>       IN      PTR     <FQDN-of-system>
```

<ultima-cifra-IP> si riferisce all'ultimo numero in un indirizzo IP che dovrebbe far riferimento all'FQDN di un determinato sistema.

Nell'esempio riportato di seguito gli indirizzi IP da `10.0.1.20` a `10.0.1.25` fanno riferimento agli FQDN corrispondenti.

```
$ORIGIN 1.0.10.in-addr.arpa.
$TTL 86400
@     IN      SOA     dns1.example.com.     hostmaster.example.com. (
                      2001062501 ; serial
                      21600      ; refresh after 6 hours
                      3600       ; retry after 1 hour
                      604800     ; expire after 1 week
                      86400 )    ; minimum TTL of 1 day

      IN      NS      dns1.example.com.
      IN      NS      dns2.example.com.

20    IN      PTR     alice.example.com.
21    IN      PTR     betty.example.com.
22    IN      PTR     charlie.example.com.
23    IN      PTR     doug.example.com.
24    IN      PTR     ernest.example.com.
25    IN      PTR     fanny.example.com.
```

Questo file zone viene utilizzato con l'istruzione `zone` nel file `named.conf` simile a quello riportato di seguito:

```
zone "1.0.10.in-addr.arpa" IN {
  type master;
  file "example.com.rr.zone";
  allow-update { none; };
```

```
};
```

Esiste una differenza davvero minima tra questo esempio e un'istruzione standard `zone`, salvo per il nome della zona. Una zona per la risoluzione inversa dei nomi richiede che siano invertiti i primi tre blocchi dell'indirizzo IP e che dopo di questi venga aggiunto "`.in-addr.arpa`". Ciò permette che il blocco singolo di numeri IP utilizzato nel file della zona per la risoluzione inversa dei nomi venga collegato correttamente in questa zona.

12.4. Uso di `rndc`

BIND dispone di una utility chiamata `rndc` che vi consente di amministrare il demone `named` in modo locale o remoto tramite istruzioni dalla linea di comando.

Per impedire l'accesso non autorizzato del demone `named`, BIND usa un metodo di autenticazione a chiave segreta condivisa per garantire i privilegi a determinati host. Ció significa che una chiave identica deve essere presente in entrambi i file di configurazione `/etc/named.conf` e `rndc`, `/etc/rndc.conf`.

12.4.1. Configurazione di `/etc/named.conf`

Per consentire a `rndc` di connettersi al servizio `named`, è necessario disporre dell'istruzione`controls` nel proprio file `/etc/named.conf`.

L'istruzione `controls`, riportata nel seguente esempio, permette a `rndc` di collegarsi dal localhost.

```
controls {
  inet 127.0.0.1 allow { localhost; } keys { <key-name>; };
};
```

Questa istruzione indica a `named` di ascoltare sulla porta TCP 953 di default dell'indirizzo di loopback e abilita i comandi `rndc` provenienti dall'host locale, su corretta indicazione della chiave. Il *<nome-chiave>* specifica un nome nell'istruzione `key` all'interno del file `/etc/named.conf`. L'esempio successivo mostra l'istruzione `key`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

In questo caso, il *<valore-chiave>* usa l'algoritmo MD5. Usate il seguente comando per generare le vostre chiavi usando l'algoritmo HMAC-MD5:

```
dnssec-keygen -a hmac-md5 -b <bit-length> -n HOST <key-file-name>
```

È consigliabile una chiave con una lunghezza minima di 256 bit. La chiave effettiva da inserire nell'area *<valore-chiave>* si trova nel file *<nome-file-chiave>* generato da questo comando.

Avvertenza

Poichè `/etc/named.conf` viene letto da tutti, è consigliabile posizionare l'istruzione `key` in un file separato e leggibile solo da un utente root, per poi usare una istruzione `include` come riferimento. Per esempio:

```
include "/etc/rndc.key";
```

12.4.2. Configurazione di `/etc/rndc.conf`

`key` é l'istruzione piú importante contenuta nel file `/etc/rndc.conf`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

Il <*nome-chiave*> e il <*valore-chiave*> devono avere le stesse impostazioni indicate nel file `/etc/named.conf`.

Per mettere insieme le chiavi specificate nel file `/etc/named.conf` del server, aggiungere le seguenti righe a `/etc/rndc.conf`.

```
options {
  default-server  localhost;
  default-key     "<key-name>";
};
```

Questa direttiva imposta la chiave di default globale. Tuttavia il file di configurazione `rndc` puó specificare chiavi diverse per server diversi, come nell'esempio riportato:

```
server localhost {
  key  "<key-name>";
};
```

Avvertenza

Assicurarsi che solo un utente root possa leggere o scrivere sul file `/etc/rndc.conf`.

Per maggiori informazioni sul file `/etc/rndc.conf`, controllare la pagina man di `rndc.conf`.

12.4.3. Opzioni della linea di comando

Un comando `rndc` ha la seguente forma:

```
rndc <options> <command> <command-options>
```

Quando si esegue `rndc` in un host locale configurato in modo corretto, è possibile utilizzare i seguenti comandi:

- `halt` — interrompe immediatamente il servizio `named`.
- `querylog` — Attiva la registrazione delle richieste effettuate dai client a questo server dei nomi.
- `refresh` — aggiorna il database del server dei nomi.
- `reload` — Indica al server dei nomi di ricaricare i file zone, ma di non cancellare tutti i risultati memorizzati in precedenza. Ciò vi consente di effettuare delle modifiche ai file zone senza perdere tutte le risoluzioni di nomi archiviate.

Se le modifiche riguardano solo una zona specifica, potete ricaricare solo quella zona aggiungendo il nome della zona dopo il comando `reload`.

- `stats` — Trasferisce le attuali statistiche di `named` nel file `/var/named/named.stats`.
- `stop` — Interrompe il server in modo tale da salvare tutti gli aggiornamenti dinamici e i dati *Incremental Zone Transfers* (*IXFR*) prima di uscire.

Se desiderate annullare le impostazioni predefinite nel file `/etc/rndc.conf`, sono disponibili le seguenti opzioni:

- `-c <file-configurazione>` — Specifica la posizione alternata di un file di configurazione.
- `-p <port-number>` — Specifica il numero di una porta da usare per la connessione `rndc`, diversa dalla porta 953 di default.
- `-s <server>` — Specifica un server diverso da `default-server` elencato in `/etc/rndc.conf`.
- `-y <key-name>` — Vi consente di specificare una chiave diversa da quella indicata dall'opzione `default-key` nel file `/etc/rndc.conf`.

Per ulteriori informazioni su queste opzioni, consultate la pagina man di `rndc`.

12.5. BIND: caratteristiche avanzate

La maggior parte delle versioni di BIND utilizza `named` per fornire servizi di risoluzione dei nomi o per fungere da autorità per un particolare dominio o sottodominio. Tuttavia la versione 9 di BIND comprende una serie di caratteristiche avanzate che, se opportunamente configurate e utilizzate, garantiscono un servizio DNS più sicuro ed efficiente.

Avvertenza

Alcuni di questi contenuti, come DNSSEC, TSIG e IXFR (i quali vengono definiti nella seguente sezione), andrebbero usati solo in ambienti di rete con server dei nomi capaci di supportarli. Se l'ambiente di rete comprende i server dei nomi non BIND o versioni BIND precedenti, verificate che ogni contenuto sia supportato prima di usarlo.

Tutte le caratteristiche trattate in questo paragrafo vengono approfondite nel *BIND 9 Administrator Reference Manual* nella Sezione 12.7.

12.5.1. Miglioramenti del protocollo DNS

BIND supporta i trasferimenti di zona incrementali (IXFR), grazie ai quali un server dei nomi slave effettua solo il download delle parti aggiornate di una zona modificata su di un server dei nomi master. Il processo di trasferimento standard richiede che l'intera zona venga trasferita a ogni server dei nomi slave, perfino per la più piccola modifica. Per domini molto diffusi con file di zona lunghi e numerosi server dei nomi slave, IXFR semplifica i processi di notifica e aggiornamento.

IXFR è disponibile solo se utilizzate un *aggiornamento dinamico* per modificare i record della zona master. Se invece modificate manualmente il file zone per effettuare delle modifiche, viene utilizzato Automatic Zone Transfer (AXFR). Per maggiori informazioni sull'aggiornamento dinamico, consultate il *BIND 9 Administrator Reference Manual*. Per maggiori informazioni, far riferimento a la Sezione 12.7.1.

12.5.2. Visualizzazioni multiple

Mediante l'uso dell'istruzione `view` del file `named.conf` BIND presenta informazioni diverse a seconda di quale rete effettua la richiesta.

Questa opzione è utile soprattutto se desiderate che i client esterni alla vostra rete non possano eseguire un determinato servizio DNS, ma non volete invece escludere i client interni.

L'istruzione `view` utilizza l'opzione `match-clients` per far corrispondere indirizzi IP o reti intere conferendo loro opzioni speciali e dati di zona.

12.5.3. Sicurezza

BIND supporta vari metodi di protezione per l'aggiornamento e il trasferimento di zone, in entrambi i server master e slave:

- *DNSSEC* — abbreviazione di *DNS SECurity*, questa caratteristica consente di cifrare alcune zone con una *chiave zona*.

  In tal modo le informazioni relative a zone specifiche possono essere verificate come provenienti da un server che le ha firmate con una determinata chiave privata, se il destinatario possiede la chiave pubblica del server dei nomi.

  La versione 9 di BIND supporta inoltre il metodo SIG(0) chiave pubblica/privata per l'autenticazione del messaggio.
- *TSIG* — abbreviazione di *Transaction SIGnatures*, questa caratteristica permette un trasferimento da master a slave solo dopo aver verificato l'esistenza della chiave segreta condivisa su entrambi i nameserver.

  Questa caratteristica rafforza il metodo IP standard basato sull'indirizzo per l'autorizzazione al trasferimento. Infatti un eventuale intruso per poter trasferire la zona non solo dovrebbe conoscere l'indirizzo IP ma anche la chiave segreta.

  La versione 9 di BIND supporta inoltre *TKEY*, ovvero un altro metodo a chiave segreta condivisa per l'autorizzazione a trasferimenti di zona.

12.5.4. IP versione 6

La versione 9 di BIND supporta il servizio del nome in ambienti IP versione 6 (IPv6) utilizzando i record di zona `A6`.

Se il vostro ambiente di rete comprende host con IPv4 e IPv6, è necessario usare il demone `lwresd`, lightweight resolver daemon, nei vostri client. Questo demone è un server dei nomi 'caching-only' davvero efficiente, che riconosce i nuovi record `A6` e `DNAME` utilizzati con IPv6. Per maggiori informazioni, consultate la pagina man di `lwresd`.

12.6. Errori comuni da evitare

Spesso i principianti commettono alcuni errori quando modificano i file di configurazione di BIND. Assicuratevi quindi di evitare i seguenti problemi:

- *Quando modificate un file zone, assicuratevi di incrementare il numero seriale.*

  Se non incrementate il numero seriale, il server dei nomi master potrà disporre delle nuove informazioni, ma il server dei nomi slave non riceverà notifiche di cambiamenti, e non aggiornerà quindi i propri dati relativi a quella zona.

- *Ricordatevi di usare in modo corretto le parentesi graffe e i punti e virgola nel file* `/etc/named.conf`

  Se omettete un punto e virgola oppure una parentesi, ne consegue il rifiuto di `named` all'avvio.

- *Non dimenticate di mettere i punti (`.`) nei file zone dopo tutti gli FQDN e di ometterli negli hostname.*

  Il punto indica che il nome assegnato è completo. Se manca il punto, `named` completerà questo nome con quello della zona o con il valore di `$ORIGIN`.

- *Se un firewall blocca le connessioni tra il demone* `named` *e altri server dei nomi, potrebbe essere necessario modificare il file di configurazione.*

  Per default, la versione 9 di BIND utilizza infatti porte randomiche superiori alla 1024 per interrogare altri nameserver. Alcuni firewall, tuttavia, presuppongono che i nameserver comunichino tra loro utilizzando la porta 53. Quindi per forzare `named` all'uso della porta 53, inserite la seguente riga nell'istruzione `options` di `/etc/named.conf`:

  ```
  query-source address * port 53;
  ```

12.7. Risorse aggiuntive

Le seguenti fonti potranno fornirvi ulteriori informazioni relative all'uso di BIND.

12.7.1. Documentazione installata

- BIND dispone di documentazione installata molto esauriente su diversi argomenti, ciascuno dei quali è contenuto in una cartella propria:
  - Directory `/usr/share/doc/bind-<numero-versione>/` — Un elenco dei contenuti più recenti. Sostituire `<numero-versione>` con la versione di `bind` installata sul sistema.
  - Directory `/usr/share/doc/bind-<numero-versione>/arm/` — Contiene i formati HTML e SGML del *BIND 9 Administrator Reference Manual* il quale elenca nel dettaglio i requisiti delle risorse di BIND, illustra come configurare diversi tipi di nameserver, esegue il bilanciamento del carico e spiega altre caratteristiche avanzate. Questo manuale è il punto di partenza, soprattutto per i nuovi utenti di BIND. Sostituite `<numero-versione>` con la versione di `bind` installata sul sistema.
  - Directory `/usr/share/doc/bind-<numero-versione>/draft/` — Contiene documenti tecnici di vario genere su problemi correlati al servizio DNS e ai relativi metodi per risolverli. Sostituire `<numero-versione>` con la versione di `bind` installata sul sitema.
  - Directory `/usr/share/doc/bind-<numero-versione>/misc/` — Contiene documenti ideati per trattare tematiche complesse. Gli utenti della versione 8 di BIND dovrebbero consultare il documento `migration`, per le modifiche da eseguire prima di migrare alla versione 9 di BIND. Il file `options` elenca tutte le opzioni implementate in BIND 9 e utilizzate in `/etc/named.conf`. Sostituite `<numero-versione>` con la versione di `bind` installata sul sistema.
  - Directory `/usr/share/doc/bind-<numero-versione>/rfc/` — In questa directory si trovano tutti i documenti RFC relativi a BIND. Sostituire `<numero-versione>`, con la versione di `bind` installata sul sistema.

- Pagine man relative a BIND — Con BIND sono presenti numerose pagine man per varie applicazioni e per i file di configurazione. Il seguente elenco riporta alcune delle pagine man più importanti.

Applicazioni di gestione

- `man rndc` — Esplicita opzioni diverse disponibili usando il comando `rndc` per controllare un server dei nomi BIND.

Applicazioni del server

- `man named` — Esplicitano diversi argomenti che possono essere usati per controllare il demone del server dei nomi BIND.
- `man lwresd` — Descrive lo scopo e le opzioni disponibili per il demone lightweight resolver.

File di configurazione

- `man named.conf` — Un elenco completo delle opzioni disponibili all'interno del file di configurazione `named`.
- `man rndc.conf` — Un elenco completo delle opzioni disponibili all'interno del file di configurazione `rndc`.

12.7.2. Siti Web utili

- http://www.isc.org/products/BIND — La home page del progetto BIND contenente le informazioni relative alle release attuali e della versione PDF del *BIND 9 Administrator Reference Manual*.
- http://www.redhat.com/mirrors/LDP/HOWTO/DNS-HOWTO.html — Illustra l'uso di BIND come nameserver di risoluzione, 'caching', e la configurazione dei vari file zone che fungono da nameserver primari per un dominio.

12.7.3. Libri correlati

- *Red Hat Enterprise Linux System Administration Guide* — Il capitolo *Configurazione BIND* spiega come impostare un server DNS usando **Tool di configurazione del servizio del nome del dominio**.
- *DNS e BIND* di Paul Albitz e Cricket Liu; edito da O'Reilly & Associates — un famoso libro di riferimento che illustra le opzioni di configurazione di BIND, incluso le strategie per rendere sicuroun server DNS.
- *The Concise Guide to DNS and BIND* di Nicolai Langfeldt; edito da Que — approfondisce la connessione tra servizi di rete multipli e BIND, concentrandosi in modo particolare sugli argomenti tecnici "task-oriented".

Capitolo 13.

LDAP (Lightweight Directory Access Protocol)

Lightweight Directory Access Protocol (*LDAP*) è un insieme di protocolli open usati per accedere alle informazioni conservate centralmente attraverso una rete. È basato su standard *X.500* per la condivisione della directory, ma è meno complesso e richiede meno risorse. Per questa ragione, LDAP viene indicato come "*X.500 Lite*." Lo standard LDAP viene talvolta indicato come ad una directory contenente informazioni sulla categoria e sulla gerarchia, tra le suddette informazioni si possono trovare i nomi, gli indirizzi ed i numero di telefono.

Come X.500, LDAP organizza le informazioni attraverso una scala gerarchica usando delle directory. Queste directory possono conservare una certa varietà di informazioni e possono anche essere usate in un modo simile al Network Information Service (NIS), abilitando chiunque ad accedere il proprio account da qualsiasi macchina presente sulla rete LDAP abilitata.

In molti casi LDAP viene usato come directory telefonica virtuale, permettendo agli utenti di accedere facilmente alle informazioni di contatto per altri utenti. LDAP è molto più flessibile della directory telefonica tradizionale, in quanto è capace di effettuare una richiesta ad altri server LDAP nel mondo, fornendo un deposito di informazioni globale ideale. Attualmente, tuttavia, LDAP è maggiormente usato all'interno di organizzazioni individuali, come università, uffici governativi, e di compagnie.

LDAP è un sistema client/server. Il server può usare una varietà di database per conservare una directory, ognuna delle quali è ottimizzata per operazioni di lettura veloci. Quando un'applicazione del client LDAP si collega ad un server LDAP, può sia interrogare la directory che cercare di modificarla. Nel caso in cui si verifica una interrogazione, il server può rispondere in modo locale, oppure può fare riferimento alla richiesta di un server LDAP il quale è in possesso di una risposta. Se l'applicazione di un client stà cercando di modificare le informazioni all'interno di una directory LDAP, il server verifica se l'utente possiede il permesso di effettuare il cambiamento, e successivamente aggiunge o aggiorna le informazioni.

Questo capitolo fà riferimento alla configurazione e all'uso di OpenLDAP 2.0, una implementazione della open source dei protocolli LDAPv2 e LDAPv3.

13.1. Perchè usare LDAP?

Il beneficio principale nell'uso di LDAP, è rappresentato dal fatto che le informazioni per una intera organizzazione possono essere consolidate in un deposito centrale. Per esempio, invece di gestire gli elenchi di un utente per ogni gruppo, all'interno di una organizzazione, LDAP può essere usato come una directory centrale accessibile da qualsiasi posizione della rete. Poichè LDAP supporta Secure Sockets Layer (SSL) e il Transport Layer Security (TLS), i dati sensibili possono essere protetti da utenti indiscreti.

LDAP supporta anche un numero di database del tipo back-end nei quali archiviare le directory. Ciò conferisce agli amministratori una certa flessibilità nell'impiegare il database che meglio si addice al tipo di informazioni che il server diffonde. Poichè LDAP possiede anche un Application Programming Interface (API) ben definito del client, il numero delle applicazioni abilitate-LDAP sono numerose e in aumento sia in quantità che in qualità.

13.1.1. Contenuti di OpenLDAP

OpenLDAP 2.0 presenta un numero di contenuti molto importanti.

- *Supporto LDAPv3* — OpenLDAP 2.0 supporta il Simple Authentication and Security Layer (SASL), Transport Layer Security (TLS), ed il Secure Sockets Layer (SSL), insieme ad altri

miglioramenti. Molti dei cambiamenti apportati al protocollo, dalla versione 2 di LDAP, sono stati effettuati per rendere LDAP più sicuro.

- *Supporto IPv6 Support* — OpenLDAP supporta il protocollo Internet versione 6.
- *LDAP tramite IPC* — OpenLDAP può comunicare all'interno di un sistema usando un interprocess communication (IPC). Questo permette di aumentare la sicurezza, eliminando il bisogno di comunicare attraverso la rete.
- *API C aggiornata* — Migliora il modo in cui i programmatori possono collegarsi e usare i server della directory LDAP.
- *Supporto LDIFv1* — Interamente compatibile con la versione 1 di LDAP Data Interchange Format (LDIF).
- *Server LDAP stand-alone aggiornato* — Comprende un sistema di controllo dell'accesso aggiornato, un raggruppamento dei thread, tool più efficaci e altro ancora.

13.2. Terminologia di LDAP

Qualsiasi discorso inerente LDAP, richiede una comprensione di base di un insieme di termini specifici di LDAP:

- *entry* è Una unità singola all'interno di una directory LDAP. Ogni directory è identificata dal proprio e unico *Distinguished Name* (*DN*).
- *attributi* —, Ossia informazione direttamente associate ad una entry. Per esempio, un'azienda potrebbe essere rappresentata come una voce LDAP. Gli attributi associati all'azienda possono essere il numero di fax, l'indirizzo e così via. Le persone potrebbero essere rappresentate come altre voci nella directory LDAP. Gli attributi comuni per le persone sono il numero di telefono e l'indirizzo e-mail.

  Alcuni attributi sono necessari, mentre altri sono facoltativi. Una tipologia di oggetti ben specifica *'objectclass'*, imposta gli attributi necessari e quelli facoltativi per ogni entry. Le definizioni di objectclass si trovano in diversi file contenuti nella directory `/etc/openldap/schema/`. Per maggiori informazioni consultate la Sezione 13.5.
- *LDIF* — L'*LDAP Data Interchange Format* (LDIF) è una rappresentazione del testo ASCII delle entry LDAP. I file usati per importare i dati ai server LDAP, devono essere in formato LDIF. Il seguente è un esempio di entry LDIF:

```
[<id>]
dn: <distinguished name>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
```

  Ogni entry può contenere tante coppie di `<attrtype>: <attrvalue>` quante ne sono necessarie. Una riga bianca indica la fine di una entry.

Attenzione

Tutte le coppie `<attrtype>` e `<attrvalue>` *devono* essere definite in un file schema corrispondente per usare questa informazione.

Ogni valore racchiuso fra < e >, è una variabile e può essere impostato quando viene creata una nuova entry LDAP. Tuttavia questa regola non viene applicata a `<id>`. `<id>` è un numero determinato dall'applicazione usata per modificare la entry.

13.3. Demoni e utility di OpenLDAP

La suite dei tool e delle librerie di OpenLDAP, si trovano all'interno dei seguenti pacchetti:

- `openldap` — Contiene le librerie necessarie per eseguire il server OpenLDAP e le applicazioni del client.
- `openldap-clients` — Contiene i tool della linea di comando per visualizzare e modificare le directory su di un server LDAP.
- `openldap-servers` — Contiene i server e altre utility necessarie a configurare ed eseguire il server LDAP.

Ci sono due server contenuti nel pacchetto `openldap-servers`: lo *Standalone LDAP Daemon* (`/usr/sbin/slapd`) e lo *Standalone LDAP Update Replication Daemon* (`/usr/sbin/slurpd`).

Il demone `slapd` è il server LDAP standalone mentre il demone `slurpd` è usato per sincronizzare i cambiamenti da un server LDAP ad un altro server LDAP sulla rete. Il demone `slurpd` viene usato solo quando si è in presenza di server LDAP multipli.

Per effettuare compiti amministrativi, il pacchetto `openldap-servers` installa le seguenti utility nella directory `/usr/sbin/`:

- `slapadd` — Aggiunge entry da un file LDIF a una directory LDAP. Per esempio, il comando `/usr/sbin/slapadd -l ldif-input`, legge nel file LDI, *`ldif-input`*, che contiene le nuove entry.

  
  Importante

  Solo l'utente root può usare `/usr/sbin/slapadd`. Tuttavia, il server della directory, viene esguito come utente `ldap`. Per questo motivo il server della directory non può modificare alcun file creato da `slapadd`. Per correggere questo problema, dopo aver usato `slapadd`, digitare il seguente comando:

  ```
  chown -R ldap /var/lib/ldap
  ```

- `slapcat` — Estrae le entry da una directory LDAP nel formato di default, il sistema *Berkeley DB di Sleepycat Software*, e le salva in un file LDIF. Per esempio, il comando `/usr/sbin/slapcat -l ldif-output` emette un file LDIF chiamato *`ldif-output`* contenente le entry dalla directory LDAP.
- `slapindex` — Ricrea l'indice della directory `slapd` basato sul contenuto corrente. Questo tool dovrebbe essere eseguito quando le opzioni dell'indice all'interno di `/etc/openldap/slapd.conf` sono cambiate.
- `slappasswd` — Genera un valore per la password cifrata dell'utente da usare con `ldapmodify` o il valore `rootpw` nel file di configurazione `slapd`, `/etc/openldap/slapd.conf`. Eseguite il comando `/usr/sbin/slappasswd` per creare la password.


Avvertenza

Assicuratevi di interrompere `slapd` emettendo il comanado `/sbin/service ldap stop`, prima di utilizzare `slapadd`, `slapcat` oppure `slapindex`. In caso contrario, rischiate di compromettere l'integrità della directory LDAP.

Per maggiori informazioni su come usare queste utility, consultate le rispettive pagine man.

Il pacchetto `openldap-clients` installa i tool all'interno di `/usr/bin/`, i quali vengono usati per aggiungere, modificare e cancellare le entry in una directory LDAP. Questi tool includono quanto segue:

- `ldapadd` — Aggiunge le entry ad una directory LDAP, accettando input standard o mediante file; `ldapadd` rappresenta un collegamento a `ldapmodify -a`.
- `ldapdelete` — Cancella le entry da una directory LDAP, accettando l'input dell'utente tramite un file oppure un prompt della shell.
- `ldapmodify` — Modifica le entry in una directory LDAP, accettandol'input tramite un input standard o tramite un file.
- `ldappasswd` — Imposta una password per un utente LDAP.
- `ldapsearch` — Cerca le entry in una directory LDAP utilizzando un prompt della shell.

Ad eccezione di `ldapsearch`, ognuna di queste utility è utilizzata più facilmente quando si riferisce ad un file contenente i cambiamenti da eseguire, invece di digitare un comando per ogni entry da cambiare all'interno di una directoryLDAP. Il formato di un file di questo tipo, è specificato nella pagina man per ogni utility.

13.3.1. NSS,PAM e LDAP

In aggiunta ai pacchetti OpenLDAP, Red Hat Enterprise Linux include un pacchetto chiamato `nss_ldap`, il quale aumenta l'abilità di LDAP di integrarsi in entrambi gli ambienti Linux e UNIX.

Il pacchetto `nss_ldap` fornisce i seguenti moduli:

- `/lib/libnss_ldap-<`*`glibc-versione`*`>.so`
- `/lib/security/pam_ldap.so`

Il pacchetto `nss_ldap` fornisce i seguenti moduli per le architetture Itanium o AMD64:

- `/lib64/libnss_ldap-<`*`glibc-versione`*`>.so`
- `/lib64/security/pam_ldap.so`

Il modulo `libnss_ldap-<`*`glibc-versione`*`>.so` permette alle applicazioni di cercare gli utenti, i gruppi, gli host e altre informazioni usando una directory LDAP tramite l'interfaccia di glibc *Nameservice Switch* (NSS) (sostituire `<`*`glibc-versione`*`>` con la versione di `libnss_ldap` in uso). NSS permette alle applicazioni di effettuare l'autenticazione usando LDAP insieme al NIS name service e ai file di autenticazione flat.

Il modulo `pam_ldap` permette alle apllicazioni PAM-aware di autenticare gli utenti usando informazioni conservate in una directory LDAP. Le applicazioni del tipo PAM-aware includono il log in della console, i server mail IMAP e POP, e Samba. Impiegando un server LDAP su di una rete, tutte queste applicazioni possono effettuare l'autenticazione usando lo stesso user ID e la combinazione password, semplificando notevolmente la gestione.

Per maggiori informazioni su come configurare PAM, consultate il Capitolo 16 e le relative pagine man.

13.3.2. PHP4, LDAP, e Server HTTP Apache

Red Hat Enterprise Linux include un pacchetto contenente un modulo LDAP per lo scripting della lingua del server-side PHP

Il pacchetto `php-ldap` aggiunge supporto LDAP allo scripting della lingua PHP4 HTML-embedded tramite il modulo `/usr/lib/php4/ldap.so`. Questo modulo permette agli script PHP4 di accedere alle informazioni conservate in una directory LDAP.

Red Hat Enterprise Linux contiene il modulo `mod_authz_ldap` per Server HTTP Apache. Questo modulo usa la forma abbreviata del distinguished name per il soggetto, e l'emittente del certificato SSL del client per determinare il distinguished name dell'utente all'interno della directory LDAP. È

altresì in grado di abilitare gli utenti in base agli attributi della entry della directory LDAP dell'utente stesso, determinando un accesso alle risorse in base ai privilegi dell'utente o del gruppo, negando tale accesso agli utenti che possiedono una password scaduta. È necessario il modulo `mod_ssl`, quando si usa il modulo `mod_authz_ldap`.

Importante

Il modulo `mod_authz_ldap` non autentica l'utente su di una directory LDAP che usa una password cifrata. Questa funzionalità viene fornita dal modulo sperimentale `mod_auth_ldap`, il quale non è incluso con Red Hat Enterprise Linux. Consultate il sito web di Apache Software Foundation, disponibile su http://www.apache.org/ per ottenere maggiori informazioni.

13.3.3. Applicazioni del client LDAP

Sono disponibili client LDAP grafici, i quali supportano la creazione e la modifica delle directory, essi però *non* sono inclusi con Red Hat Enterprise Linux. Una di queste applicazioni è **LDAP Browser/Editor** — Un tool basato su Java, disponibile online su http://www.iit.edu/~gawojar/ldap/.

Molti altri client LDAP accedono alle directory con permessi di sola lettura, usandole come riferimento, senza alterare, le informazioni inerenti all'organizzazione. Alcuni esempi di tali applicazioni sono Sendmail, **Mozilla**, **Gnome Meeting**, e **Evolution**.

13.4. File di configurazione di OpenLDAP

I file di configurazione di OpenLDAP vengono installati nella directory `/etc/openldap`. Il seguente rappresenta un breve elenco delle directory e dei file più importanti:

- `/etc/openldap/ldap.conf` — Esso rappresenta il file di configurazione per tutte le applicazioni del *client* che usano le librerie OpenLDAP, come ad esempio `ldapsearch`, `ldapadd`, Sendmail, **Evolution**, e **Gnome Meeting**.
- `/etc/openldap/slapd.conf` — Rappresenta il file di configurazione per il demone `slapd`. Consultare la Sezione 13.6.1per maggiori informazioni.
- `/etc/openldap/schema/` directory — Questa subdirectory contiene lo schema usato dal demone `slapd`. Consultare la Sezione 13.5 per maggiori informazioni.Modificate il file `/etc/openldap/slapd.conf` per mettere in relazione il vostro dominio e server LDAP. Per maggiori informazioni, consultate la Sezione 13.6.1.

NOTA BENE

Se è installato il pacchetto `nss_ldap`, viene creato un file chiamato `/etc/ldap.conf`. Questo file viene usato dai moduli PAM e NSS forniti dal pacchetto `nss_ldap`. Consultare la Sezione 13.7 per maggiori informazioni.

13.5. La directory `/etc/openldap/schema/`

La directory `/etc/openldap/schema/` contiene le varie definizioni di LDAP, che precedentemente si trovavano nei file `slapd.at.conf` e `slapd.oc.conf`. La directory `/etc/openldap/schema/redhat/` contiene gli schemi personalizzati distribuiti da Red Hat per Red Hat Enterprise Linux.

Tutte le *definizioni della sintassi degli attributi* e *le definizioni objectclass*, si trovano ora nei vari file di schema. Un riferimento viene fatto a questi file in `/etc/openldap/slapd.conf` utilizzando righe `include`, come visualizzato qui di seguito:

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

Attenzione

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

Potete estendere lo schema utilizzato da OpenLDAP in modo che supporti tipi di attributi aggiuntivi e tipi di oggetto che utilizzano i file schema di default come guida. Per farlo, create un file `local.schema` nella directory `/etc/openldap/schema`. Fate riferimento a questo nuovo schema all'interno di `slapd.conf` aggiungendo la seguente linea sotto le linee schema di default`include`:

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

È ora necessario definire i nuovi tipi di attributi e le classi degli oggettiall'interno del file `local.schema`. Molte organizzazioni utilizzano tipi di attributi esistenti dai file schema installati per default e aggiungono nuove classi al file `local.schema`.

La procedura di estensione dello schema per soddisfare determinati requisiti è piuttosto complessa ed esula dall'obiettivo di questo capitolo. Per ulteriori informazioni consultate il sito http://www.openldap.org/doc/admin/schema.html.

13.6. Panoramica sulla configurazione di OpenLDAP

Questa sezione presenta una breve panoramica su come installare e configurare una directory OpenLDAP. Per maggiori informazioni, consultate le seguenti URL:

- http://www.openldap.org/doc/admin/quickstart.html — La *Guida abbreviata su come iniziare* sul sito web di OpenLDAP.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — *LDAP Linux HOWTO* dalla Linux Documentation Project, riportata sul sito web di Red Hat.

Ecco riportate le fasi di base per la creazione di un server LDAP:

1. Installate i pacchetti RPM `openldap`, `openldap-servers` e `openldap-clients`.
2. Modificate il file `/etc/openldap/slapd.conf` per specificare il dominio LDAP e il server. Per maggiori informazioni, consultate la Sezione 13.6.1.

3. Avviate `slapd` con il comando:
   `/sbin/service ldap start`

   Dopo aver configurato LDAP, usare `chkconfig`, `ntsysv`, o lo **Strumento di configurazione dei servizi** per configurare LDAP in modo tale che inizi al momento dell'avvio. Per maggiori informazioni su come configurare i servizi, consultate il capitolo intitolato *Controllo dell'accesso ai servizi* nella *Red Hat Enterprise Linux System Administration Guide*.
4. Aggiungete le entry ad una directory LDAP con `ldapadd`.
5. Usate `ldapsearch` per determinare se `slapd` stia effettuando un accesso alle informazioni in modo corretto.
6. A questo punto, la directory LDAP dovrebbe funzionare correttamente e può essere configurata con applicazioni abilitate-LDAP.

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

Per usare il server LDAP `slapd`, modificare il proprio file di configurazione, `/etc/openldap/slapd.conf`, per specificare il dominio e i server corretti.

La riga `suffix` nomina il dominio per il quale il server LDAP fornisce le informazioni, tale riga và modificata nel modo seguente:

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

in modo che rifletta il nome del dominio qualificato. Per esempio:

```
suffix          "dc=example,dc=com"
```

La entry `rootdn` è il *Distinguished Name* (*DN*) per un utente che non ha limitazioni nei controlli di accesso o nei parametri limite amministrativi impostati per le operazioni sulla directory LDAP. L'utente `rootdn` può essere considerato un utente root per la directory LDAP. Nel file di configurazione, cambiare la riga `rootdn` dal suo valore di default come riportato dal seguente esempio:

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

Quando si popola una directory LDAP attraverso una rete, cambiare la riga `rootpw` — sostituendo il valore di default con una stringa della password cifrata. Per creare una stringa della password cifrata, digitare il seguente comando:

```
slappasswd
```

Quando richiesto, digitare due volte la password. Il programma visualizza la password cifrata risultante sul prompt della shell.

Successivamente, copiare la password cifrata appena creata in `/etc/openldap/slapd.conf` su di una delle righe `rootpw`,e rimuovere il carattere (`#`).

Quando avete terminato, la riga dovrebbe essere simile al seguente esempio:

```
rootpw {SSHA}vv2y+i6V6esazrIv70xSSnNAJE18bb2u
```

Avvertenza

Le password LDAP, incluso la direttiva `rootpw` specificata in `/etc/openldap/slapd.conf`, vengono inviate attraverso la rete in modo *non cifrato*, a meno che la codifica TLS non è abilitata.

Per abilitare la codifica TLS, rivedere i commenti in `/etc/openldap/slapd.conf`, e consultare la pagina man per `slapd.conf`.

Per maggiore sicurezza, la direttiva `rootpw`dovrebbe essere deselezionata dopo aver popolato la directory LDAP, precedendola con un carattere (`#`).

Quando usate il tool della linea di comando `/usr/sbin/slapadd` in modo locale per popolare la directory LDAP, non è necessario l'uso della direttiva `rootpw`.

Importante

Solo l'utente root può usare `/usr/sbin/slapadd`. Tuttavia, il server della directory viene eseguito come utente `ldap`. In questo modo il suddetto server non è in grado di modificare i file creati da `slapadd`. Per correggere questo problema, dopo aver usato `slapadd`, digitare il seguente comando:

```
chown -R ldap /var/lib/ldap
```

13.7. Configurazione di un sistema per l'autenticazione usando OpenLDAP

Questa sezione offre un riepilogo su come configurare una autenticazione dell'utente di OpenLDAP. A meno che non siate esperti nell'uso di OpenLDAP, sarà necessaria una documentazione più dettagliata di quella fornita. Per ulteriori informazioni, consultate i riferimenti forniti nella Sezione 13.9.

Installazione del pacchetto LDAP richiesto

Per prima cosa dovrete assicurarvi che vengano installati i pacchetti adeguati sia sul server LDAP, sia sulle macchine client LDAP. Il server LDAP necessita del pacchetto `openldap-servers`.

I pacchetti `openldap`, `nss_ldap` e `openldap-clients` devono essere installati su tutte le macchine client LDAP.

Modifica dei file di configurazione

- Sul server, modificare il file `/etc/openldap/slapd.conf` sul server LDAP per assicurarsi che corrisponda alle specifiche dell'organizzazione. Consultare la Sezione 13.6.1 per le istruzioni su come modificare `slapd.conf`.
- Sulle macchine client, sia `/etc/ldap.conf` che `/etc/openldap/ldap.conf` necessitano di contenere il server appropriato e ricercare le informazioni di base per l'organizzazione.

  Per fare questo, eseguire lo **Strumento di Configurazione per l'Autenticazione** (`system-config-authentication`) grafico e selezionare **Abilita il supporto LDAP** sotto la tabella **Informazioni dell'utente**.

  È possibile anche modificare questi file manualmente.
- Sulle macchine client, `/etc/nsswitch.conf` deve essere modificato in modo da poter usare LDAP.

  Per fare questo, eseguire lo **Strumento di Configurazione per l'Autenticazione** (`system-config-authentication`) e selezionare **Abilita il supporto LDAP** sotto la tabella **Informazioni dell'utente**.

Se si modifica manualmente `/etc/nsswitch.conf`, aggiungere `ldap` alle righe appropriate.

Per esempio:

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

13.7.1. PAM e LDAP

Per ottenere applicazioni PAM standard, utilizzare LDAP per l'autenticazione, eseguire lo **Strumento di Configurazione per l'Autenticazione** (`system-config-authentication`) e selezionare **Abilita il supporto LDAP** sotto la tabella **Autenticazione**. Per maggiori informazioni su come configurare PAM, consultare Capitolo 16 e le pagine man di PAM.

13.7.2. Migrazione delle vecchie informazioni sull'autenticazione nel formato LDAP

La directory `/usr/share/openldap/migration` contiene un insieme di script shell e Perl, che consentono di migrare le vecchie informazioni sull'autenticazione nel formato LDAP.

NOTA BENE

Per poter usare questi script, Perl deve essere installato.

Prima di tutto modificare il file `migrate_common.ph` in modo che rispecchi il dominio corretto. Il dominio DNS di default dovrebbe essere modificato dai suoi valori di default in modo seguente:

```
$DEFAULT_MAIL_DOMAIN = "example";
```

È consigliabile modificare anche la base di default, in modo seguente:

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

Il lavoro di migrazione di un database di un utente, in un formato che può essere letto dall'LDAP, viene effettuato da un gruppo di script di migrazione installati nella stessa directory. Usando la Tabella 13-1, selezionare quale script eseguire per migrare il database dell'utente.

Eseguite lo script adeguato in funzione al name service esistente.

I file `README` e `migration-tools.txt` nella directory `/usr/share/openldap/migration` forniscono maggiori dettagli su migrare le informazioni.

Name service attuale	LDAP è in esecuzione	Utilizzate questo script:
`/etc` flat files	sì	`migrate_all_online.sh`
`/etc` flat files	no	`migrate_all_offline.sh`
NetInfo	sì	`migrate_all_netinfo_online.sh`
NetInfo	no	`migrate_all_netinfo_offline.sh`

Name service attuale	LDAP è in esecuzione	Utilizzate questo script:
NIS (YP)	sì	`migrate_all_nis_online.sh`
NIS (YP)	no	`migrate_all_nis_offline.sh`

Tabella 13-1. Script di migrazione LDAP

13.8. Migrazione delle directory dalle release precedenti

Con Red Hat Enterprise Linux, OpenLDAP utilizza il sistema Berkeley DB di Sleepy Cat Software come il proprio formato di memoria su-disco per le directory. Le versioni precedenti di OpenLDAP usavano *GNU Database Manager* (*gdbm*). Per questa ragione, prima di aggiornare una implementazione LDAP in Red Hat Enterprise Linux 4, i dati LDAP originali dovrebbero essere esportati prima di poter procedere con tale aggiornamento, per poi reimportarli in un momento successivo. Quanto detto può essere fatto seguendo le fasi sotto riportate:

1. Prima di aggiornare il sistema operativo, eseguire il comando `/usr/sbin/slapcat -l` *`ldif-output`*. Questo emette un file LDIF chiamato *`ldif-output`* contenente le entry dalla directory LDAP.
2. Aggiornare il sistema operativo, prestate attenzione a non riformattare la partizione contenente il file LDIF.
3. Importare nuovamente la directory LDAP nel formato Berkeley DB aggiornato, per fare ciò eseguite il comando `/usr/sbin/slapadd -l` *`ldif-output`*.

13.9. Risorse aggiuntive

Le seguenti risorse offrono informazioni aggiuntive su LDAP. Usate queste risorse e, in particolare, visitate il sito Web OpenLDAP e LDAP HOWTO, prima di configurare LDAP sul sistema.

13.9.1. Documentazione installata

- Directory `/usr/share/docs/openldap-`*`numeroversione`* — Contiene un documento generale `README` e informazioni varie.
- Pagine man relative a LDAP — Sono presenti un certo numero di pagine man per le varie applicazioni e per i file di configurazione coinvolti con LDAP. Il seguente è un elenco di alcune delle più importanti pagine man.

  Applicazioni client

  - `man ldapadd` — Descrive come aggiungere le entry in una directory LDAP.
  - `man ldapdelete` — Descrive come cancellare le entry in una directory LDAP.
  - `man ldapmodify` — Descrive come modificare le entry in una directory LDAP.
  - `man ldapsearch` — Descrive come cercare le entry in una directory LDAP.
  - `man ldappasswd` — Descrive come impostare o cambiare la password di un utente LDAP.

Applicazioni server

- `man slapd` — Descrive le opzioni della linea di comando disponibili per il server LDAP.
- `man slurpd` — Descrive le opzioni della linea di comando disponibili per il server di replica LDAP.

Applicazioni amministrative

- `man slapadd` — Descrive le opzioni della linea di comando, usate per aggiungere delle entry su un database `slapd`.
- `man slapcat` — Descrive le opzioni della linea di comando, usate per generare un file LDIF da un database `slapd`.
- `man slapindex` — Descrive le opzioni della linea di comando, usate per generare un indice basato sui contenuti di un database `slapd`.
- `man slappasswd` — Descrive le opzioni della linea di comando, usate per generare le password di un utente per le directory LDAP.

File di configurazione

- `man ldap.conf` — Descrive il formato e le opzioni disponibili all'interno del file di configurazione per i client LDAP.
- `man slapd.conf` — Descrive il formato e le opzioni disponibili all'interno del file di configurazione riferito da entrambe le applicazioni del server LDAP (`slapd` e `slurpd`) e dai tool amministrativi LDAP (`slapadd`, `slapcat`, e `slapindex`).

13.9.2. Siti Web utili

- http://www.openldap.org/ — Home dell'OpenLDAP Project. Questo sito web contiene importanti informazioni su come configurare OpenLDAP, insieme con una pianificazione futura e alle modifiche apportate alla versione.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — Un LDAP HOWTO completo, importante e aggiornato.
- http://www.padl.com/ — Sviluppatori di `nss_ldap` e `pam_ldap`, insieme ad altri tool LDAP.http://www.padl.com — sviluppatori di `nss_ldap` e `pam_ldap` e altri tool LDAP.
- http://www.kingsmountain.com/ldapRoadmap.shtml — la Road Map LDAP di Jeff Hodges contiene link a numerose e utili FAQ e include le news sul protocollo LDAP.
- http://www.newarchitectmag.com/archives/2000/05/wilcox/ — Un sito utile per gestire i gruppi in LDAP.
- http://www.ldapman.org/articles/ — Contiene articoli che offrono una buona introduzione a LDAP, tra cui metodi per creare un albero della directory, e come personalizzare le strutture della directory stessa.

13.9.3. Libri correlati

- *OpenLDAP by Example* di John Terpstra e Benjamin Coles; Prentice Hall.
- *Implementing LDAP* di Mark Wilcox, pubblicato da Wrox Press, Inc.
- *Understanding and Deploying LDAP Directory Services* di Tim Howes et al., pubblicato da Macmillan Technical Publishing

Capitolo 14.

Samba

Samba è una implementazione open source del protocollo Server Message Block (SMB). Abilita il networking di Microsoft Windows®, Linux, UNIX, ed altri sistemi operativi, permettendo l'accesso ai file basati su Windows e delle condivisioni della stampante. L'utilizzo dell'SMB da parte di Samba, gli permette di apparire come un Windows server ai client di Windows.

14.1. Introduzione

La terzarelease di Samba, la versione 3.0.0, presenta diversi miglioramenti provenienti dalle versioni precedenti:

- La possibilità di registrarsi ad un Active Directory domain per mezzo di LDAP e Kerberos
- Supporto Unicode interno per tutte le lingue
- Supporto per i collegamenti sui server Samba di Microsoft Windows XP Professional client, senza la necessità di un local registry hacking
- Due nuovi documenti sviluppati dal team di Samba, i quali includono un manuale di riferimento con più di 400 pagine, ed uno con più di 300 pagine d'implementazione. Per maggiori informazioni, consultate la Sezione 14.9.3.

14.1.1. Contenuti di Samba

Samba è una applicazione server potente e versatile. Anche gli amministratori di sistema più esperti devono conoscere le sue abilità ed i suoi limiti prima di una sua installazione e configurazione.

Che cosa Samba è in grado di fare:

- Servire le diverse ramificazioni della directory e le stampanti a Linux, UNIX, e ai client di Windows
- Assistere al browsing della rete (con o senza NetBIOS)
- Autenticare i login al dominio di Windows
- Fornire il Windows Internet Name Service (WINS) per la risoluzione del nome del server
- Comportarsi come un Windows NT®-style Primary Domain Controller (PDC)
- Comportarsi come un Backup Domain Controller (BDC) per un PDC basato su Samba
- Comportarsi come un Active Directory domain member server
- Scegliete Windows NT/2000/2003 PDC

Cosa non è in grado di fare Samba:

- Comportarsi come un BDC per un PDC di Windows (e viceversa)
- Comportarsi come un Active Directory domain controller

14.2. Demoni di Samba e Servizi correlati

Quanto segue rappresenta una breve introduzione ai demoni Samba individuali ed ai servizi, insieme ai dettagli su come iniziarli ed arrestarli.

14.2.1. Panoramica sul Demone

Samba è composto da tre demoni (`smbd`, `nmbd`, e `winbindd`). Due servizi (`smb` e `windbind`) in grado di controllare il processo di avvio e di arresto dei demoni, e altri contenuti relativi al servizio. Ogni demone viene elencato in dettaglio insieme al servizio specifico che lo controlla.

14.2.1.1. Il demone `smbd`

Il demone del server `smbd` permette il file sharing e fornisce i servizi di stampa ai client di Windows. In aggiunta, è responsabile per l'autenticazione degli utenti, del resource locking, e della condivisione dei dati attraverso il protocollo SMB. Le porte di default attraverso le quali il server esegue l'ascolto del traffico SMB, sono porte TCP 139 e 445.

iIl demone `smbd` viene controllato dal servizio `smb`

14.2.1.2. Il demone `nmbd`

Il demone del server `nmbd` prende atto e replica alle richieste del nome del servizo NetBIOS, come quelle fornite da SMB/CIFS in sistemi basati su Windows. Questi sistemi includono Windows 95/98/ME, Windows NT, Windows 2000, Windows XP, e LanManager clients. Partecipa anche al browsing del protocollo che costituisce le **Risorse di Rete 'Network Neighborhood'** di Windows. La porta di default attraverso la quale il server ascolta il traffico NBM, è la porta UDP 137.

Il demone `nmbd` viene controllato dal servizio `smb`.

14.2.1.3. Demone `winbindd`

Il servizio `winbind` risolve le informazioni riguardanti l'utente ed il gruppo, su di un server Windows NT, rendendole compronsibili dalle piattaforme UNIX. Questo può essere fatto utilizzando le chiamate Microsoft RPC, Pluggable Authentication Modules (PAM), e Name Service Switch (NSS). Ciò permette agli utenti del dominio Windows NT, di comportarsi come utenti UNIX su di una macchina UNIX. Insieme con la distribuzione Samba, il servizio `winbind` è controllato separatamente dal servizio `smb`.

Il demone `winbindd` viene controllato dal servizio `winbind`, e non necessita del servizio `smb` per funzionare. Poichè `winbind` è un servizio di tipo client-side, utilizzato per collegarsi ai server basati su Windows NT, questo manuale non intende affrontare il demone `winbind`.

14.2.2. Come avviare e arrestare Samba

Per avviare un server Samba, digitare il seguente comando in un prompt della shell come utente root:

```
/sbin/service smb start
```

Importante

Per poter impostare un domain member server, dovete registrarvi al dominio o all'Active Directory usando il comando `net join`, *prima* di iniziare il servizio `smb`.

Per arrestare il server, digitare il seguente comando in un prompt della shell come utente root:

```
/sbin/service smb stop
```

L'opzione `restart` è un modo veloce per arrestare e successivamente avviare Samba. Questo rappresenta il modo più sicuro per apportare dei cambiamenti alla configurazione subito dopo la modifica del file di configurazione di Samba. Notate che l'opzione di riavvio, avvia il demone anche se esso non era in esecuzione.

Per riavviare il server, digitare il seguente comando in un prompt della shell come utenti root:

```
/sbin/service smb restart
```

L'opzione `condrestart` (*conditional restart*) avvia `smb` solo se lo stesso era precedentemente in esecuzione. Questa opzione è utile per gli script, in quanto non avvia il demone se lo stesso non era in esecuzione.

Nota Bene

Quando viene cambiato il file `smb.conf`, Samba lo ricarica automaticamente dopo pochi istanti. Eseguendo un comando manuale di `restart` o `reload` si ottiene lo stesso risultato.

Per riavviare il server in modo condizionato, digitare come utente root il seguente comando:

```
/sbin/service smb condrestart
```

Un ricaricamento manuale del file `smb.conf` può risultare utile nel caso in cui il ricaricamento manuale da parte del servizio `smb` fallisca. Per assicurarsi che il file di configurazione di Samba venga ricaricato senza riavviare il servizio, digitare come utente root il seguente comando:

```
/sbin/service smb reload
```

Per default, il servizio `smb` *non* viene avviato in modo automatico al momento dell'avvio. Per configurare Samba al momento dell'avvio, usare una utility initscript, come ad esempio `/sbin/chkconfig`, `/sbin/ntsysv`, o il programma **Strumento di configurazione dei servizi**. Consultate il capitolo intitolato *Controllo dell'Accesso ai Servizi* nella *Red Hat Enterprise Linux System Administration Guide* per maggiori informazioni su questi tool.

14.3. Tipi di server Samba e file `smb.conf`

La configurazione di Samba è molto semplice, Tutte le modifiche di Samba sono fatte nel file di configurazione `/etc/samba/smb.conf`. Anche se il file di default `smb.conf` è documentato molto bene, esso non risolve le problematiche più complesse come ad esempio LDAP, Active Directory, e le numerose implementazioni del controller del dominio.

Le seguenti sezioni descrivono i vari modi per configurare un server Samba. Tenete presente le vostre esigenze e le varie modifiche del file `smb.conf` necessarie per effettuare una configurazione corretta.

14.3.1. Server di tipo Stand-alone

Un server di tipo stand-alone può essere sia un server di tipo workgroup oppure un membro di un ambiente workgroup. Un server stand-alone non rappresenta un domain controller, e non partecipa in un dominio in alcun modo. I seguenti esempi mostrano diverse configurazioni di sicurezza 'share-level' anonime, ed una configurazione sicura 'user-level'. Per maggiori informazioni sulle modalità di sicurezza share-level e user-level consultate la Sezione 14.4.

14.3.1.1. Read-Only Anonimo

Il file `smb.conf` mostra un esempio di configurazione necessaria per implementare un file sharing di sola lettura anonimo. Il parametro `security = share` rende una condivisione anonima. Nota bene, il livello di sicurezza per un server Samba singolo non può essere diversificato. La direttiva `security` rappresenta un paramentro Samba globale, e si trova nella sezione di configurazione `[global]` del file `smb.conf`.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = share

[data]
comment = Documentation Samba Server
path = /export
read only = Yes
guest only = Yes
```

14.3.1.2. Lettura/Scrittura anonima

Il file `smb.conf` mostra un esempio di configurazione necessaria per implementare un file sharing di lettura/scrittura anonimo. Per abilitare il file sharing di lettura/scrittura anonimo, impostare la direttiva `read only` su `no`. Le direttive `force user` e `force group` vengono aggiunte per rinforzare l'ownership di qualsiasi nuovo file specificato nella condivisione.

Nota Bene

Anche se è possibile avere un server di lettura/scrittura anonimo, questo non è consigliato. A qualsiasi file che si trova nello spazio di condivisione, senza tener conto dell'utente, viene assegnato una combinazione utente/gruppo, come specificato da un utente generico (`force user`) e gruppo (`force group`), nel file `smb.conf`.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = share

[data]
comment = Data
path = /export
force user = docsbot
force group = users
read only = No
guest ok = Yes
```

14.3.1.3. Server di stampa anonimo

Il file `smb.conf` mostra un esempio di configurazione necessario per implementare un server di stampa anonimo. Impostando `browseable` su `no`, non viene elencata la stampante in Windows **Risorse di Rete 'Network Neighborhood'**. Anche se nascosto dal browsing, è possibile configurare la stampante. Collegandosi a `DOCS_SRV` usando NetBIOS, il client può accedere alla stampante se lo stesso client fà parte del workgroup `DOCS`. Si presume anche che il client abbia installato il corretto driver della stampante locale, in quanto la direttiva `use client driver` è impostata su `Yes`. In questo caso, il server Samba non ha alcuna responsabilità per la condivisione dei driver di stampa col client.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = share
printcap name = cups
disable spools= Yes
show add printer wizard = No
printing = cups

[printers]
comment = All Printers
path = /var/spool/samba
guest ok = Yes
printable = Yes
use client driver = Yes
browseable = Yes
```

14.3.1.4. File sicuri Read/Write e server di stampa

Il file `smb.conf` mostra un esempio di configurazione necessaria per implementare un server di stampa di lettura/scrittura sicuro. Impostando la direttiva `security` su `user`, si forza Samba all'autenticazione dei collegamenti client. Notate che la condivisione `[homes]` non possiede una direttiva `force user` o `force group` al contrario della condivisione `[public]`. La condivisione `[homes]` utilizza le informazioni dell'utente autenticato, per qualsiasi file creato in contrapposizione a `force user` e `force group` in `[public]`.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = user
printcap name = cups
disable spools = Yes
show add printer wizard = No
printing = cups

[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No

[public]
comment = Data
path = /export
force user = docsbot
force group = users
guest ok = Yes
```

```
[printers]
comment = All Printers
path = /var/spool/samba
printer admin = john, ed, @admins
create mask = 0600
guest ok = Yes
printable = Yes
use client driver = Yes
browseable = Yes
```

14.3.2. Server del Membro del Dominio

Un membro del dominio, anche se simile ad un server di tipo stand-alone, viene registrato nel domain controller (Windows o Samba), ed è soggetto alle regole di sicurezza del dominio. Un esempio di server del membro del dominio è rappresentato da un server dipartimentale in grado di eseguire Samba, il quale possiede un account della macchina sul Primary Domain Controller (PDC). Tutti i department client eseguono l'autenticazione con il PDC, includendo i profili desktop e tutti i file della policy di rete. La differenza è che il server dipartimentale possiede l'abilità di controllare le condivisioni di rete e di stampa.

14.3.2.1. Active Directory Domain Member Server

Il file `smb.conf` mostra un esempio di configurazione necessaria per implementare un Active Directory domain member server. In questo esempio, Samba esegue l'autenticazione degli utenti per i servizi eseguiti in modo locale, esso rappresenta anche un client dell'Active Directory. Assicuratevi che i vostri parametri `realm` di kerberos siano mostrati in modo completo (per esempio `realm = EXAMPLE.COM`). Poichè Windows 2000/2003 ha bisogno di Kerberos per l'autenticazione dell'Active Directory, è necessaria la direttiva `realm`. Se Active Directory e Kerberos sono in esecuzione su diversi server, potrebbe essere necessaria la direttiva `password server` per aiutare la suddetta distinzione.

```
[global]
realm = EXAMPLE.COM
security = ADS
encrypt passwords = yes
# Optional. Use only if Samba cannot determine the Kerberos server automatically.
password server = kerberos.example.com
```

Per poter unire un member server su di un Active Directory domain, è necessario completare le seguenti fasi:

- Configurazione del file `smb.conf` sul member server
- Configurazione di Kerberos, incluso il file `/etc/krb5.conf` sul member server
- Creazione dell'account della macchina sull'Active Directory domain server
- Associazione del member server sull'Active Directory domain

Per creare l'account della macchina e ottenere il Windows 2000/2003 Active Directory, è necessario inizializzzare prima Kerberos per i member server che desiderano unirsi all'Active Directory domain. Per creare un ticket amministrativo di Kerberos, digitare il seguente comando come utente root sul member server:

```
root# kinit administrator@EXAMPLE.COM
```

Il comando `kinit` è uno script di inizializzazione di Kerberos che fà riferimento all'Active Directory administrator account e al realm di Kerberos. Poichè l'Active Directory ha bisogno dei ticket di Kerberos, `kinit` ottiene e conserva il ticket proveniente dal kerberos ticket-granting per l'autenticazione del client/ server. Per maggiori informazioni su Kerberos, sul file `/etc/krb5.conf` e sul comando `kinit`, consultate il Capitolo 19.

Per far parte di un Active Directory server (windows1.example.com), digitare il seguente comando come utente root sul member server:

```
root# net ads join -S windows1.example.com -U administrator%password
```

Poichè la macchina `windows1` è stata trovata automaticamente nel realm del kerberos corrispondente (Il comando `kinit` successivo), il comando `net` si collega all'Active Directory server utilizzando l'account dell'amministratore e la password. Ciò crea l'account corretto della macchina sull'Active Directory e garantisce i permessi al server del membro di dominio Samba in modo da unirsi al dominio.

Nota Bene

Poichè viene utilizzato `security = ads` e non `security = user`, è necessario una password backend locale come ad esempio `smbpasswd`. I client più vecchi che non supportano `security = ads`, vengono autenticati come se `security = domain` sia stato impostato. Questa modifica non influenza la funzionalità e abilita gli utenti locali all'interno del dominio.

14.3.2.2. Domain Member Server basato su Windows NT4

Il file `smb.conf` mostra un esempio di configurazione necessaria per implementare un domain member server basato su Windows NT4. Diventare un member server di un dominio basato su NT4, è simile ad un collegamento ad una Active Directory. La differenza sostanziale è che i domini basati su NT4 non utilizzano Kerberos nei loro metodi di autenticazione, rendendo il file `smb.conf` più semplice. In questo esempio, il Samba member server serve da pass fino al domain server basato su NT4.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = domain

[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No

[public]
comment = Data
path = /export
force user = docsbot
force group = users
guest ok = Yes
```

Avere Samba come domain member server, può essere utile in molte situazioni. Ci sono momenti dove il server Samba può essere utile in determinate circostanze oltre al file sharing e al printer sharing. Potrebbe risultare utile fare di Samba un domain member server in casi dove solo le applicazioni Linux

sono necessarie per un loro utilizzo nell'ambiente di dominio. Gli amministratori preferiscono avere informazioni su tutte le macchine presenti nel dominio, anche se non sono basate su Windows. Nel caso in cui non viene consigliato un server hardware basato su Windows, risulta semplice modificare il file `smb.conf` per convertire il server in un PDC basato su Samba. Se i server basati su Windows NT vengono migliorati ad una versione di Windows 2000/2003, il file `smb.conf` è facilmente modificabile in modo da integrare la modifica dell'infrastruttura in Active Directory se necessario.

Importante

Dopo aver configurato il file `smb.conf`, registratevi nel dominio *prima* di avviare Samba, potete fare questo digitando il seguente comando come utente root:

```
root# net rpc join -U administrator%password
```

Notate che l'opzione `-S`, la quale specifica il domain server hostname, non ha bisogno di essere presente nel comando `net rpc join`. Samba utilizza l'hostname specificato dalla direttiva `workgroup` nel file `smb.conf`, invece di essere esplicitamente mensionato.

14.3.3. Controller del Dominio

Un controller del dominio di Windows NT è simile in termini funzionali ad un server Network Information Service (NIS) in un ambiente Linux. I controller del dominio ed i server NIS, ospitano entrambi i database per le informazioni user/group ed i servizi relativi. Tali controller vengono usati principalmente per motivi di sicurezza, incluso per l'autenticazione degli utenti che hanno accesso alle risorse del dominio. Il servizio che mantiene l'integrità del database user/group viene chiamato *Security Account Manager* (SAM). Il database SAM viene conservato in modo diverso tra i sistemi basati su Windows e quelli basati su Linux Samba, per questo motivo la replica di SAM non può essere eseguita, e le piattaforme non possono essere mischiate in un ambiente PDC/BDC.

In un ambiente Samba, ci può essere solo un PDC e zero o più BDC.

Importante

Samba non è in grado di esistere in un ambiente del tipo domain controller Samba/Windows misto (Samba non può essere un BDC di un PDC di Windows o viceversa). Alternativamente, i PDC ed i BDC di Samba *possono* coesistere.

14.3.3.1. Primary Domain Controller (PDC) usando `tdbsam`

L'implementazione più semplice e comune di un Samba PDC utilizza la password database backend `tdbsam`. Ideato per sostituire `smbpasswd` backend, `tdbsam` presenta numerosi miglioramenti, affrontati in dettaglio nella Sezione 14.5. La direttiva `passdb backend` controlla quale backend deve essere usato per il PDC.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
passdb backend = tdbsam
security = user
add user script = /usr/sbin/useradd -m %u
```

```
delete user script = /usr/sbin/userdel -r %u
add group script = /usr/sbin/groupadd %g
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/sbin/usermod -G %g %u
add machine script = \
 /usr/sbin/useradd -s /bin/false -d /dev/null \
 -g machines %u
# The following specifies the default logon script
# Per user logon scripts can be specified in the user
# account using pdbedit
logon script = logon.bat
# This sets the default profile path.
# Set per user paths with pdbedit
logon path = \\%L\Profiles\%U
logon drive = H:
logon home = \\%L\%U
domain logons = Yes
os level = 35
preferred master = Yes
domain master = Yes
idmap uid = 15000-20000
idmap gid = 15000-20000

[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No
writable = Yes

[public]
comment = Data
path = /export
force user = docsbot
force group = users
guest ok = Yes

[netlogon]
comment = Network Logon Service
path = /var/lib/samba/netlogon/scripts
admin users = ed, john, sam
guest ok = No
browseable = No
writable = No

# For profiles to work, create a user directory under the
# path shown. mkdir -p /var/lib/samba/profiles/john
[Profiles]
comment = Roaming Profile Share
path = /var/lib/samba/profiles
read only = No
browseable = No
guest ok = Yes
profile acls = Yes

# Other resource shares
...
...
```

Nota Bene

Se avete bisogno di più di un controller del dominio o se avete più di 250 utenti, *non* utilizzate una autenticazione `tdbsam` backend. Vi consigliamo in questo caso LDAP.

14.3.3.2. Primary Domain Controller (PDC) usando LDAP

L'implementazione più potente e versatile di un Samba PDC è rappresentata dalla sua abilità di avere un LDAP password backend. LDAP è molto scalabile. I server del database di LDAP possono essere utilizzati per ridondanza e per fail-over, replicando ad un Samba BDC. Gruppi di LDAP PDC e BDC con un bilanciamento del carico, sono ideali per un ambiente enterprise. D'altro canto le configurazioni LDAP sono complesse da impostare e gestire. Se SSL deve essere incorporato con LDAP, la complessità si raddoppia. Nonostante questo, con una pianificazione attenta e precisa, LDAP rappresenta la soluzione ideale per gli ambienti enterprise.

Notate la direttiva `passdb backend` insieme alle specificazioni del suffisso LDAP specifico. Anche se la configurazione Samba per LDAP è molto semplice, l'installazione di OpenLDAP non è semplice. LDAP dovrebbe essere installato e configurato prima di ogni configurazione Samba. Da notare anche che Samba e LDAP non hanno bisogno di essere sullo stesso server per poter funzionare. È consigliato separare i due in un ambiente enterprise.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
passdb backend = ldapsam:ldap://ldap.example.com
username map = /etc/samba/smbusers
security = user
add user script = /usr/sbin/useradd -m %u
delete user script = /usr/sbin/userdel -r %u
add group script = /usr/sbin/groupadd %g
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/sbin/usermod -G %g %u
add machine script = \
 /usr/sbin/useradd -s /bin/false -d /dev/null \
 -g machines %u
# The following specifies the default logon script
# Per user logon scripts can be specified in the
# user account using pdbedit
logon script = scripts\logon.bat
# This sets the default profile path.
# Set per user paths with pdbedit
logon path = \\%L\Profiles\%U
logon drive = H:
logon home = \\%L\%U
domain logons = Yes
os level = 35
preferred master = Yes
domain master = Yes
ldap suffix = dc=example,dc=com
ldap machine suffix = ou=People
ldap user suffix = ou=People
ldap group suffix = ou=Group
ldap idmap suffix = ou=People
ldap admin dn = cn=Manager
ldap ssl = no
```

```
ldap passwd sync = yes
idmap uid = 15000-20000
idmap gid = 15000-20000
...

# Other resource shares
...
...
```

Nota Bene

Per poter implementare un LDAP all'interno del file `smb.conf`, ènecessario installare correttamente un server LDAP funzionante su `ldap.example.com`.

14.3.3.3. Backup Domain Controller (BDC) usando LDAP

BDC rappresenta una parte integrale di qualsiasi soluzione Samba/LDAP. I file `smb.conf` tra PDC e BDC sono virtualmente identici, ad eccezione della direttiva `domain master`. Assicuratevi che PDC abbia il valore `Yes` e che BDC abbia un valore `No`. Se avete BDC multipli per un PDC, la direttiva `os level` risulta essere utile nell'impostazione della priorità di elezione di BDC. Più alto risulta essere il valore, e più alto è la priorità del server per i client che si collegano.

Nota Bene

Un BDC è in grado di utilizzare il database LDAP del PDC, oppure il proprio database LDAP. Questo esempio utilizza il database LDAP del PDC come mostrato dalla direttiva `passdb backend`.

```
[global] workgroup = DOCS
netbios name = DOCS_SRV2
passdb backend = ldapsam:ldap://ldap.example.com
username map = /etc/samba/smbusers
security = user
add user script = /usr/sbin/useradd -m %u
delete user script = /usr/sbin/userdel -r %u
add group script = /usr/sbin/groupadd %g
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/sbin/usermod -G %g %u
add machine script = \
 /usr/sbin/useradd -s /bin/false -d /dev/null \
 -g machines %u
# The following specifies the default logon script
# Per user logon scripts can be specified in the
# user account using pdbedit
logon script = scripts\logon.bat
# This sets the default profile path.
# Set per user paths with pdbedit
logon path = \\%L\Profiles\%U
logon drive = H:
logon home = \\%L\%U
domain logons = Yes
```

```
os level = 35
preferred master = Yes
domain master = No
ldap suffix = dc=example,dc=com
ldap machine suffix = ou=People
ldap user suffix = ou=People
ldap group suffix = ou=Group
ldap idmap suffix = ou=People
ldap admin dn = cn=Manager
ldap ssl = no
ldap passwd sync = yes
idmap uid = 15000-20000
idmap gid = 15000-20000
...

# Other resource shares
...
...
```

14.3.3.4. Primary Domain Controller (PDC) con una Active Directory

Anche se risulta possibile per Samba essere membro di una Active Directory, non risulta possibile operare come un Active Directory domain controller.

14.4. Modalità di sicurezza di Samba

Con Samba sono presenti solo due modalità di sicurezza, *share-level* e *user-level*, i quali sono conosciuti come *livelli di sicurezza*. Share-level security può essere implementato solo in un modo, mentre user-level security è in grado di essere implemantato in quattro diverse modalità. I diversi modi per implementare un livello di sicurezza sono chiamati *security modes*.

14.4.1. User-Level Security

User-level security risulta essere l'impostazione di default di Samba. Anche se la direttiva `security = user` non è elencata nel file `smb.conf`, essa viene usata ugualmente da Samba. Se il server accetta il nome utente/password del client, il client stesso è in grado di montare le condivisioni multiple senza specificare, per ogni esempio, una password. Samba è in grado di accettare delle richieste nome utente/password basate sulla sessione. Per ogni logon, utilizzando un unico UID, il client è in grado di mantenere dei contesti multipli per l'autenticazione.

In `smb.conf`, la direttiva `security = user` che imposta user-level security è:

```
[GLOBAL]
...
security = user
...
```

14.4.2. Share-Level Security

Con lo share-level security, il server accetta solo una password senza un nome utente specifico del client. Il server si aspetta una password per ogni condivisione, indipendente dal nome utente. Sono presenti alcuni rapporti recenti dove i client di Microsoft Windows presentano delle problematiche di compatibilità con i server dello share-level security. Gli sviluppatori di Samba sconsigliano vivamente l'utilizzo di share-level security.

In `smb.conf`, la direttiva `security = share` che imposta lo share-level security è:

```
[GLOBAL]
...
security = share
...
```

14.4.3. Modalità di Sicurezza del Dominio (User-Level Security)

Nella modalità di sicurezza del dominio, il server Samba presenta un account della macchina (domain security trust account) e permette a tutte le richieste di autenticazione, di passare attraverso i controller del dominio. Il server Sambaviene concepito in un domain member server utilizzando la seguente direttiva in `smb.conf`:

```
[GLOBAL]
...
security = domain
workgroup = MARKETING
...
```

14.4.4. Modalità di sicurezza dell'Active Directory (User-Level Security)

Se avete un ambiente Active Directory, è possibile unirsi ad un dominio come un membro nativo dell'Active Directory. Anche se la policy sulla sicurezza limita l'uso di protocolli di autenticazione compatibili con NT, il server Samba è in grado di unirsi ad un ADS utilizzando Kerberos. Samba in Active Directory member mode è in grado di accettare i ticket di Kerberos.

In `smb.conf`, le seguenti direttive rendono Samba un Active Directory member server:

```
[GLOBAL]
...
security = ADS
realm = EXAMPLE.COM
password server = kerberos.example.com
...
```

14.4.5. Modalità di sicurezza del server (User-Level Security)

Il Server security mode è stato utilizzato precedentemente quando Samba non era in grado di comportarsi come un domain member server.

Nota Bene

È vivamente consigliato di *non* utilizzare questa modalità in quanto presenta numerosi svantaggi.

In `smb.conf`, le seguenti direttive abilitano Samba ad operare in server security mode:

```
[GLOBAL]
...
encrypt passwords = Yes
security = server
password server = "NetBIOS_of_Domain_Controller"
...
```

14.5. Database d'informazione sull'account di Samba

L'ultimissima release di Samba offre contenuti nuovi, essi includono nuove password per i database backend, i quali non erano disponibili nelle versioni precedenti. La versione Samba 3.0.0 supporta pienamente tutti i database utilizzati nelle versioni precedenti di Samba. Tuttavia, anche se supportati, molti backend potrebbero non essere idonei per un loro utilizzo nella produzione.

14.5.1. Backend compatibile all'indietro

Testo normale

I backend con un testo normale 'Plain text' non sono altro che tipi di backend `/etc/passwd`. Con un testo normale di tipo backend, tutti i nomi utente e le password vengono inviate, tra il client ed il server Samba, in chiaro. Questo metodo risulta essere molto insicuro e di conseguenza viene deplorato. È possibile che diversi client di Windows che si collegano al server diSamba con password non codificate, non sono in grado di supportare tale metodo.

`smbpasswd`

Un backend molto diffuso utilizzato nei pacchetti Samba precedenti, il backend `smbpasswd`, utilizza una struttura del tipo plain ASCII text che include MS Windows LanMan e NT account, e informazioni password codificate. Il backend `smbpasswd` non presenta lo storage dei controlli estesi di SAM di Windows NT/2000/2003. Il backend `smbpasswd` non è consigliato in quanto non riporta bene o non è in grado di gestire alcuna informazione di Windows, come ad esempio i RID per i gruppi basati su NT. Il backend `tdbsam` risolve queste problematiche per un utilizzo in database più piccoli (250 utenti), ma non rappresenta ancora una soluzione di classe enterprise.

Avviso

Questo tipo di backend potrebbe essere sconsigliato per release future e sostituito dal backend `tdbsam`, il quale include i controlli estesi di SAM.

`ldapsam_compat`

Il backend `ldapsam_compat` permette un supporto continuo di OpenLDAP per un utilizzo di versioni aggiornate di Samba. Questa opzione è l'ideale per eseguire una migrazione, ma non è necessaria. Questo tool verrà eventualmente sconsigliato.

14.5.2. Nuovi Backend

`tdbsam`

Il backend `tdbsam` fornisce un backend del database ideale per server locali, sever che non necessitano di una replica del database interno, e per server che non hanno bisogno di scalabilità o di una complessità di LDAP. Il backend `tdbsam` include tutte le informazioni del database `smbpasswd`, insieme con le informazioni SAM precedentemente escluse. L'inclusione dei dati estesi di SAM permette a Samba di implementare lo stesso account e controlli di accesso al sistema come nei sistemi basati su Windows NT/2000/2003.

Il backend `tdbsam` è consigliato per un massimo di 250 utenti. Organizzazioni più grandi hanno bisogno di una Active Directory o di una integrazione LDAP, a causa della scalabilità e dell'infrastruttura della rete.

`ldapsam`

Il backend `ldapsam` fornisce un metodo distribuito in modo ottimale per l'installazione dell'account di Samba. LDAP è il più idoneo in quanto possiede una certa abilità nella replica del proprio database, ad ogni server che utilizza il demone OpenLDAP `slurpd`. I database LDAP sono scalabili e di media potenza, perfetti per la maggior parte delle organizzazioni, in modo particolare per enterprise molto grandi. LDAP rappresenta il "futuro" per quanto riguarda Samba. Costantemente, vengono implementati su Samba i miglioramenti riguardanti LDAP, in modo da semplificare le problematiche inerenti la configurazione e l'installazione.

`mysqlsam`

Il backend `mysqlsam` utilizza un backend del database basato su MySQL. Questo è utile per i siti che già implementano MySQL.

`xmlsam`

Il backend `xmlsam` utilizza i dati dell'account e della password conservati in un file formattato in XML. Questo metodo risulta essere utile per la migrazione di diversi backend database o per i backup.

14.6. Browsing della rete di Samba

Il browsing della rete è un concetto che permette ai server Samba e di Windows di apparire nelle **Risorse della Rete** di Windows. All'interno delle **Risorse della Rete**, le icone vengono presentate come dei server, e se aperti, le condivisioni e le stampanti del server che sono disponibili, vengono visualizzate.

Le capacità del browsing della rete necessitano di NetBIOS invece di TCP/IP. Il networking basato su NetBIOS utilizza il messaging (UDP) di trasmissione, per ottenere il browse list management. Senza NetBIOS e WINS come metodo primario per la risoluzione dell'hostname TCP/IP, è necessario utilizzare altri metodi come ad esempio file statici (`/etc/hosts`) o DNS.

Un domain master browser è in grado di unire gli elenchi del browse da un local master browser su tutte le sottoreti, in modo tale che si verifichi un browsing tra i workgroup e le sottoreti stesse. Altresì, il domain master browser dovrebbe essere il local master browser per la propria sottorete.

14.6.1. Browsing del Workgroup

Per ogni workgroup ci deve essere uno e solo un domain master browser. Potete avere un local master browser per sottorete senza un domain master browser, ma ciò può risultare in un workgroup isolato. Per risolvere i nomi NetBIOS nei workgroup a reti incrociate, è richiesto l'ausilio di WINS.

Nota Bene

Il Domain Master Browser può essere la stessa macchina del server WINS.

Ci può essere solo un domain master browser per workgroup name. Ecco un esempio del file `smb.conf` nel quale il Samba server rappresenta il domain master browser:

```
[global]
domain master = Yes
local master = Yes
preferred master = Yes
os level = 35
```

Successivamente ecco un esempio del file `smb.conf` nel quale il server Samba server è un local master browser:

```
[global]
domain master = no
local master = Yes
preferred master = Yes
os level = 35
```

La direttiva `os level` opera, in una sottorete, come un sistema di priorità per i master browser. L'impostazione di valori diversi assicura che i master browser non entrino in conflitto.

Suggerimento

Diminuendo la direttiva `os level` ne risulta un conflitto di Samba con altri master browser sulla stessa sottorete. Più elevato è il valore, maggiore è la priorità. Il valore più elevato al quale un server di Windows è in grado di operare è 32. Questo rappresenta il modo migliore per eseguire il tuning di local master browser multipli.

Vi sono alcuni esempi nei quali una macchina NT di Windows presente sulla sottorete, potrebbe essere il local master browser. Ecco riportato un esempio di configurazione `smb.conf`, nel quale il server Samba non esegue alcun servizio nelle capacità di browsing:

```
[global]
domain master = no
local master = no
preferred master = no
os level = 0
```

Avviso

Avere dei local master browser multipli ne può scaturire in una gara tra server per le richieste di elezione per il browsing. Assicuratevi che ci sia solo un local master browser per sottorete.

14.6.2. Browsing del Dominio

Per default, un PDC NT di Windows di un dominio, rappresenta anche il domain master browser del dominio stesso. In questo tipo di situazione un server Samba deve essere impostato come un domain master server. Il browsing della rete potrebbe non riuscire se il server Samba esegue WINS insieme con altri controller del dominio in funzione.

Per le sottoreti che non includono il PDC NT di Windows, un server Samba può essere implementato come un local master browser. La configurazione di `smb.conf` per un local master browser (o senza il browsing) in un ambiente domain controller, è uguale alla configurazione del workgroup.

14.6.3. WINS (Windows Internetworking Name Server)

Sia un server Samba che un server di Windows NT, possono funzionare come un server WINS. Quando si utilizza un server WINS, e NetBIOS è abilitato, gli UDP unicast possono essere direzionati in modo da permettere una risoluzione dei nomi attraverso la rete. Senza un server WINS, la trasmissione UDP è limitata alla sottorete locale, e quindi non può essere direzionata su altre sottoreti, workgroup, o domini. Se è necessario una replica WINS, non utilizzate Samba come server WINS primario, in quanto Samba non supporta attualmente la replica WINS.

In un server NT/2000/2003 misto e in un ambiente Samba, è consigliato utilizzare le capacità WINS di Microsoft. Solo in un ambiente Samba, è consigliato usare *solo un* server Samba per WINS.

Ecco un esempio del file `smb.conf`, nel quale il server Samba si comporta come un server di WINS:

```
[global]
wins support = Yes
```

Suggerimento

Tutti i server (incluso Samba), dovrebbero collegarsi ad un server di WINS per poter risolvere i nomi NetBIOS. Senza WINS, il browsing avviene solo sulla sottorete locale. Inoltre, anche se si ottiene un elenco completo dei domini, gli host non sono risolvibili per il client senza WINS.

14.7. Samba con il supporto di stampa CUPS

Samba permette alle macchine client di condividere le stampanti collegate al server Samba, altresì invia i documenti Linux alle condivisioni della stampante di Windows. Anche se sono disponibili altri sistemi di stampa che funzionano con Red Hat Enterprise Linux, CUPS (Common UNIX Print System) è il sistema di stampa consigliato a causa della sua possibile integrazione con Samba.

14.7.1. Impostazioni semplici di `smb.conf`

Il seguente esempio mostra una configurazione di `smb.conf` basica per un supporto CUPS:

```
[global]
load printers = Yes
printing = cups
printcap name = cups

[printers]
comment = All Printers
```

```
path = /var/spool/samba/print
printer = IBMInfoP
browseable = No
public = Yes
guest ok = Yes
writable = No
printable = Yes
printer admin = @ntadmins

[print$]
comment = Printer Drivers Share
path = /var/lib/samba/drivers
write list = ed, john
printer admin = ed, john
```

È possibile eseguire molte altre configurazioni di stampa più complicate. Per implementare maggiore sicurezza e privacy ai documenti classificati di stampa, gli utenti possono avere il proprio print spooler non posizionato in un percorso pubblico. Se si verifica quindi un errore in un particolare compito, gli altri utenti non avranno la possibilità di accedere al file.

La condivisione `print$` contiene le unità della stampante, le quali possono essere accesse dai client se le stesse non sono disponibili in modo locale. La condivisione `print$` è opzionale e potrebbe non essere necessaria a seconda dell'organizzazione.

Impostando `browseable` su `Yes`, si abilita la stampante da visualizzare nelle risorse di rete di Windows, questo se il server Samba è stato impostato in modo corretto nel dominio/workgroup.

14.8. Programmi di distribuzione di Samba

14.8.1. `findsmb`

`findsmb <`*`subnet_broadcast_address`*`>`

Il programma `findsmb` è uno script Perl il quale riporta le informazioni inerenti i sistemi SMB-aware su di una sottorete specifica. Se non si specifica alcuna sottorete, allora viene usata la sottorete locale. Gli oggetti visualizzati includono l'indirizzo IP, il nome NetBIOS, il workgroup o nome del dominio, il sistema operativo e la versione.

Il seguente esempio mostra l'output di una esecuzione di `findsmb` come qualsiasi utente valido presente sul sistema:

`findsmb`

```
IP ADDR       NETBIOS NAME  WORKGROUP/OS/VERSION
------------------------------------------------------------------------
10.1.59.25    VERVE          [MYGROUP] [Unix] [Samba 3.0.0-15]
10.1.59.26    STATION22      [MYGROUP] [Unix] [Samba 3.0.2-7.FC1]
10.1.56.45    TREK          +[WORKGROUP] [Windows 5.0] [Windows 2000 LAN Manager]
10.1.57.94    PIXEL          [MYGROUP] [Unix] [Samba 3.0.0-15]
10.1.57.137   MOBILE001      [WORKGROUP] [Windows 5.0] [Windows 2000 LAN Manager]
10.1.57.141   JAWS          +[KWIKIMART] [Unix] [Samba 2.2.7a-security-rollup-fix]
10.1.56.159   FRED          +[MYGROUP] [Unix] [Samba 3.0.0-14.3E]
10.1.59.192   LEGION        *[MYGROUP] [Unix] [Samba 2.2.7-security-rollup-fix]
10.1.56.205   NANCYN        +[MYGROUP] [Unix] [Samba 2.2.7a-security-rollup-fix]
```

14.8.2. `make_smbcodepage`

`make_smbcodepage <c|d> <codepage_number> <inputfile> <outputfile>`

Il programma `make_smbcodepage` compila un file codepage binario da una definizione in formato di testo. È vero anche il contrario, e cioè è possibile decompilare un file codepage binario in una definizione in formato di testo. Questo programma piuttosto obsoleto, è parte dei contenuti di internazionalizzazione delle precedenti versioni di Samba incluse per default, con la sua versione corrente.

14.8.3. `make_unicodemap`

`make_unicodemap <codepage_number> <inputfile> <outputfile>`

Il programma `make_unicodemap` è in grado di compilare i file Unicode binari dai file di testo, in modo tale che Samba sia in grado di visualizzare l'insieme di caratteri ASCII. Questo programma piuttosto obsoleto, è parte dei contenuti di internazionalizzazione presenti nelle versioni precedenti di Samba, e contenute ora nella sua release attuale.

14.8.4. `net`

`net <protocol> <function> <misc_options> <target_options>`

La utility `net` è simile alla utility `net`, utilizzata per Windows e MS-DOS. Il primo argomento viene usato per specificare il protocollo da utilizzare quando si esegue un comando. L'opzione `<protocol>` può essere `ads`, `rap`, o `rpc` in modo da specificare il tipo di collegamento server. L'Active Directory utilizza `ads`, Win9x/NT3 utilizza `rap`, e Windows NT4/2000/2003 utilizza `rpc`. Se si omette il protocollo, `net` tenta di determinarlo in modo automatico.

Il seguente esempio mostra un elenco delle condivisioni disponibili per un host chiamato `wakko`:

```
net -l share -S wakko
Password:

Enumerating shared resources (exports) on remote server:


Share name   Type     Description
----------   ----     -----------
data         Disk     Wakko data share
tmp          Disk     Wakko tmp share
IPC$         IPC      IPC Service (Samba Server)
ADMIN$       IPC      IPC Service (Samba Server)
```

Il seguente esempio mostra un elenco di utenti Samba per un host chiamato `wakko`:

```
net -l user -S wakko
root password:

User name             Comment
-----------------------------
andriusb              Documentation
joe                   Marketing
lisa                  Sales
```

14.8.5. nmblookup

`nmblookup <options> <netbios_name>`

Il programma `nmblookup` risolve i nomi NetBIOS in indirizzi IP. Il programma trasmette le proprie richieste alla sottorete locale, fino a quando la macchina interessata non risponde.

Ecco un esempio:

```
nmblookup trek
querying trek on 10.1.59.255
10.1.56.45 trek<00>
```

14.8.6. pdbedit

`pdbedit <options>`

Il programma `pdbedit` è in grado di gestire gli account che si trovano all'interno del database SAM. Tutti i backend sono supportati, incluso `smbpasswd`, LDAP, NIS+, e la libreria del database `tdb`.

Ecco alcuni esempi su come aggiungere, cancellare ed elencare gli utenti:

```
pdbedit -a kristin
new password:
retype new password:
Unix username:        kristin
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-1210235352-3804200048-1474496110-2012
Primary Group SID:    S-1-5-21-1210235352-3804200048-1474496110-2077
Full Name:
Home Directory:       \\wakko\kristin
HomeDir Drive:
Logon Script:
Profile Path:         \\wakko\kristin\profile
Domain:               WAKKO
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 22:14:07 GMT
Kickoff time:         Mon, 18 Jan 2038 22:14:07 GMT
Password last set:    Thu, 29 Jan 2004 08:29:28 GMT
Password can change:  Thu, 29 Jan 2004 08:29:28 GMT
Password must change: Mon, 18 Jan 2038 22:14:07 GMT

pdbedit -v -L kristin
Unix username:        kristin
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-1210235352-3804200048-1474496110-2012
Primary Group SID:    S-1-5-21-1210235352-3804200048-1474496110-2077
Full Name:
Home Directory:       \\wakko\kristin
HomeDir Drive:
Logon Script:
Profile Path:         \\wakko\kristin\profile
Domain:               WAKKO
Account desc:
```

```
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 22:14:07 GMT
Kickoff time:         Mon, 18 Jan 2038 22:14:07 GMT
Password last set:    Thu, 29 Jan 2004 08:29:28 GMT
Password can change:  Thu, 29 Jan 2004 08:29:28 GMT
Password must change: Mon, 18 Jan 2038 22:14:07 GMT
```

```
pdbedit -L
andriusb:505:
joe:503:
lisa:504:
kristin:506:
```

```
pdbedit -x joe
```

```
pdbedit -L
andriusb:505:
lisa:504:
kristin:506:
```

14.8.7. `rpcclient`

`rpcclient` <*server*> <*options*>

Il programma `rpcclient` emette dei comandi amministrativi utilizzando gli RPC di Microsoft, i quali forniscono l'accesso alle graphical user interfaces (GUI) di gestione di Windows per la gestione dei sistemi. Viene utilizzato spesso da utenti esperti, in grado di capire tutta la complessità degli RPC di Microsoft.

14.8.8. `smbcacls`

`smbcacls` <*//server/share*> <*filename*> <*options*>

Il programma `smbcacls` modifica le ACL di Windows sui file e sulle directory condivise dal server Samba.

14.8.9. `smbclient`

`smbclient` <*//server/share*> <*password*> <*options*>

Il programma `smbclient` è un client UNIX molto versatile il quale fornisce una funzionalità simile a `ftp`.

14.8.10. `smbcontrol`

`smbcontrol -i` <*options*>

`smbcontrol` <*options*> <*destination*> <*messagetype*> <*parameters*>

Il programma `smbcontrol` invia messaggi di controllo per l'esecuzione dei demoni `smbd` o `nmbd`. Eseguendo `smbcontrol -i` si eseguono dei comandi in modo interattivo fino a quando non si inserisce una riga vuota o una 'q'.

14.8.11. smbgroupedit

`smbgroupedit <options>`

Il programma `smbgroupedit` esegue una mappatura tra i gruppi di Linux ed i gruppi di Windows. Permette altresì ad un gruppo Linux di essere un gruppo del dominio.

14.8.12. smbmount

`smbmount <//server/share> <mount_point> <-o options>`

Il programma `smbmount` utilizza il programma low-level `smbmnt`, per montare un file system smbfs (condivisione di Samba). Il comando `mount -t smbfs <//server/share> <mount_point> <-o options>` funziona correttamente.

Per esempio:

```
smbmount //wakko/html /mnt/html -o username=kristin
Password: <password>
[root@yakko /]# ls -l /mnt/html
total 0
-rwxr-xr-x    1 root     root            0 Jan 29 08:09 index.html
```

14.8.13. smbpasswd

`smbpasswd <options> <username> <password>`

Il programma `smbpasswd` è in grado di gestire le password cifrate. Questo programma può essere eseguito da un superutente per modificare qualsiasi password, oppure da un utente normale per modificare la propria password Samba.

14.8.14. smbspool

`smbspool <job> <user> <title> <copies> <options> <filename>`

Il programma `smbspool` è una interfaccia di stampa compatibile con CUPS per Samba. Anche se ideato per un utilizzo con le stampanti CUPS, `smbspool` è anche in grado di funzionare con stampanti non-CUPS

14.8.15. smbstatus

`smbstatus <options>`

Il programma `smbstatus` visualizza lo stato dei collegamenti attuali per un server Samba.

14.8.16. smbtar

`smbtar <options>`

Il programma `smbtar` esegue il backup ed il ripristino dei file di condivisione basati su Windows e delle directory, su di un archivio locale a nastro. Anche se simile al comando `tar`, essi non sono compatibili.

14.8.17. `testparm`

`testparm <options> <filename> <hostname IP_address>`

Il programma `testparm` controlla la sintassi del file `smb.conf`. Se il vostro file `smb.conf` si trova in un luogo di default (`/etc/samba/smb.conf`), allora dovete specificarne la posizione. Specificando l'hostname e l'indirizzo IP sul programma `testparm`, si verifica se i file `hosts.allow` e `host.deny` sono stati configurati correttamente. Il programma `testparm` visualizza anche un sommario del file `smb.conf` e del ruolo del server (stand-alone, dominio, ecc.) dopo la prova. Ciò risulta conveniente quando si esegue il debugging, in quanto vengono esclusi i commenti, presentando informazioni utili per gli amministratori più esperti.

Per esempio:

```
testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[tmp]"
Processing section "[html]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
<enter>
# Global parameters
[global]
        workgroup = MYGROUP
        server string = Samba Server
        security = SHARE
        log file = /var/log/samba/%m.log
        max log size = 50
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        dns proxy = No

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[tmp]
        comment = Wakko tmp
        path = /tmp
        guest only = Yes

[html]
        comment = Wakko www
        path = /var/www/html
        force user = andriusb
        force group = users
        read only = No
        guest only = Yes
```

14.8.18. `testprns`

`testprns <printername> <printcapname>`

Il programma `testprns` controlla se `printername` sia valido e presente in `printcap`. Se `printcapname` non viene specificato, allora viene utilizzato il default in Samba o nel file di configurazione `printcap`.

14.8.19. `wbinfo`

`wbinfo <options>`

Il programma `wbinfo` visualizza le informazioni provenienti dal demone `winbindd`. Il demone `winbindd` deve essere in esecuzione per far sì che `wbinfo` funzioni correttamente.

14.9. Risorse aggiuntive

Le seguenti sezioni vi offrono la possibilità di esplorare Samba in modo dettagliato.

14.9.1. Documentazione installata

- `/usr/share/doc/samba-<version-number>/` — Tutti i file aggiuntivi presenti nella distribuzione Samba. Questo include tutti gli script d'aiuto, gli esempi dei file di configurazione e la documentazione.

14.9.2. Documentazione di Red Hat

- *Red Hat Enterprise Linux System Administration Guide*; Red Hat, Inc. — Il capitolo *Samba* spiega come configurare un server Samba.

14.9.3. Libri correlati

- *The Official Samba-3 HOWTO-Collection* di John H. Terpstra and Jelmer R. Vernooij; Prentice Hall — La documentazione ufficiale di Samba 3, ideata dal team di sviluppo di Samba. Rappresenta più un reference guide che una guida passo dopo passo.
- *Samba-3 by Example* by John H. Terpstra; Prentice Hall — Questo rappresenta un'altra release ufficiale del team di sviluppo di Samba, il quale affronta in modo dettagliato gli esempi di OpenLDAP, DNS, DHCP, e dei file di configurazione di stampa. Sono presenti delle informazioni passo dopo passo, in grado di assistervi nelle vostre implementazioni.
- *Using Samba, 2nd Edition* di Jay T's, Robert Eckstein, and David Collier-Brown; O'Reilly — Una buonissima risorsa sia per utenti nuovi che per utenti esperti, sono presenti risorse complete di riferimento.

14.9.4. Siti Web utili

- http://www.samba.org/ — La home page per la distribuzione di Samba e di tutte le documentazioni ufficiali create dal team di sviluppo di Samba. Molte risorse sono disponibili in formati HTML e

PDF, mentre altre sono solo disponibili all'acquisto. Anche se molti di questi link non sono specifici a Red Hat Enterprise Linux, i loro concetti possono essere molto validi.

- http://samba.org/samba/archives.html — Elenchi email attivi per la community di Samba. È consigliato abilitare il digest mode a causa dei livelli elevati nell'attività riguardante l'elenco.
- Newsgroup di Samba — Sono disponibili i newsgroup trattati da Samba, come ad esempio gmane.org, che utilizzano il protocollo NNTP. Ciò rappresenta un'alternativa alla ricezione delle email per la mailing list.
- http://samba.idealx.org/ — Idealx.org distribuisce gli script di configurazione e installazione per l'integrazione di Samba e OpenLDAP. Essi sono fortemente consigliati per l'ausilio alla gestione delle risorse relative a LDAP. Gli script si trovano su `/usr/share/doc/samba-3.0.3/LDAP/smbldap-tools` o possono essere scaricati direttamente dal sito web di Idealx.

Capitolo 15.

FTP

File Transfer Protocol (FTP) è uno dei protocolli più vecchi e usati in Internet. Il suo compito è quello di trasferire i file tra host su di una rete in modo sicuro, senza richiedere all'utente di eseguire un log direttamente nell'host remoto o di sapere come usare il sistema remoto. Esso permette agli utenti di accedere i file su sistemi remoti, usando un insieme di comandi molto semplici.

Questo capitolo riporta le informazioni di base del protocollo FTP, insieme con le opzioni di configurazione per il server FTP primario presente con Red Hat Enterprise Linux, `vsftpd`.

15.1. Il File Transport Protocol

FTP usa un'architettura server client per trasferire i file usando il protocollo di rete TCP. Poichè FTP è un protocollo più vecchio, viene usato un metodo di autenticazione password e nome utente non cifrato. Per questa ragione, viene considerato un protocollo non sicuro, e dovrebbe essere usato solo se necessario. Un sostituto idoneo per FTP è `sftp`, dalla suite OpenSSH dei tool. Per informazioni su come configurare OpenSSH, consultare il capitolo intitolato *OpenSSH* in *Red Hat Enterprise Linux System Administration Guide*. Per informazioni sul protocollo SSH, consultare Capitolo 20.

Tuttavia, poichè FTP è prevalentemente presente su Internet, viene richiesto spesso di condividere alcuni file con il pubblico. Gli amministratori del sistema, dovrebbero essere a conoscenza delle caratteristiche uniche del protocollo FTP.

15.1.1. Porte multiple, Modalità multiple

Diversamente dai protocolli usati su Internet, FTP necessita di porte di rete multiple per funzionare in modo corretto. Quando una applicazione del client FTP inizia un collegamento ad un server FTP, verrà aperta sul server la porta 21 — conosciuta come *porta di comando*. Questa porta viene usata per emettere tutti i comandi al server. Qualsiasi dato richiesto dal server, viene ritornato al client tramite una *porta dati*. Il numero della porta per i collegamenti dei dati e il modo con il quale i suddetti collegamenti vengono inizializzati, varia a seconda se il client richiede i dati in modalità *attiva* o *passiva*.

Di seguito viene riportata la descrizione delle suddette modalità:

modalità attiva

La modalità attiva è il metodo originale usato dal protocollo FTP per il trasferimento dei dati all'applicazione del client. Quando il trasferimento dei dati della modalità attiva viene iniziato dal client FTP, il server apre un collegamento dalla porta 20 sul server per l'indirizzo IP, e una porta non privilegiata randomica (maggiore di 1024) specificata dal client. Questo significa che la macchina del client deve essere abilitata ad accettare i collegamenti attraverso qualsiasi porta al di sopra di 1024. Con la crescita delle reti non sicure, come ad esempio Internet, l'uso dei firewall per proteggere le macchine dei client è molto importante. Poichè questi firewall spesso impediscono i collegamenti in entrata provenienti dai server FTP in modalità attiva, è stato ideata la modalità passiva.

modalità passiva

La modalità passiva, come quella attiva, viene iniziata dall'applicazione client FTP. Quando si richiedono dati al server, il client FTP indica che desidera accedere ai dati in modalità passiva, e il server fornisce l'indirizzo IP e una porta non privilegiata e randomica (maggiore di 1024)

sul server stesso. Il client si collega sulla porta presente sul server, per scaricare le informazioni richieste.

Anche se la modalità passiva risolve le problematiche dovute all'interferenza dei firewall con i dati di collegamento, tale modalità può complicare la gestione dei firewall del server. Limitando la gamma di porte non privilegiate offerte per i collegamenti passivi nel file di configurazione del server FTP, rappresenta un modo per limitare il numero di porte aperte su di un server, e semplifica il compito di creazione delle regole del firewall per il server. Consultare la Sezione 15.5.8 per maggiori informazioni su come limitare le porte passive.

15.2. Sever FTP

Red Hat Enterprise Linux contiene due diversi server FTP:

- **Red Hat Content Accelerator** — Un Web server basato sul Kernel che consente di avere un web server e servizi FTP con elevate prestazioni. Poichè la velocità rappresenta la sua prima caratteristica, esso presenta una funzionalità limitata e viene eseguito solo come server FTP anonimo. Per maggiori informazioni su come configurare e gestire **Red Hat Content Accelerator**, consultare la documentazione disponibile online su http://www.redhat.com/docs/manuals/tux/.
- `vsftpd` — Un demone FTP sicuro e veloce, il quale rappresenta il server FTP preferito per Red Hat Enterprise Linux. Il remainder di questo capitolo si concentra su `vsftpd`.

15.2.1. `vsftpd`

Il Very Secure FTP Daemon (`vsftpd`) è stato creato per essere veloce, stabile e in modo particolare sicuro. La sua abilità di gestire in modo efficiente e sicuro un gran numero di collegamenti, rappresenta il motivo per il quale `vsftpd` è il solo FTP 'stand-alone' distribuito con Red Hat Enterprise Linux.

Il modello di sicurezza usato da `vsftpd` presenta tre aspetti primari:

- *Una separazione sostanziale di processi privilegiati e non* — I suddetti processi gestiscono compiti diversi, e ognuno di questi processi viene eseguito con privilegi minimi necessari per affrontare un compito.
- *I compiti che richiedono privilegi elevati vengono gestiti da processi che richiedono privilegi minimi* — Facendo leva sullecompatibilità presenti nella libreria `libcap`, i compiti che generalmente richiedono i privilegi completi di root, possono essere eseguiti in modo più sicuro da un processo con meno privilegi.
- *La maggior parte dei processi vengono eseguiti in una cella `chroot`* — Quando possibile, variare la directory root dei processi, sulla directory condivisa; la suddetta directory viene così considerata una cella `chroot`. Per esempio, se la directory `/var/ftp/` risulta essere la directory condivisa primaria, `vsftpd` assegna nuovamente `/var/ftp/` alla nuova directory root, conosciuta come `/`. Questa operazione non permette alcuna azione da parte di hacker nei confronti di ogni directory non contenuta sotto la nuova directory root.

L'uso di queste pratiche di sicurezza provoca i seguenti effetti su come `vsftpd` affronta queste richieste:

- *Il processo genitore viene eseguito con il minimo dei privilegi necessari.* — Il processo genitore calcola dinamicamente il livello dei privilegi necessari per minimizzare il livello di rischio. I processi figli gestiscono l'interazione diretta con i client FTP e vengono eseguiti con il numero più basso possibile di privilegi.
- *Tutte le operazioni che richiedono privilegi elevati, vengono gestite da un processo genitore piccolo.* — Similmente al Server HTTP Apache, `vsftpd` lancia i processi figli non privilegiati, in modo da

gestire i collegamenti in entrata. Ciò permette al processo genitore privilegiato, di essere il più piccolo possibile e di gestire un numero più basso di compiti.

- *Tutte le richieste provenienti dai processi figlio non privilegiati, vengono distribuiti dal processo genitore.* — Le comunicazioni con i processi figlio vengono ricevute attraverso un socket, e la validità di una informazione provenienti dai processi figlio, viene controllata prima di essere abilitata.
- *Molte interazioni con i client FTP vengono gestite in una cella `chroot` da processi figlio non privilegiati.* — Poichè questi processi figlio non sono privilegiati e hanno accesso solo alla directory che è stata condivisa, qualsiasi processo interrotto permette all'aggressore un accesso ai file condivisi.

15.3. File installati con `vsftpd`

L'RPM `vsftpd` è in grado d'installare il demone (`/usr/sbin/vsftpd`), la sua configurazione con i file relativi, ed anche le sue directory FTP sul sistema. Il seguente è un elenco di file e directory maggiormente considerati quando si configura `vsftpd`:

- `/etc/rc.d/init.d/vsftpd` — *script d'inizializzazione* (*initscript*) usato dal comando `/sbin/service` per avviare, arrestare o ricaricare `vsftpd`. Consultate la Sezione 15.4 per maggiori informazione sull'uso di questo script.
- `/etc/pam.d/vsftpd` — Il file di configurazione Pluggable Authentication Modules (PAM) per `vsftpd`. Questo file definisce i requisiti che un utente deve rispettare per eseguire un login sul server FTP. Per maggiori informazioni consultate Capitolo 16.
- `/etc/vsftpd/vsftpd.conf` — Il file di configurazione per `vsftpd`. Consultate la Sezione 15.5 per un elenco di opzioni importanti presenti all'interno di questo file.
- `/etc/vsftpd.ftpusers` — Un elenco di utenti non abilitati ad eseguire un log in su `vsftpd`. Per default questo elenco include anche gli utenti `root`, `bin`, e `daemon`.
- `/etc/vsftpd.user_list` — Questo file può essere configurato in modo da permettere o negare l'accesso agli utenti presenti nell'elenco, a seconda se la direttiva `userlist_deny` è impostata in `/etc/vsftpd/vsftpd.conf` su `YES` (default) o `NO`. Se `/etc/vsftpd.user_list` viene usato per garantire l'accesso agli utenti, i nomi degli utenti elencati *non* devono apparire in `/etc/vsftpd.ftpusers`.
- `/var/ftp/` — Tale directory contiene i file serviti da `vsftpd`. Essa contiene inoltre la directory `/var/ftp/pub/` per gli utenti anonimi. Entrambe le directory sono leggibili da tutti, ma possono essere modificate solo dall'utente root.

15.4. Avvio e arresto di `vsftpd`

L'RPM `vsftpd` installa lo script `/etc/rc.d/init.d/vsftpd`, il quale lo si può accedere usando il comando `/sbin/service`.

Per avviare il server come utente root, digitare:

```
/sbin/service vsftpd start
```

Per arrestare il server come utente root, digitare:

```
/sbin/service vsftpd stop
```

L'opzione `restart` rappresenta un modo più semplice per arrestare e riavviare `vsftpd`. Esso rappresenta il modo più efficiente per confermare i cambiamenti apportati alla configurazione, dopo aver modificato il file di configurazione per `vsftpd`.

Per riavviare il server come utente root digitare:

```
/sbin/service vsftpd restart
```

L'opzione `condrestart` (*conditional restart*) avvia solo `vsftpd` se quest'ultimo è in esecuzione. Questa opzione è utile per gli script, in quanto non avvia il demone se lo stesso non è in esecuzione.

Per riavviare il server in modo condizionato come utente root, digitare:

```
/sbin/service vsftpd condrestart
```

Per default, il servizio `vsftpd` *non* si avvia automaticamente al momento dell'avvio. Per configurare il servizio `vsftpd` in modo da avviarsi al momento dell'avvio, usare una utility initscript, come ad esempio `/sbin/chkconfig`, **/sbin/ntsysv**, o il programma **Strumento di configurazione dei servizi**. Consultate il capitolo *Controllo dell'accesso ai servizi* in *Red Hat Enterprise Linux System Administration Guide* per maggiori informazioni su questi tool.

15.4.1. Avvio di copie multiple di `vsftpd`

Talvolta un solo computer viene usato per servire i domini FTP multipli. Questa tecnica viene chiamata *multihoming*. Un modo per eseguire tale tecnica, multihome, usando `vsftpd`, è quello di eseguire delle copie multiple del demone, ognuna delle quali con il proprio file di configurazione.

Per fare questo, assegnare prima tutti gli indirizzi IP pertinenti ai dispositivi della rete o dispositivi alias presenti sul sistema. Consultare il capitolo intitolato *Configurazione della rete* in *Red Hat Enterprise Linux System Administration Guide* per maggiori informazioni sulla configurazione dei dispositivi della rete e dei dispositivi alias. Informazioni aggiuntive sugli script di configurazione della rete, si possono trovare nel Capitolo 8.

Successivamente, il server DNS per i domini FTP deve essere configurato in modo da indicare le macchine corrette. Se il server DNS è in esecuzione su Red Hat Enterprise Linux, consultare il capitolo *Configurazione BIND* in *Red Hat Enterprise Linux System Administration Guide*, per informazioni sull'uso di **Tool di configurazione del servizio del nome del dominio** (`redhat-config-bind`). Per informazioni su BIND e sui file di configurazione, consultare il Capitolo 12.

Per far sì che `vsftpd` risponda alle richieste su diversi indirizzi IP, bisogna eseguire copie multiple del demone. La prima copia deve essere eseguita usando gli initscript `vsftpd`, come riportato nella Sezione 15.4. Questa copia usa il file di configurazione standard, `/etc/vsftpd/vsftpd.conf`.

Ogni sito FTP aggiuntivo deve avere il file di configurazione con un nome unico nella directory `/etc/vsftpd/`, come ad esempio `/etc/vsftpd/vsftpd-site-2.conf`. Ogni file di configurazione deve essere leggibile e scrivibile solo da utenti root. All'interno di ogni file di configurazione per ogni server FTP in ascolto su di una rete IPv4, le seguenti direttive devono essere uniche:

```
listen_address=N.N.N.N
```

Sostituire `N.N.N.N` con l'indirizzo IP *unico* per il sito FTP servito. Se il sito stà usando IPv6, usare invece la direttiva `listen_address6`.

Una volta che ogni server aggiuntivo possiede un file di configurazione, il demone `vsftpd` deve essere lanciato da un prompt della shell root usando il seguente comando:

```
vsftpd /etc/vsftpd/<configuration-file> &
```

Nel comando sopra indicato, sostituire `<configuration-file>` con il nome unico per il file di configurazione del server, come ad esempio `/etc/vsftpd/vsftpd-site-2.conf`.

Altre direttive da alterare in base al server sono:

- `anon_root`
- `local_root`
- `vsftpd_log_file`
- `xferlog_file`

Per un elenco completo delle direttive disponibili all'interno del file di configurazione di `vsftpd`, consultare la Sezione 15.5.

Per configurare qualsiasi server aggiuntivo in modo da avviarsi automaticamente al momento dell'avvio, aggiungere il comando sopra citato alla fine del file `/etc/rc.local`.

15.5. Opzioni di configurazione `vsftpd`

Anche se `vsftpd` potrebbe non offrire un livello di personalizzazione offerto da altri server FTP disponibili, esso offre opzioni sufficienti per far fronte a molte delle esigenze di un amministratore. Per questo motivo gli errori di configurazione e quelli programmatici sono limitati.

Tutta la configurazione di `vsftpd` è gestita dal suo file di configurazione, `/etc/vsftpd/vsftpd.conf`. Ogni direttiva è situata sulla propria riga all'interno del file e segue il formato seguente:

<directive>=*<value>*

Per ogni direttiva, sostituire *<directive>* con una valida direttiva, e *<value>* con un valore accettato.

Importante

Non ci deve essere alcun spazio tra *<directive>*, il simbolo uguale, e *<value>* in una direttiva.

Le righe di commento devono essere precedute dal carattere `#` e sono ignorate dal demone.

Per un elenco completo di tutte le direttive disponibili, consultare la pagina man per `vsftpd.conf`.

Importante

Per una panoramica dei modi su come rendere sicuro `vsftpd`, consultate il capitolo intitolato *Sicurezza del Server* nella *Red Hat Enterprise Linux Security Guide*.

Il seguente è un elenco di alcune delle direttive più importanti all'interno di `/etc/vsftpd/vsftpd.conf`. Tutte le direttive non esplicitamente trovate all'interno del file di configurazione di `vsftpd`, sono impostate nel loro valore di default.

15.5.1. Opzioni del demone

Il seguente è un elenco delle direttive che controllano il comportamento generale del demone `vsftpd`.

- `listen` — Quando abilitata, `vsftpd` viene eseguita in modalità standalone. Red Hat Enterprise Linux imposta questo valore su `YES`. Questa direttiva non può essere usata insieme con la direttiva `listen_ipv6`.

  Il valore di default è `NO`.

- `listen_ipv6` — Quando abilitata, `vsftpd` viene eseguita in modalità standalone, ma è in ascolto sui socket IPv6. Questa direttiva non può essere usata insieme con la direttiva `listen`.

  Il valore di default è `NO`.

- `session_support` — Quando abilitata, `vsftpd` cerca di mantenere le sessioni di login per ogni utente attraverso i Pluggable Authentication Modules (PAM). Consultate Capitolo 16 per maggiori informazioni. Se la sessione di logging non è necessaria, disabilitando questa opzione si permette a `vsftpd` di essere eseguito con meno processi e privilegi.

  Il valore di default è `YES`.

15.5.2. Opzioni di log in e controlli d'accesso

Il seguente è un elenco di direttive le quali controllano il comportamento di login e dei meccanismi di controllo dell'accesso.

- `anonymous_enable` — Quando abilitata, gli utenti anonimi sono abilitati al log in. Il nome utente `anonymous` e `ftp` sono accettati.

  Il valore di default è `YES`.

  Consultare la Sezione 15.5.3 per un elenco di direttive che influenzano gli utenti anonimi.

- `banned_email_file` — Se la direttiva `deny_email_enable` viene impostata su `YES`, la stessa specifica il file contenente un elenco di password email anonime, le quali non hanno un accesso al server.

  Il valore di default è `/etc/vsftpd.banned_emails`.

- `banner_file` — Specifica il file contenente il testo mostrato quando viene stabilito un collegamento con il server. Questa opzione annulla qualsiasi testo specificato nella direttiva `ftpd_banner`.

  Non vi è alcun valore di default per questa direttiva.

- `cmds_allowed` — Specifica un elenco di comandi delimitati da una virgola abilitati dal server. Tutti gli altri comandi vengono rifiutati.

  Non vi è alcun valore di default per questa direttiva.

- `deny_email_enable` — Quando abilitata, qualsiasi utente anonimo che utilizza le password delle email specificate in `/etc/vsftpd.banned_emails` non sarà in grado di accedere al server. Il nome del file di riferimento di questa direttiva può essere specificato usando la direttiva `banned_email_file`.

  Il valore di default è `NO`.

- `ftpd_banner` — Quando abilitata, la stringa specificata all'interno di questa direttiva, viene visualizzata quando viene stabilito un collegamento al server. Questa opzione può essere annullata dalla direttiva `banner_file`.

  Per default `vsftpd` mostra i suoi banner standard.

- `local_enable` — Quando abilitata, gli utenti locali sono abilitati ad eseguire un log in nel sistema.

Il valore di default è `YES`.

Consultare la Sezione 15.5.4 per un elenco di direttive che influenzano gli utenti locali.

- `pam_service_name` — Specifica il nome del servizio PAM per `vsftpd`.

  Il valore di default è `ftp`. Da notare tuttavia che con Red Hat Enterprise Linux il valore è impostato su `vsftpd`.

- `tcp_wrappers` — Quando abilitata, i wrapper TCP vengono usati per garantire l'accesso al server. Inoltre, se il server FTP è configurato con indirizzi IP multipli, l'opzione `VSFTPD_LOAD_CONF` può essere usata per caricare i diversi file di configurazione basati su indirizzi IP richiesti dal client. Per maggiori informazioni sui Wrapper TCP, consultate Capitolo 17.

  Il valore di default è `NO`. Da notare tuttavia che con Red Hat Enterprise Linux il valore è impostato su `YES`.

- `userlist_deny` — Quando usato insieme con la direttiva `userlist_enable` e impostato su `NO`, tutti gli utenti locali sono impossibilitati ad eseguire un accesso, a meno che il nome utente non sia presente nel file specificato dalla direttiva `userlist_file`. Poichè l'accesso viene negato prima di richiedere la password al client, impostando questa direttiva su `NO`, impedisce agli utenti locali di richiedere una password in modo non cifrato attraverso la rete.

  Il valore di default è `YES`.

- `userlist_enable` — Quando abilitata, gli utenti presenti nel file specificato dalla direttiva `userlist_file`, non possono eseguire l'accesso. Poichè l'accesso viene negato prima di richiedere la password al client, gli utenti non hanno la necessità di richiedere delle password non cifrate attraverso la rete.

  Il valore di default è `NO`, tuttavia con Red Hat Enterprise Linux il valore è impostato su `YES`.

- `userlist_file` — Specifica il file indicato da `vsftpd`, quando è abilitata la direttiva `userlist_enable`.

  Il valore di default è `/etc/vsftpd.user_list` ed è creato durante l'installazione.

- `cmds_allowed` — Specifica un elenco, separato da una virgola, di comandi FTP abilitati dal server. Qualsiasi altro comando viene rifiutato.

  Non vi è alcun valore di default per questa direttiva.

15.5.3. Opzioni per l'utente anonimo

Il seguente è un elenco di direttive le quali controllano l'accesso al server degli utenti anonimi. Per usare queste opzioni, la direttiva `anonymous_enable` deve essere impostata su `YES`.

- `anon_mkdir_write_enable` — Quando abilitata insieme con la direttiva `write_enable`, gli utenti anonimi sono in grado di creare nuove directory all'interno di una directory genitore, la quale possiede i permessi di scrittura.

  Il valore di default è `NO`.

- `anon_root` — Specifica i cambiamenti della directory `vsftpd`, dopo che un utente anonimo ha eseguito il log in.

  Non vi è alcun valore di default per questa direttiva.

- `anon_upload_enable` — Quando abilitata insieme con la direttiva `write_enable`, gli utenti anonimi sono abilitati ad eseguire un upload di file all'interno della directory genitore la quale possiede i permessi di scrittura.

  Il valore di default è `NO`.

- `anon_world_readable_only` — Quando abilitata, gli utenti anonimi possono solo scaricare i file letti da tutti 'world-readable'.

  Il valore di default è `YES`.

- `ftp_username` — Specifica l'account dell'utente locale (riportato in `/etc/passwd`), usato per un utente FTP anonimo. La home directory specificata in `/etc/passwd` per l'utente, è la directory root dell'utente FTPanonimo.

  Il valore di default è `ftp`.

- `no_anon_password` — Quando abilitata, non viene richiesta alcuna password all'utente anonimo.

  Il valore di default è `NO`.

- `secure_email_list_enable` — Quando abilitata, viene accettato solo un elenco specificato di email password per login anonimi. Ciò rappresenta un modo molto conveniente di offrire una sicurezza limitata per contenuti resi pubblici senza la necessità di utenti virtuali.

  I login anonimi vengono evitati a meno che la password risulta essere presente nell'elenco `/etc/vsftpd.email_passwords`. Il formato del file è di una password per riga, senza alcuno spazio.

  Il valore di default è `NO`.

15.5.4. Opzioni dell'utente locale

Il seguente è un elenco di direttive che caratterizzano il modo di accesso al server dell'utente locale. Per usare queste opzioni, la direttiva `local_enable` deve essere impostata su `YES`.

- `chmod_enable` — Quando abilitata, il comando FTP `SITE CHMOD` viene abilitato per gli utenti locali. Questo comando permette agli utenti locali di cambiare i permessi presenti sui file.

  Il valore di default è `YES`.

- `chroot_list_enable` — Quando abilitata, gli utenti locali presenti nel file specificato nella direttiva `chroot_list_file`, vengono posizionati in una cella `chroot` previo log in.

  Se abilitata con la direttiva `chroot_local_user`, gli utenti locali elencati nel file specificato nella direttiva `chroot_list_file`, *non* vengono posizionati in una cella `chroot` dopo il log in.

  Il valore di default è `NO`.

- `chroot_list_file` — Specifica il file contenente un elenco di utenti locali indicati quando la direttiva `chroot_list_enable` è impostata su `YES`.

  Il valore di default è `/etc/vsftpd.chroot_list`.

- `chroot_local_user` — Quando abilitata, la directory root verrà cambiata, dopo aver eseguito il log in, nella home directory degli utenti locali.

  Il valore di default è `NO`.

  
  Avvertimento

  Abilitando `chroot_local_user` si và incontro a diverse problematiche riguardanti la sicurezza, in special modo per utenti che possiedono dei privilegi di upload. Per questo motivo tale configurazione *non* è consigliata.

- `guest_enable` — Quando abilitata, tutti gli utenti che non sono anonimi, vengono registrati come utenti `guest`, i quali rappresentano gli utenti locali specificati nella direttiva `guest_username`.

  Il valore di default è `NO`.

- `guest_username` — Specifica il nome utente sul quale viene mappato l'utente `guest`.

Il valore di default è `ftp`.

- `local_root` — Specifica il cambiamento della directory di `vsftpd` dopo che l'utente locale ha eseguito il log in.

  Non vi è alcun valore di default per questa direttiva.

- `local_umask` — Specifica il valore di umask per la creazione di un file. Da notare che il valore di default viene espresso con un numero ottale 'octal mode' (un sistema numerico basato su otto cifre), il quale include un prefisso "0". In caso contrario il valore viene considerato come un numero intero con base decimale.

  Il valore di default è `022`.

- `passwd_chroot_enable` — Quando abilitata insieme con la direttiva `chroot_local_user`, viene modificata la directory root `vsftpd` degli utenti locali in base all'evento della `/./` nel campo della home directory all'interno di `/etc/passwd`.

  Il valore di default è `NO`.

- `user_config_dir` — Specifica il percorso per una directory contenente i file di configurazione che presentano il nome degli utenti locali del sistema, il quale contiene a sua volta le impostazioni specifiche per quell'utente. Qualsiasi direttiva nel file di configurazione dell'utente, annulla quelle trovate in `/etc/vsftpd/vsftpd.conf`.

  Non vi è alcun valore di default per questa direttiva.

15.5.5. Opzioni della directory

Il seguente è un elenco di direttive che influenzano le directory.

- `dirlist_enable` — Quando abilitata, gli utenti possono visualizzare gli elenchi della directory.

  Il valore di default è `YES`.

- `dirmessage_enable` — Quando abilitata, viene visualizzato un messaggio ogni qualvolta un utente inserisce una directory con un file di messaggio. Questo messaggio si trova all'interno della directory che è stata inserita. Il nome di questo file è specificato nella direttiva `message_file` ed è `.message` per default.

  Il valore di default è `NO`. Da notare tuttavia che con Red Hat Enterprise Linux il valore è impostato su `YES`.

- `force_dot_files` — Quando abilitata, i file che iniziano con un punto (`.`), vengono elencati negli elenchi delle directory, con l'accezione dei file `.` and `..`

  Il valore di default è `NO`.

- `hide_ids` — Quando abilitata, tutti gli elenchi delle directory mostrano `ftp` come l'utente e il gruppo per ogni file.

  Il valore di default è `NO`.

- `message_file` — Specifica il nome del file di messaggio quando si usa la direttiva `dirmessage_enable`.

  Il valore di default è `.message`.

- `text_userdb_names` — Quando abilitata, vengono usati i nomi dell'utente e dei gruppi in formato di test, al posto delle voci UID e GID. Abilitando questa opzione potrebbe rallentare le prestazioni del server.

  Il valore di default è `NO`.

- `use_localtime` — Quando abilitata, gli elenchi della directory rivelano l'orario locale per il computer invece dell'orario GMT.

Il valore di default è NO.

15.5.6. Opzioni di trasferimento del file

Il seguente è un elenco di direttive che influenzano le directory.

- download_enable — Quando abilitata, è possibile scaricare i file.

  Il valore di default è YES.

- chown_uploads — Quando abilitata, tutti i file caricati dagli utenti anonimi, sono posseduti dall'utente specificato nella direttiva chown_username.

  Il valore di default è NO.

- chown_username — Specifica il proprietario dei file caricati anonimamente, se si abilita la direttiva chown_uploads.

  Il valore di default è root.

- write_enable — Quando abilitata, sono abilitati i comandi FTP che possono modificare il file system, come ad esempio DELE, RNFR, e STOR.

  Il valore di default è YES.

15.5.7. Opzioni di Logging

Il seguente è un elenco di direttive che influenzano il comportamento di vsftpd durante un logging.

- dual_log_enable — Quando abilitata insieme con xferlog_enable, vsftpd registra contemporaneamente due file: un log wu-ftpd-compatibile per il file specificato nella direttiva xferlog_file (/var/log/xferlog per default) e un file log standard vsftpd specificato nella direttiva vsftpd_log_file (/var/log/vsftpd.log per default).

  Il valore di default è NO.

- log_ftp_protocol — Quando abilitato insieme con xferlog_enable e con xferlog_std_format impostato su NO, vengono registrati tutti i comandi FTP e le risposte. Questa direttiva è utile per il debugging.

  Il valore di default è NO.

- syslog_enable — Quando abilitata insieme con xferlog_enable, tutti i logging registrati normalmente sul file log vsftpd standard specificato nella direttiva vsftpd_log_file (/var/log/vsftpd.log per default), vengono inviati al sistema che li registra invece della facility FTPD.

  Il valore di default è NO.

- vsftpd_log_file — Specifica il file log vsftpd. Per usare questo file, xferlog_enable deve essere abilitato e xferlog_std_format deve essere impostato su NO o, se si imposta xferlog_std_format su YES, dual_log_enable deve essere abilitato. È importante notare che se syslog_enable è impostato su YES, viene usato il sistema di log, invece del file specificato in questa direttiva.

  Il valore di default è /var/log/vsftpd.log.

- xferlog_enable — Quando abilitata, vsftpd registra i collegamenti (solo in formato vsftpd) e le informazioni di trasferimento del file sul file log specificato nella direttiva vsftpd_log_file (per default /var/log/vsftpd.log). Se xferlog_std_format è impostato su YES, vengono registrate solo le informazioni sul trasferimento del file e non i collegamenti, e viene usato il file

log specificato in `xferlog_file` (`/var/log/xferlog` per default). È importante notare che entrambi i file log ed i formati log vengono usati se `dual_log_enable` è impostato su `YES`.

Il valore di default è `NO`. Da notare tuttavia che con Red Hat Enterprise Linux il valore è impostato su `YES`.

- `xferlog_file` — Specifica il file log `wu-ftpd`-compatibile. Per usare questo file, bisogna abilitare `xferlog_enable`, e `xferlog_std_format` deve essere impostato su `YES`. Esso viene anche usato se `dual_log_enable` è impostato su `YES`.

  Il valore di default è `/var/log/xferlog`.

- `xferlog_std_format` — Quando abilitata insieme con `xferlog_enable`, viene registrato, sul file specificato nella direttiva `xferlog_file`, solo un log di tresferimento del file `wu-ftpd`-compatibile (`/var/log/xferlog` per default). È importante notare che questo file registra solo i trasferimenti del file e non registra i collegamenti al server.

  Il valore di default è `NO`. Da notare tuttavia che con Red Hat Enterprise Linux il valore è impostato su `YES`.

Importante

Per mantenere una compatibilità con i file log scritti dal server FTP `wu-ftpd` più vecchi, la direttiva `xferlog_std_format` è impostata su `YES` con Red Hat Enterprise Linux. Tuttavia, questa impostazione significa che i collegamenti al server non sono registrati.

Per eseguire un log dei collegamenti in formato `vsftpd` e gestire un log di trasferimento del file `wu-ftpd`-compatibile, impostare `dual_log_enable` su `YES`.

Se non è importante mantenere un log di trasferimento del file `wu-ftpd`-compatibile, impostare `xferlog_std_format` su `NO`, e commentare la riga con un carattere `#`, oppure cancellare l'intera riga.

15.5.8. Opzioni della rete

Il seguente è un elenco di direttive che influenzano il modo con il quale `vsftpd` interagisce con la rete.

- `accept_timeout` — Specifica la quantità di tempo per un client, nell'uso della modalità passiva, per stabilire un collegamento.

  Il valore di default è `60`.

- `anon_max_rate` — Specifica la velocità massima di trasferimento dei dati per gli utenti anonimi in byte al secondo.

  Il valore di default è `0`, il quale non limita la velocità di trasferimento.

- `connect_from_port_20` Quando abilitata, `vsftpd` viene eseguita con privilegi sufficienti per aprire la porta 20 sul server, durante i trasferimenti dei dati in modalità attiva. Disabilitare questa opzione permette a `vsftpd` di essere eseguito con meno privilegi, ma potrebbe essere non compatibile con alcuni client FTP.

  Il valore di default è `NO`. Da notare tuttavia che con Red Hat Enterprise Linux il valore è impostato su `YES`.

- `connect_timeout` — Specifica il tempo massimo, in secondi, al quale un client che usa una modalità attiva, deve rispondere per un collegamento dei dati.

  Il valore di default è `60`.

- `data_connection_timeout` — Specifica il tempo massimo, in secondi, all'interno del quale il trasferimento dei dati può arrestarsi. Una volta azionato, il collegamento al client remoto viene chiuso.

  Il valore di default è `300`.

- `ftp_data_port` — Specifica la porta usata per i collegamenti attivi dei dati quando `connect_from_port_20` è impostato su `YES`.

  Il valore di default è `20`.

- `idle_session_timeout` — Specifica il tempo massimo che intercorre tra due comandi da un client remoto. Una volta azionato, il collegamento al client remoto viene chiuso.

  Il valore di default è `300`.

- `listen_address` — Specifica l'indirizzo IP sul quale `vsftpd` è in ascolto per i collegamenti di rete.

  Non vi è alcun valore di default per questa direttiva.

  

  Suggerimento

  Se si eseguono copie multiple di `vsftpd` e si servono indirizzi IP diversi, il file di configurazione per ogni copia del demone `vsftpd`, deve avere un valore diverso per questa direttiva. Consultare la Sezione 15.4.1 per maggiori informazioni sui server FTP 'multihomed'.

- `listen_address6` — Specifica l'indirizzo IPv6 sul quale `vsftpd` è in ascolto per i collegamenti di rete, quando `listen_ipv6` è impostato su `YES`.

  Non vi è alcun valore di default per questa direttiva.

  

  Suggerimento

  Se si eseguono copie multiple di `vsftpd` e si servono indirizzi IP diversi, il file di configurazione per ogni copia del demone `vsftpd`, deve avere un valore diverso per questa direttiva. Consultare la Sezione 15.4.1 per maggiori informazioni sui server FTP 'multihomed'.

- `listen_port` — Specifica la porta sulla quale `vsftpd` è in ascolto per i collegamenti di rete.

  Il valore di default è `21`.

- `local_max_rate` — Specifica la velocità massima di trasferimento dei dati, in byte al secondo, per utenti locali registrati nel server.

  Il valore di default è `0`, il quale non limita la velocità di trasferimento.

- `max_clients` — Specifica il numero massimo di client simultanei che si possono collegare al server, quando lo stesso è in esecuzione in modalità 'standalone'. Qualsiasi altro collegamento client aggiuntivo causerà la generazione di un messaggio di errore.

  Il valore di default è `0`, il quale non limita i collegamenti.

- `max_per_ip` — Specifica il numero massimo di client che si possono collegare dallo stesso indirizzo IP della sorgente.

  Il valore di default è `0`, il quale non limita i collegamenti.

- `pasv_address` — Specifica l'indirizzo IP per l'indirizzo IP 'public facing' del server, per i server situati dietro i firewall Network Address Translation (NAT). Ciò abilita `vsftpd` a fornire l'indirizzo di ritorno corretto per i collegamenti in modalità passiva.

  Non vi è alcun valore di default per questa direttiva.

- `pasv_enable` — Quando abilitata, sono permessi i collegamenti in modalità passiva.

  Il valore di default è `YES`.

- `pasv_max_port` — Specifica la porta più alta inviata ai client FTP per i collegamenti in modalità passiva. Questa impostazione viene usata per limitare la gamma della porta, in modo da semplificare la creazione delle regole del firewall.

  Il valore di default è `0`, il quale non limita la gamma della porta passiva più alta. Il valore non deve eccedere `65535`.

- `pasv_min_port` — Specifica la porta più bassa inviata ai client FTP per i collegamenti in modalità passiva. Questa impostazione viene usata per limitare la gamma della porta, in modo da semplificare la creazione delle regole del firewall.

  Il valore di default è `0`, il quale non limita la gamma della porta passiva più bassa. Il valore non deve essere minore di `1024`.

- `pasv_promiscuous` — Quando abilitata, i collegamenti dei dati non vengono controllati in modo da assicurare che gli stessi siano originati dallo stesso indirizzo IP. Questa impostazione è utile solo per alcuni tipi di tunneling.

  

  Attenzione

  Non abilitate questa opzione se non è necessario, in quanto essa disabilita un contenuto di sicurezza molto importante, il quale verifica che i collegamenti in modalità passiva siano originati dallo stesso indirizzo IP del collegamento di controllo che inizia il trasferimento dei dati.

  Il valore di default è `NO`.

- `port_enable` — Quando abilitata, sono permessi i collegamenti in modalità attiva.

  Il valore di default è `YES`.

15.6. Risorse aggiuntive

Per maggiori informazioni su `vsftpd`, consultate le seguenti risorse.

15.6.1. Documentazione installata

- Directory `/usr/share/doc/vsftpd-<version-number>/` — Sostituire `<version-number>` con la versione installata del pacchetto `vsftpd`. Questa directory contiene un file `README` con informazioni di base sul software. Il file `TUNING` contiene alcuni suggerimenti sulla regolazione della prestazione di base e la directory `SECURITY/` la quale contiene le informazioni sul modello di sicurezza impiegato da `vsftpd`.
- Pagine man relative a `vsftpd` — Sono disponibili un certo numero di pagine man per il demone ed i file di configurazione. Il seguente è un elenco di alcune delle più importanti pagine man.

  Applicazioni del server

  - `man vsftpd` — Descrive le opzioni della linea di comando disponibili per `vsftpd`.

File di configurazione

- `man vsftpd.conf` — Contiene un elenco dettagliato di opzioni disponibili all'interno del file di configurazione per `vsftpd`.
- `man 5 hosts_access` — Descrive il formato e le opzioni disponibili all'interno dei file di configurazione dei wrapper TCP: `hosts.allow` e `hosts.deny`.

15.6.2. Siti web utili

- http://vsftpd.beasts.org/ — La pagina del progetto `vsftpd` è molto utile per trovare la documentazione più recente e per contattare l'autore del software.
- http://slacksite.com/other/ftp.html — Questo sito web fornisce una breve spiegazione delle differenze tra un FTP in modalità attiva e passiva.
- http://war.jgaa.com/ftp/?cmd=rfc — Un elenco completo di *Request for Comments* (*RFC*) 'Richiesta di commenti', relativi al protocollo FTP.

15.6.3. Libri correlati

- *Red Hat Enterprise Linux Security Guide*; Red Hat, Inc. — Il capitolo *Sicurezza del server* spiega i modi per rendere sicuro `vsftpd` e gli altri servizi.

III. Riferimento alla sicurezza

Usare protocolli sicuri rappresenta una parte fondamentale sulla gestione dell'integrità del sistema. Questa parte descrive i tool più importanti per l'autenticazione dell'utente, per il controllo dell'accesso alla rete, per avere delle comunicazioni di rete sicure. Per maggiori informazioni su come rendere sicuro un sistema Red Hat Enterprise Linux, consultate *Red Hat Enterprise Linux Security Guide*.

Sommario

16. Moduli di autenticazione PAM 267
17. Wrapper TCP e `xinetd` 277
18. `iptables` 293
19. Kerberos 307
20. Protocollo SSH 317
21. SELinux 325

Capitolo 16.

Moduli di autenticazione PAM

Il processo che consente l'accesso di un utente ad un sistema, previa verifica dell'identitá, viene chiamato *autenticazione*. Generalmente, ogni programma è in possesso di un proprio modo di autenticazione. Con Red Hat Enterprise Linux, vi é un unico programma che centralizza i programmi d'identificazione usati in passato, questo programma viene chiamato *Pluggable Authentication Modules* (*PAM*).

Le caratteristiche di PAM, permettono all'amministratore del sistema di possedere una buona flessibilitá nell'impostazione delle policy di autenticazione per il sistema stesso.

Nella maggior parte dei casi, il file di configurazione PAM per una applicazione che la riconosce, é sufficiente. Tuttavia, talvolta puó essere necessario modificare tale file di configurazione. A causa di ció, si potrebbe compromettere la sicurezza del sistema, é importante quindi conoscere la struttura del file (vedere la Sezione 16.2 per maggiori informazioni).

16.1. I vantaggi dei PAM

PAM offre i seguenti vantaggi:

- Fornisce uno schema di autenticazione comune che può essere usato con diverse applicazioni.
- Consente di avere una grande flessibilità e controllo tramite l'autenticazione, sia per gli amministratori del sistema che per gli sviluppatori dell'applicazione.
- Permette agli sviluppatori dell'applicazione di sviluppare programmi senza creare il proprio schema di autenticazione.

16.2. File di configurazione PAM

La directory `/etc/pam.d/` contiene i file di configurazione PAM per ogni applicazione supportata. Nelle versioni precedenti di PAM veniva usato il file `/etc/pam.conf`, ma ora il suo utilizzo è sconsigliato, e viene usato solo se la directory `/etc/pam.d/` non è esistente.

16.2.1. File di servizio PAM

Ogni applicazione o *service* che supporta PAM possiede un file all'interno della directory `/etc/pam.d/`. Ogni file all'interno di questa directory, viene nominato dopo il servizio per il quale controlla l'accesso.

Spetta al programma che supporta PAM definire il nome del servizio e installare il relativo file di configurazione PAM nella directory `/etc/pam.d`. Per esempio, il programma `login` definisce il proprionome del servizio come login e installa in file di configurazione PAM `/etc/pam.d/login`.

16.3. Formato del file di configurazione PAM

Ogni file di configurazione PAM contiene un gruppo di direttive formattate come segue:

<module interface> *<control flag>* *<module name>* *<module arguments>*

Ciascuno di questi elementi è spiegato nelle sezioni successive.

16.3.1. Interfaccia del modulo

Esistono quattro tipi di interfacce di moduli PAM che permettono di controllare l'accesso a determinati servizi e sono correlati ad aspetti diversi del processo di autorizzazione:

- `auth` — Questa interfaccia del modulo autentica l'uso. Per esempio, esso richiede e verifica la validità di una password. I moduli con questa interfaccia possono anche impostare delle credenziali come l'appartenenza al gruppo o i ticket di Kerberos.
- `account` — Questo modulo esegue un controllo per verificare che l'accesso sia abilitato. Per esempio, controlla se un account è scaduto o se l'utente ha il permesso di collegarsi ad una determinata ora del giorno.
- `password` — Questa interfaccia imposta e verifica le password.
- `session` — Questa interfaccia configura e gestisce le sessioni dell'utente. I moduli con questa interfaccia, possono effettuare ulteriori compiti richiesti per autorizzare l'accesso, per esempio montando la home directory dell'utente o rendendo disponibile la sua mailbox.

Nota Bene

Un singolo modulo può fornire una o tutte le interfacce del modulo.Per esempio `pam_unix.so` fornisce tutti e quattro le interfacce del modulo.

In un file di configurazione PAM l'interfaccia del modulo è il primo aspetto definito. Per esempio una riga tipica di configurazione potrebbe essere:

```
auth      required  pam_unix.so
```

Ciò indica a PAM di utilizzare l'interfaccia `auth` del modulo `pam_unix.so`.

16.3.1.1. Stacking delle interfacce del modulo

Le direttive dell'interfaccia del modulo possono essere*conservate* o messe l'una sull'altra, in modo tale che moduli multipli possano essere utilizzati insieme per un unico scopo. L'ordine con cui vengono elencati i moduli è molto importante per il processo di autenticazione.

Tale operazione rende più facile per l'amministratore richiedere la verifica di determinate condizioni prima di autenticare l'utente. Per esempio, `rlogin` utilizza normalmente almeno cinque moduli `auth`, come lo dimostra il suo file di configurazione PAM:

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

Prima che qualcuno possa usare `rlogin`, PAM controlla che non esista alcun file `/etc/nologin`, verifica se si stia provando ad effettuare un collegamento remoto come utente root attraverso una connessione di rete,e se vi sia la possibilità di caricare tutte le variabili d'ambiente. Quindi, se viene eseguita con successo un'autenticazione `rhosts`, il collegamento viene abilitato. Se l'autenticazione `rhosts` non va a buon fine, viene effettuata un'autenticazione standard della password.

16.3.2. Control Flag

Quando vengono controllati, tutti i moduli PAM generano un risultato positivo o negativo. I Control flag indicano a PAM cosa fare con il risultato. Poiché i moduli possono essere ordinati in determinati modi, i control flag permettono di stabilire l'importanza di un risultato positivo o negativo di un particolare modulo per l'autenticazione dell'utente al servizio.

Ci sono quattro control flag predefinite:

- `required` — Il modulo deve superare il controllo perché l'autenticazione sia autorizzata. Se il controllo di un modulo `required` fallisce, l'utente non ne viene avvisato finché tutti gli altri moduli dello stesso tipo non sono stati controllati.
- `requisite` — il modulo deve superare la verifica perché l'autenticazione vada a buon fine. Tuttavia, se la verifica di un modulo `requisite` fallisce, l'utente ne viene immediatamente avvisato tramite un messaggio che richiama il primo modulo `required` *o* `requisite`.
- `sufficient` — Il risultato del modulo viene ignorato se fallisce. Tuttavia, se il risultato del modulo con opzione `sufficient` supera la verifica *e* nessun modulo con opzione `required` che lo precedono abbia fallito, non viene richiesto nessun altro risultato e l'utente viene autenticato.
- `optional` — Il risultato del modulo viene ignorato.L'unico caso in cui un modulo con opzione `optional` è necessario ai fini dell'autenticazione è quando non ci sono altri moduli che si riferiscono all'interfaccia.

Importante

L'ordine con il quale i moduli `required` sono chiamati non é importante. I control flag `sufficient` e `requisite` invece, conferiscono una certa importanza all'ordine.

Adesso è disponibile una nuova sintassi di controllo ancora più efficace per PAM. Per maggiori informazioni, consultate la documentazione su PAM contenuta nella directory `/usr/share/doc/pam-`*`numero-versione`*`/` (dove *`numero-versione`* é il numero della versione per PAM).

16.3.3. Nome del modulo

Il nome del modulo fornisce a PAM il nome del modulo 'pluggable' contenente l'interfaccia del modulo specificato. Con le vecchie versioni di Red Hat Enterprise Linux, il percorso intero per il modulo veniva fornito all'interno del file di configurazione di PAM, come ad esempio `/lib/security/pam_stack.so`. Tuttavia con l'avvento di sistemi con librerie multiple, i quali possono conservare moduli PAM a 64-bit all'interno della directory `/lib64/security/`, il nome della directory viene omesso perchè le applicazioni sono collegate alla versione appropriata di `libpam`, la quale può trovare la versione corretta del modulo.

16.3.4. Argomenti del modulo

PAM utilizza degli argomenti per fornire informazioni a un modulo pluggable durante il processo di autenticazione di un determinato tipo di modulo.

Per esempio il modulo `pam_userdb.so` utilizza file nascosti del Berkeley DB per autenticare l'utente. Il Berkeley DB è un database Open Source concepito per essere incorporato in varie applicazioni. Il modulo prende un argomento `db` specificando il file Berkeley DB da usare, che può variare in funzione del servizio.

Pertanto la riga `pam_userdb.so` di un file di configurazione PAM è:

```
auth      required  pam_userdb.so db=<path-to-file>
```

Nell'esempio precedente, sostituire *<percorso-per-file>* con il percorso completo per il file del database Berkeley DB.

Gli argomenti non validi vengono ignorati e non influenzano il successo né il fallimento del modulo PAM. Tuttavia, molti moduli riporteranno un errore sul file `/var/log/messages`.

16.4. Esempi di file di configurazione PAM

Di seguito è riportato un esempio del file di configurazione PAM:

```
#%PAM-1.0
auth      required  pam_securetty.so
auth      required  pam_unix.so shadow nullok
auth      required  pam_nologin.so
account   required  pam_unix.so
password  required  pam_cracklib.so retry=3
password  required  pam_unix.so shadow nullok use_authtok
session   required  pam_unix.so
```

La prima riga è un commento, come indicato dal carattere `#` all'inizio della stessa.

Le righe da due a quattro contengono tre moduli da usare per l'autenticazione del login.

```
auth      required  pam_securetty.so
```

Questa riga assicura che *se* l'utente prova a collegarsi come root, la tty in uso sia elencata nel file `/etc/securetty`, *se* tale file esiste.

```
auth      required  pam_unix.so shadow nullok
```

Questo modulo richiede all'utente una password, che poi verifica usando le informazioni conservate in `/etc/passwd` e, se esiste, `/etc/shadow`. Il modulo `pam_unix.so` rileva e utilizza automaticamente le password shadow per autenticare gli utenti. Consultate la Sezione 6.5 per maggiori informazioni.

L'argomento `nullok` specifica al modulo `pam_unix.so` di accettare una password vuota.

```
auth      required  pam_nologin.so
```

Questa è la fase finale di autenticazione. Con la suddetta fase si controlla l'esistenza del file `/etc/nologin`. Se `nologin` esiste e l'utente non è root, l'autenticazione non ha successo.

Nota Bene

In questo esempio, tutti e tre i moduli `auth` vengono controllati, anche se il primo modulo `auth` non supera la verifica. Questa strategia impedisce all'utente di sapere perché l'autenticazione non è permessa. Se conoscesse il motivo, l'utente riuscirebbe a capire come irrompere nel sistema.

```
account   required  pam_unix.so
```

Questo modulo effettua qualsiasi verifica necessaria dell'account. Per esempio se le password shadow sono state abilitate, la componente dell'account del modulo `pam_unix.so` verifica se l'account è scaduto o se l'utente non ha modificato la password nel periodo stabilito.

```
password  required  pam_cracklib.so retry=3
```

Se la password è scaduta, il componente del modulo `pam_cracklib.so` ne richiede una nuova. Quindi verifica la nuova password per vedere se può essere facilmente indovinata da un programma che ricostruisce le password. Se la verifica non va a buon fine, offre all'utente altre due possibilità per creare una password meno facile, in base all'argomento `retry=3`.

```
password  required  pam_unix.so shadow nullok use_authtok
```

Questa riga specifica che se il programma modifica la password dell'utente, dovrebbe utilizzare il componente `password` del modulo `pam_unix.so` per farlo. Succede solo se la porzione `auth` del modulo `pam_unix.so` ha stabilito che la password deve essere cambiata — per esempio se una password shadow è scaduta.

L'argomento `shadow` specifica al modulo di creare password shadow durante l'aggiornamento della password dell'utente.

L'argomento `nullok` specifica al modulo di consentire all'utente di modificare la password *da* una password vuota, altrimenti questa viene considerata come un blocco dell'account.

L'argomento finale di questa riga, `use_authtok`, fornisce un buon esempio sull'importanza dell'ordine quando si mettono insieme i moduli PAM. Questo argomento specifica al modulo di non richiedere all'utente una nuova password. Deve invece accettare qualsiasi password passata dal modulo precedente. In questo modo tutte le nuove password devono passare il controllo `pam_cracklib.so` per verificare la sicurezza delle password prima di accettarle.

```
session required pam_unix.so
```

La riga finale specifica che il componente della sessione del modulo`pam_unix.so` viene usato per gestire la sessione stessa. Questo modulo registra il nome utente e il tipo di servizio in `/var/log/messages` all'inizio e alla fine di ogni sessione. Puòessere supportato da altri moduli di sessione per ottenere una migliore funzionalità.

Nel file di configurazione nell'esempio successivo viene illustrato l'uso del modulo `auth` per il programma `rlogin`.

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

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

```
auth       required     pam_securetty.so
```

Il modulo `pam_securetty.so` impedisce quindi i login di root su terminali non sicuri. In questo modo tutti i tentativi `rlogin` di root sono disabilitati per ragioni di sicurezza.

Suggerimento

Se dovete collegarvi in modo remoto come utente root, usate OpenSSH. Per maggiori informazioni consultate Capitolo 20.

```
auth       required     pam_env.so
```

Questa riga carica il modulo `pam_env.so`, che imposta le variabili d'ambiente specificate in `/etc/security/pam_env.conf`.

```
auth       sufficient  pam_rhosts_auth.so
```

Il modulo `pam_rhosts_auth.so` quindi autentica l'utente per l'uso di `.rhosts` nella sua home directory. Se va a buon fine, PAM considera immediatamente che l'autenticazione abbia avuto un esito positivo. Se `pam_rhosts_auth.so` non riesce ad autenticare l'utente, il tentativo di autenticazione non riuscito viene ignorato.

```
auth       required    pam_stack.so service=system-auth
```

Se il modulo `pam_rhosts_auth.so` non riesce ad autenticare l'utente, il modulo `pam_stack.so` esegue una regolare autenticazione della password.

L'argomento `service=system-auth` indica che l'utente deve ora sottoporsi all'autenticazione PAM per l'autorizzazione del sistema in `/etc/pam.d/system-auth`.

Suggerimento

Se non volete che venga visualizzato il prompt per inserire la password quando `securetty` fallisce, potete cambiare il modulo `pam_securetty.so` da `required` a `requisite`.

16.5. Creazione dei moduli PAM

I nuovi moduli PAM possono essere aggiunti in qualsiasi momento su applicazioni che supportano PAM. Per esempio, se uno sviluppatore inventa un metodo di creazione della password e scrive un modulo PAM per supportarlo, i programmi che supportano PAM, usano immediatamente il nuovo modulo e il metodo password senza essere modificati o ricompilati. Questo permette agli sviluppatori e agli amministratori del sistema, di effettuare una sorta di mix e match, e di prova, dei metodi di autenticazione per programmi diversi senza ricompilarli.

La documentazione sulla scrittura dei moduli é inclusa nella directory `/usr/share/doc/pam-<numero-versione>/` (dove `<numero-versione>` rappresenta il numero della versione di PAM)

16.6. Conservazione delle credenziali di gestione e di PAM

Una varietà di tool di gestione presenti con Red Hat Enterprise Linux permette all'utente di avere elevati privilegi fino a cinque minuti tramite il modulo `pam_timestamp.so`. È importante capire come questo meccanismo funzioni, in quanto se un utente si allontana dal terminale mentre `pam_timestamp.so` è in funzione, lascia la macchina vulnerabile a manipolazioni apportate da un altro utente che ha un accesso fisico alla console.

Con lo schema di timestamp di PAM, l'applicazione di gestione grafica richiede all'utente una password root quando lanciata. Una volta autenticato, il modulo `pam_timestamp.so` crea, per default, un file timestamp all'interno della directory `/var/run/sudo/`. Se il file timestamp è già esistente, gli altri programmi di gestione non richiederanno una password. Invece, il modulo `pam_timestamp.so` aggiornerà il file timestamp — riservando cinque minuti aggiuntivi di accesso amministrativo per l'utente.

L'esistenza del file di timestamp viene delineata da una icona di autenticazione nell'area di notifica del pannello. Di seguito viene illustrata una icona di autenticazione:

Figura 16-1. L'icona di autenticazione

16.6.1. Rimozione del file di timestamp

Si consiglia prima di allontanarsi da una console dove è attivo un timestamp di PAM, di eliminare il file di timestamp. Per fare ciò all'interno di un ambiente grafico, fate clic sull'icona di autenticazione sul pannello. Quando appare una finestra di dialogo, fate clic sul pulsante **Dimentica l'autorizzazione**.

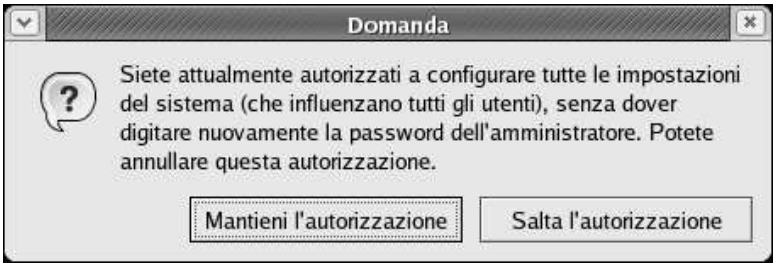

Figura 16-2. Dialogo dell'icona di autenticazione

Se avete effettuato un log in remoto in un sistema usando `ssh`, usare il comando `/sbin/pam_timestamp_check -k root` per eliminare il file timestamp.

Nota Bene

Dovete effettuare il log in come l'utente che originariamente ha invocato il modulo `pam_timestamp.so`, in modo da poter usare il comando `/sbin/pam_timestamp_check`. Non effettuate il log in come utente root per emettere questo comando.

Per informazioni su come eliminare il file timestamp usando `pam_timestamp_check`, consultate la pagina man di `pam_timestamp_check`.

16.6.2. Direttive `pam_timestamp` comuni

Il modulo `pam_timestamp.so` accetta diverse direttive. Di seguito sono riportate le due opzioni più comunemente usate:

- `timestamp_timeout` — Specifica il numero di secondi entro i quali il file timestamp è valido (in secondi). Il valore di default è di 300 secondi (cinque minuti).
- `timestampdir` — Specifica la directory entro la quale il file timestamp è conservato. Il valore di default è `/var/run/sudo/`.

Per maggiori informazioni sul controllo del modulo `pam_timestamp.so`, consultate la Sezione 16.8.1.

16.7. PAM e proprietà dei dispositivi

Red Hat Enterprise Linux conferisce al primo utente che effettua una registrazione sulla console fisica della macchina, una certa abilitá di manipolare alcuni dispositivi ed effettuare alcuni compiti che normalmente sono riservati all'utente root. Questo é controllato da un modulo PAM chiamato `pam_console.so`.

16.7.1. Proprietà dei dispositivi

Quando un utente si collega a un sistema Red Hat Enterprise Linux, il modulo `pam_console.so` viene chiamato da `login` o dai programmi di login grafici, **gdm** e **kdm**. Se questo utente è il primo utente a collegarsi alla console fisica — chiamata *utente console* — il modulo gli assegna la proprietà di vari dispositivi generalmente appartenenti all'utente root. L'utente della console è proprietario di questi dispositivi fino al termine della sessione locale. Quando l'utente non è più collegato, gli viene tolta la proprietà dei dispositivi.

I dispositivi interessati includono, ma non sono limitati a, schede audio, unità floppy e CD-ROM.

Questo consente all'utente locale di manipolare questi dispositivi senza avere un accesso root, semplificando i compiti più comuni per l'utente della console.

Modificando il file `/etc/security/console.perms`, l'amministratore puó modificare l'elenco dei dispositivi controllati da `pam_console.so`.

Avvertimento

Se il file di configurazione display manager **gdm**, **kdm**, o **xdm** è stato alterato in modo da permettere agli utenti remoti di effettuare un log in *e* se l'host è configurato per essere eseguito sul runlevel 5, è consigliabile cambiare le direttive `<console>` e `<xconsole>` all'interno di `/etc/security/console.perms` nei seguenti valori:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :0\.[0-9] :0
<xconsole>=:0\.[0-9] :0
```

Facendo questo, si impedirà agli utenti remoti di ottenere un accesso ai dispositivi e alle applicazioni soggette a restrizioni presenti sulla macchina.

Se il file di configurazione display manager **gdm**, **kdm**, o **xdm** è stato alterato in modo da permettere agli utenti remoti di effettuare un log in *e* se l'host è configurato per essere eseguito sul runlevel 5, è consigliabile rimuovere le direttive `<console>` e `<xconsole>` all'interno di `/etc/security/console.perms` nei seguenti valori:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]*
```

16.7.2. Accesso alle applicazioni

L'utente console può accedere a qualsiasi programma che contiene il nome del comando nella directory `/etc/security/console.apps/`.

Uno dei gruppi di applicazioni a cui l'utente console può accedere è composto da tre programmi per spegnere o riavviare il sistema. Sono:

- `/sbin/halt`
- `/sbin/reboot`
- `/sbin/poweroff`

Si tratta di applicazioni che supportano i moduli PAM, quindi chiamano `pam_console.so` per poter funzionare.

Per maggiori informazioni, consultate la Sezione 16.8.1.

16.8. Risorse aggiuntive

Le seguenti risorse spiegano maggiormente i metodi sull'uso e sulla configurazione di PAM. In aggiunta a queste risorse, leggete i file di configurazione di PAM presenti sul sistema, per capire meglio come essi sono strutturati.

16.8.1. Documentazione installata

- Pagine man relative a PAM — Vi sono un certo numero di pagine man per diversi file di configurazione e applicazioni, presenti con PAM. Il seguente, è un elenco delle pagine man più importanti.

  File di configurazione

  - `man pam` — Rappresenta una buona fonte di informazioni per l'introduzione su PAM, incluso la struttura e lo scopo dei file di configurazione di PAM. Nota bene che anche se questa pagina man parla del file `/etc/pam.conf`, i file di configurazione per PAM con Red Hat Enterprise Linux, sono nella directory `/etc/pam.d/`.
  - `man pam_console` — Descrive lo scopo del modulo `pam_console.so`. Descrive anche la sintassi appropriata per una entry all'interno del file di configurazione di PAM.
  - `man console.apps` — Descrive il formato e le opzioni disponibili all'interno di `/etc/security/console.apps`, il file di configurazione il quale definisce quali applicazioni sono accessibili dall'utente della console assegnato da PAM.
  - `man console.perms` — Descrive il formato e le opzioni disponibili all'interno di `/etc/security/console.perms`, il file di configurazione per i permessi dell'utente della console assegnato da PAM.
  - `man pam_timestamp` — Descrive il modulo `pam_timestamp.so`.

- `/usr/share/doc/pam-<numero_versione>` — Contiene una *Guida dell'amministratore del sistema*, un *Manuale dello scrittore del modulo* e un *Manuale dello sviluppatore dell'applicazione*. Contiene inoltre una copia dello standard PAM, DCE-RFC 86.0 (sostituire `<numero_versione>` con la versione del numero di PAM).
- `/usr/share/doc/pam-<numero-versione>/txts/README.pam_timestamp` — Contiene le informazioni sul modulo PAM `pam_timestamp.so` (sostituire `<numero-versione>` con il numero della versione di PAM).

16.8.2. Siti Web utili

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

Capitolo 17.

Wrapper TCP e `xinetd`

Il controllo dell'accesso ai servizi di rete é uno dei fattori che riguardanola sicurezza piú importanti che un amministratore possa incontrare. Fortunatamente, con Red Hat Enterprise Linux sono disponibili un numero di tool creati appositamente per questo. Per esempio, un firewall basato su `iptables` filtra i pacchetti di rete non desiderati all'interno dello stack di rete del kernel. Per i servizi di rete che lo utilizzano, i *wrapper TCP* aggiungono un livello di protezione, definendo quale host può collegarsi ai servizi di rete "*wrapped*". Uno dei servizi di questo tipo é il *super server* `xinetd`. Questo servizio é chiamato super server perché controlla le connessioni per un sottogruppo di servizi di rete, e garantisce un controllo di accesso piú accurato.

Figura 17-1 rappresenta una illustrazione basica di come questi tool lavorano insieme per proteggere i servizi di rete.

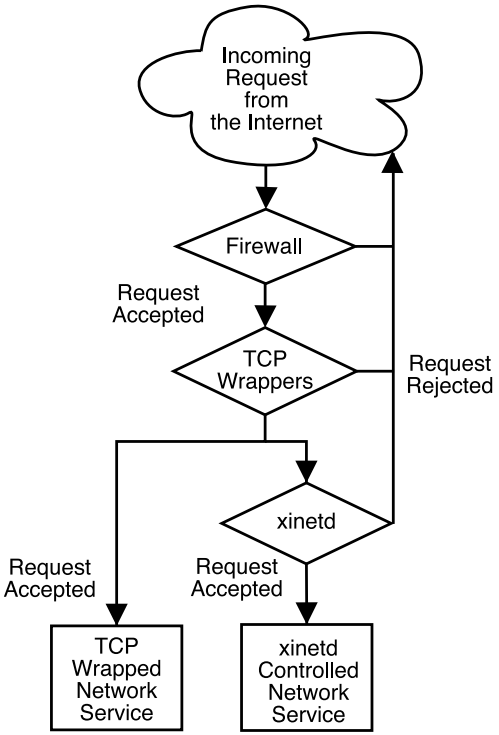

Figura 17-1. Controllo di accesso per i servizi di rete

Questo capitolo si sofferma sul ruolo dei wrapper TCP e `xinetd` nel controllo dell'accesso ai servizi di rete, indicando l'uso migliore dei tool per facilitare la gestione sia nel procedimento di logging che nella sua gestione. Per una discussione sull'uso del firewall con `iptables`, consultare Capitolo 18.

17.1. Wrapper TCP

Il pacchetto dei wrapper TCP (`tcp_wrappers`) viene installato per default e fornisce un controllo d'accesso basato su di un host per i servizi di rete. Il componente piú importante all'interno del pacchetto é la libreria `/usr/lib/libwrap.a`. In termini generali, un servizio wrapped TCP é stato compilato usando la libreria `libwrap.a`.

Quando si tenta il collegamento ad un servizio wrapped TCP, il servizio prima si riferisce ai file *hosts access* (`/etc/hosts.allow` e `/etc/hosts.deny`) per determinare se l'host del client é abilitato al collegamento. In molti casi, il servizio usa il demone syslog (`syslogd`) per scrivere il nome dell'host richiedente e del servizio richiesto su `/var/log/secure` o `/var/log/messages`.

Se un client host é abilitato al collegamento, i wrapper TCP permettono il controllo della connessione al servizio richiesto non interferendo con la comunicazione tra il client host ed il server.

In aggiunta a quanto finora detto, i wrapper TCP possono attivare i comandi per interagire con il client prima di rifiutare o permettere il controllo della connessione al servizio di rete richiesto.

Poichè i wrapper TCP rappresentano un'aggiunta molto importante per i tool di sicurezza di un amministratore del server, molti servizi di rete all'interno di Red Hat Enterprise Linux sono collegati alla libreria `libwrap.a`. Alcune applicazioni includono `/usr/sbin/sshd`, `/usr/sbin/sendmail`, e `/usr/sbin/xinetd`.

Nota Bene

Per determinare se un servizio di rete binario é collegato alla libreria `libwrap.a`, digitare il seguente comando come utente root:

```
strings -f <binary-name> | grep hosts_access
```

Sostituire <*nome-binario*> con il nome del binario del servizio di rete.

Se viene ritornato un prompt, allora il servizio di rete *non* è collegato a `libwrap.a`.

17.1.1. Vantaggi dei Wrapper TCP

I wrapper TCP forniscono i seguenti vantaggi rispetto alle altre techniche di controllo dei servizi di rete:

- *Transparenza sia per il client host sia per il servizio di rete wrapped 'inglobato'.* — Sia il client che si collega che il servizio di rete wrapped non sono a conoscenza dell'uso dei wrapper TCP. Gli utenti abilitati non si accorgeranno di niente, mentre coloro che non sono abilitati non riusciranno a collegarsi.
- *Gestione centralizzata dei protocolli multipli.* — I wrapper TCP funzionano indipendentemente dai servizi di rete da loro protetti, in questo modo, molte applicazioni possono condividere un insieme comune di file di configurazione semplificandone così la gestione.

17.2. File di configurazione dei Wrapper TCP

Per determinare se la macchina di un client é abilitata a collegarsi ad un servizio, i wrapper TCP si riferiscono ai seguenti file, i quali sono conosciuti come file di accesso degli host:

- `/etc/hosts.allow`

- `/etc/hosts.deny`

Quando la richiesta di un client viene ricevuta dal servizio TCP wrapped, viene seguita la seguente procedura:

1. *Riferimenti `/etc/hosts.allow`.* — Il servizio TCP wrapped analizza sequenzialmente il file `/etc/hosts.allow` e applica la prima regola specificata per quel servizio. Se trova una regola corrispondente, la connessione verrá abilitata. Altrimenti sará intrapresa la fase successiva.
2. *Riferimenti `/etc/hosts.deny`.* — Il servizio TCP wrapped analizza sequenzialmente il file `/etc/hosts.deny`. Se trova una regola corrispondente, rifiuterá la connessione. In caso contrario, verrá garantito l'accesso.

I seguenti punti sono molto importanti da considerare quando si usano i wrapper TCP per la protezione dei servizi di rete:

- Poichè le regole d'accesso in `hosts.allow` sono applicate prima, esse hanno la precedenza rispetto alle regole specificate in `hosts.deny`. Tuttavia, se viene permesso l'accesso ad un servizio in `hosts.allow`, viene ignorato il rifiuto d'accesso allo stesso servizio in `hosts.deny`.
- Le regole in ogni file vengono lette dall'alto verso il basso, applicando la prima regola corrispondente, data ad un servizio. L'ordine delle regole é molto importante.
- Se nessuna regola per il servizio viene trovata in entrambi i file, oppure se i file non esistono, l'accesso al servizio viene garantito.
- I servizi TCP wrapped non nascondono le regole dai file di accesso agli host, cosí qualsiasi cambiamento su `hosts.allow` o `hosts.deny` sará confermato immediatamente senza riavviare i servizi di rete.

Avvertenza

Se l'ultima riga di un file di accesso host non risulta essere un carattere di una nuova riga (creato premendo il testo [Invio]), l'ultima regola nel file fallirá, e un errore verrà registrato su `/var/log/messages` o `/var/log/secure`. Questo é anche il caso di una regola che possiede righe multiple senza l'uso del carattere barra. L'esempio riportato illustra una sezione di un messaggio di registrazione nel verificarsi di un fallimento della regola a causa delle seguenti circostanze:

```
warning: /etc/hosts.allow, line 20: missing newline or line too long
```

17.2.1. Formattazione delle regole d'accesso

Il formato per `/etc/hosts.allow` e `/etc/hosts.deny` é identico. Le righe vuote o quelle che iniziano con il segno (`#`) vengono ignorate, e ogni regola deve essere sulla propria riga.

Ogni regola usa il seguente formato di base per controllare l'accesso ai servizi di rete:

```
<daemon list>: <client list> [: <option>: <option>: ...]
```

- `<daemon list>` — Un elenco separato di nomi del processo (*non* i nomi del servizio) oppure `ALL` *wildcard* (consultare la Sezione 17.2.1.1). L'elenco del demone accetta anche gli *operatori* (consultare la Sezione 17.2.1.4) per permettere una maggiore flessibilitá.
- `<client list>` — Un elenco, separato da una virgola, di hostname, di indirizzi host IP, e *pattern* speciali (consultare la Sezione 17.2.1.2), oppure wildcard speciali (consultare la Sezione

17.2.1.1) il quale identifica gli host influenzati dalla regola. L'elenco del client accetta anche gli operatori riportati nella Sezione 17.2.1.4 per permettere una maggiore flessibilitá.

- <option> — Un'azione facoltativa o un elenco di azioni separato da due punti effettuate quando la regola viene innescata. I campi di opzione supportano le *estensioni* (vedere la Sezione 17.2.2.4) e puó essere usato per lanciare i comandi della shell, permettere o rifiutare l'accesso, e alterare il comportamento di logging (vedere la Sezione 17.2.2).

La seguente regola é un esempio di accesso degli host

```
vsftpd : .example.com
```

Questa regola indica ai wrapper TCP di cercare i collegamenti al demone FTP (`vsftpd`) da ogni host nel dominio `example.com`. Se questa regola appare in `hosts.allow`, la connessione verrá accettata. Se la regola appare in `hosts.deny`, la connessione sará rifiutata.

Il prossimo esempio di regola di accesso agli host é piú complesso e usa due campi di opzione:

```
sshd : .example.com  \
: spawn /bin/echo ‘/bin/date‘ access denied>>/var/log/sshd.log \
: deny
```

Notate in questo esempio che ogni campo è preceduto dal carattere (`\`). L'uso di questo carattere evita il fallimento della regola a causa della lunghezza.

Questo esempio indica che se si cerca di effettuare un collegamento al demone SSH (`sshd`) da un host nel dominio `example.com`, eseguire il comando `echo` (il quale registrerá il tentativo su di un file speciale), e negare il collegamento. A causa dell'uso della direttiva `deny`, questa riga rifiuterá l'accesso anche se apparirá nel file `hosts.allow`. Per maggiori informazioni sulle opzioni disponibili, consultare la Sezione 17.2.2.

17.2.1.1. Wildcard

Le Wildcard permettono ai wrapper TCP di corrispondere facilmente con i gruppi di demoni o degli host. Esse sono usate molto frequentemente nel campo dell'elenco dei client delle regole di accesso.

Possono essere usate le seguenti wildcard:

- `ALL` — Corrisponde con tutto. Puó essere usato sia per l'elenco dei demoni che per quella dei client.
- `LOCAL` — Corrisponde a qualsiasi host che non contiene un periodo (`.`), come ad esempio l'host locale.
- `KNOWN` — Corrisponde a qualsiasi host dove l'hostname e l'indirizzo host sono conosciuti o dove l'utente é conosciuto.
- `UNKNOWN` — Corrisponde a ogni host dove l'hostname o l'indirizzo host sono sconosciuti o dove anche l'utente é sconosciuto.
- `PARANOID` — Corrisponde a qualsiasi host dove l'hostname non corrisponde all'indirizzo dell'host.

Attenzione

Le wildcard `KNOWN`, `UNKNOWN`, e `PARANOID` dovrebbero essere usate con attenzione in quanto una rottura nella risoluzione del nome puó compromettere l'ingresso ad un servizio ad un utente abilitato.

17.2.1.2. Pattern

I Pattern possono essere usati nel campo dell'elenco del client delle regole di accesso, per poter meglio specificare i gruppi di host del client.

Di seguito viene riportata una lista dei pattern piú comuni accettati per una entry dell'elenco del client.

- *Hostname che iniziano con un punto (`.`)* — Posizionando un punto all'inizio di un hostname, corrisponde a tutti gli host che condividono i componenti del nome elencati. Il seguente esempio sará applicato per ogni host all'interno del dominio `example.com`:
  ```
  ALL : .example.com
  ```
- *Indirizzo IP che termina con un punto (`.`)* — Posizionando un punto alla fine di un indirizzo IP, si corrisponde a tutti gli host che condividono i gruppi numerici iniziali di un indirizzo IP. Il seguente esempio sará valido per tutti gli host all'interno della rete `192.168.x.x`.
  ```
  ALL : 192.168.
  ```
- *indirizzo IP/maschera di rete* — Espressioni della maschera di rete possono essere usate come un pattern per controllare l'accesso a un gruppo particolare di indirizzi IP. Il seguente esempio sará valido per qualsiasi host con un indirizzo di `192.168.0.0` fino a `192.168.1.255`:
  ```
  ALL : 192.168.0.0/255.255.254.0
  ```

Importante

Quando si lavora nello spazio dell'indirizzo IPv4, la lunghezza della coppia indirizzo/prefisso (*prefixlen*) non è supportata. Solo le regole IPv6 possono usare questo formato.

- *coppia [IPv6 address]/prefixlen* — Le coppie [net]/prefixlen possono essere usate come un pattern per controllare l'accesso a un gruppo particolare di indirizzi IPv6. Il seguente esempio sará valido per qualsiasi host con un indirizzo di `3ffe:505:2:1::` fino a `3ffe:505:2:1:ffff:ffff:ffff:ffff`:
  ```
  ALL : [3ffe:505:2:1::]/64
  ```

- *L'asterisco(`*`)* — L'asterisco puó essere usato quando ci si riferisce ad interi gruppi di hostname o di indirizzi IP, solo se non sono presenti in un elenco del client contenente altri tipi di pattern. Il seguente esempio sará valido per ogni host all'interno del dominio `example.com`:
  ```
  ALL : *.example.com
  ```
- *La barra (`/`)* — Se l'elenco di un client inizia con una barra, verrá trattato come un file name. Ció é utile se sono necessarie le regole che specificano numeri molto grandi di host. Il seguente esempio si riferisce ai wrapper TCP per il file `/etc/telnet.hosts` per tutti i collegamenti Telnet:
  ```
  in.telnetd : /etc/telnet.hosts
  ```

Altri pattern meno usati sono accettati dai wrapper TCP. Consultate la pagina man 5 `hosts_access` per maggiori informazioni.

Avvertenza

Prestate molta attenzione quando usate gli hostname e i nomi del dominio.Gli aggressori possono usare una varietá di trucchi per aggirare un'accurata risoluzione del nome. In aggiunta, ogni interruzione nel servizio DNS eviterebbe anche agli utenti autorizzati l'uso dei servizi di rete.

Pertanto è meglio usare indirizzi IP quando possibile.

17.2.1.3. Portmap e Wrapper TCP

Quando si creano le regole per il controllo dell'accesso per `portmap`, non usare gli hostname come implementazione `portmap` dei wrapper TCP in quanto l'implementazione dei wrapper TCP non supporta l'host look up. Per questo motivo, usate solo gli indirizzi IP o la keyword `ALL` quando si specificano gli host in `hosts.allow` o `hosts.deny`.

In aggiunta, i cambiamenti apportati alle regole di controllo per l'accesso a`portmap` possono non avere un effetto immediato se non si riavvia il servizio `portmap`.

Servizi molto diffusi, come ad esempio NIS e NFS, per operare dipendono da `portmap`, per questo motivo fate attenzione a questi limiti.

17.2.1.4. Operatori

Al momento le regole per il controllo dell'accesso, accettano un operatore, `EXCEPT`. Puó essere usato nell'elenco del demone oppure nell'elenco del client di una regola.

L'operatore `EXCEPT` abilita specifiche eccezioni a corrispondenze piú vaste all'interno della stessa regola.

Nel seguente esempio da un file `hosts.allow`, tutti gli host `example.com` sono abilitati a connettersi a tutti i servizi eccetto `cracker.example.com`:

```
ALL: .example.com EXCEPT cracker.example.com
```

In un altro esempio da un file `hosts.allow`, i client dalla rete 192.168.0.*x* possono usare tutti i servizi eccetto FTP:

```
ALL EXCEPT vsftpd: 192.168.0.
```

Nota Bene

Amministrativamente, è più semplice evitare di usare gli operatori `EXCEPT`. Questo permette ad altri amministratori di controllare velocemente i file appropriati per vedere quali sono gli host autorizzati,per accedere ai servizi senza passare per i vari operatori `EXCEPT`.

17.2.2. Campi di opzione

In aggiunta alle regole di base sul rifiuto o sul permesso all'accesso, l'implementazione Red Hat Enterprise Linux dei wrapper TCP, supporta le estensioni per la lingua di controllo per l'accesso attraverso i campi di opzione. Usando i campi di opzione all'interno delle regole di accesso degli host, gli amministratori possono ottenere una varietá di compiti come ad esempio l'alterazione del comportamento di log, il consolidamento del controllo d'accesso, e il lancio dei comandi della shell.

17.2.2.1. Logging

I campi di opzione permettono all'amministratore di cambiare la funzione di registrazione ed il livello di prioritá per una regola, usando la direttiva `severity`.

Nel seguente esempio, i collegamenti per il demone SSH, da un qualsiasi host nel dominio `example.com` sono registrati per la funzione di default `authpriv` `syslog` (perché nessun valore é specificato) con una priorità di `emerg`:

```
sshd : .example.com : severity emerg
```

É possibile specificare una funzione usando l'opzione `severity`. Il seguente esempio registra qualsiasi host dal dominio `example.com` che cerca di connettersi al servizio SSH alla funzione `local0` con una priority di `alert`:

```
sshd : .example.com : severity local0.alert
```

Nota Bene

In pratica, questo esempio non funziona fino a quando il demone syslog (`syslogd`) é configurato per effettuare un log per `local0`. Consultare la pagina man `syslog.conf` per informazioni inerenti la configurazione delle facility log personalizzate.

17.2.2.2. Controllo dell'accesso

I campi di opzione permettono agli amministratori di abilitare o negare gli host con una regola singola aggiungendo le direttive `allow` o `deny` come opzione finale.

Per esempio, le due regole seguenti abilitano dei collegamenti SSH da `client-1.example.com`, ma rifiutano i collegamenti da `client-2.example.com`:

```
sshd : client-1.example.com : allow
sshd : client-2.example.com : deny
```

Permettendo il controllo d'accesso in base alla regola, il campo di opzione permette agli amministratori di consolidare tutte le regole d'accesso in un file singolo: `hosts.allow` o `hosts.deny`. Alcuni lo considerano il modo piú facile per organizzare le regole d'accesso.

17.2.2.3. Comandi della Shell

I campi di opzione permettono alle regole d'accesso di lanciare i comandi della shell attraverso le seguenti direttive:

- `spawn` — Lancia un comando della shell come programma figlio. Questa opzione puó effettuare dei compiti come ad esempio usare `/usr/sbin/safe_finger` per ottenere piú informazioni inerenti il client richiedente, o creare file di registrazione speciali usando il comando `echo`.

  Nel seguente esempio, i client che cercano di accedere ai servizi Telnet dal dominio `example.com` sono registrati su di un file speciale:

  ```
  in.telnetd : .example.com \
    : spawn /bin/echo '/bin/date' from %h>>/var/log/telnet.log \
    : allow
  ```

- `twist` — Sostituisce il servizio richiesto con il comando specificato. Questa direttiva viene usata spesso per impostare delle trappole per gli intrusi (chiamate anche "honey pots"). Esso puó essere usato per mandare messaggi ai client. La direttiva `twist` deve essere presente alla fine della riga della regola.

  Nel seguente esempio, ai client che tentano di accedere i servizi FTP dal dominio `example.com` viene inviato un messaggio tramite il comando `echo`:

  ```
  vsftpd : .example.com \
  : twist /bin/echo "421 Bad hacker, go away!"
  ```

Per maggiori informazioni inerenti le opzioni di comando della shell, consultare la pagina man `opzioni_host`.

17.2.2.4. Espansioni

Le espansioni, quando usate insieme con le direttive `spawn` e `twist` forniscono informazioni inerenti il client, il server ed i processi coinvolti.

Di seguito viene riportata una lista delle estensioni supportate:

- `%a` — Fornisce l'indirizzo IP del client.
- `%A` — Fornisce l'indirizzo IP del server.
- `%c` — Fornisce una varietá d'informazioni inerenti il client, come ad esempio il nome utente e l'hostname, oppure il nome utente e l'indirizzo IP.
- `%d` — Fornisce il nome del processo del demone..
- `%h` — Fornisce l'hostname del client (o l'indirizzo IP se l'hostname non è disponibile).
- `%H` — Fornisce l'hostname del server (o l'indirizzo IP se l'hostname non è disponibile).
- `%n` — Fornisce l'hostname del client. Se non è disponibile, viene visualizzato `unknown`. Se l'hostname del client e l'indirizzo host non corrispondono, viene visualizzato `paranoid`.
- `%N` — Fornisce l'hostname del server. Se non è disponibile, viene visualizzato `unknown`. Se l'hostname del server e l'indirizzo host non corrispondono, compare, `paranoid`.
- `%p` — Fornisce l'ID del processo demone.
- `%s` — Fornisce vari tipi di informazioni del server, quali il processo demone e l'indirizzo host o IP del server.
- `%u` — Fornisce l'username del client. Se non è disponibile, viene visualizzato `unknown`.

Il seguente esempio usa una espansione insieme con il comando `spawn` per identificare l'host del client in un file di registrazione personalizzato.

Quando si cerca di eseguire un collegamento al demone SSH (`sshd`), da un host presente nel dominio `example.com`, eseguire il comando `echo` per registrare il tentativo, includendo l'hostname del client (usando l'espansione `%h`), per un file speciale:

```
sshd : .example.com  \
: spawn /bin/echo ‘/bin/date‘ access denied to %h>>/var/log/sshd.log \
: deny
```

In modo simile, le espansioni possono essere usate per personalizzare i messaggi per il client. Nell'esempio seguente, , i client che cercano di accedere ai servizi FTP dal dominio `example.com` sono informati che essi sono stati esclusi dal server:

```
vsftpd : .example.com \
: twist /bin/echo "421 %h has been banned from this server!"
```

Per una spiegazione completa delle estensioni disponibili, e anche delle opzioni aggiuntive del controllo di accesso, consultare la sezione 5 delle pagine man per `hosts_access` (`man 5 hosts_access`) e la pagina man per `hosts_options`.

Per informazioni aggiuntive sui wrapper TCP, consultare la Sezione 17.5. Per informazioni aggiuntive su come rendere sicuri i wrapper TCP, consultare il capitolo intitolato *Sicurezza del server* nel *Red Hat Enterprise Linux Security Guide*.

17.3. xinetd

Il demone xinetd é un TCP wrapped *super service* il quale controlla l'accesso ad una sottorete dei servizi di rete incluso FTP, IMAP e Telnet. Esso fornisce anche delle opzioni di configurazione specifiche del servizio per un controllo dell'accesso, aumento del logging, del ridirezionamento, procedura binding e controllo dell'utilizzazione delle risorse.

Quando un client host cerca di collegarsi ad un servizio di rete controllato da xinetd, il super servizio riceve la richiesta e controlla l'esistenza di regole per il controllo d'accesso dei wrapper TCP. Se si abilita l'accesso, xinetd verifica che il collegamento venga abilitato sotto le proprie regole per quel servizio e che lo stesso servizio non richieda piú risorse di quelle a lui destinate o che non vada contro le regole in vigore. Esso avvia quindi un esempio di servizio richiesto e passa il controllo del collegamento al servizio stesso. Una volta stabilito il collegamento, xinetd non interferisce nella comunicazione tra il client dell'host ed il server.

17.4. File di configurazione xinetd

I file di configurazione per xinetd sono di seguito riportati:

- /etc/xinetd.conf — Il file di configurazione xinetd globale.
- /etc/xinetd.d/ — La directory che contiene tutti i file del servizio specifico.

17.4.1. Il file /etc/xinetd.conf

Il file /etc/xinetd.conf contiene le impostazioni di configurazione generali che influenzano ogni servizio sotto il controllo di xinetd. Viene letto una volta quando il servizio xinetd viene avviato, cosí per poter confermare i cambiamenti riguardanti la configurazione, l'amministratore deve riavviare il servizio xinetd. Di seguito viene riportato un esempio del file /etc/xinetd.conf:

```
defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}
includedir /etc/xinetd.d
```

Queste righe controllano i seguenti aspetti di xinetd:

- instances — Imposta il numero massimo di richieste che xinetd puó far fronte contemporaneamente.
- log_type — Configura xinetd in modo da usare la funzione di log authpriv, il quale scrive le entry di registrazione sul file /var/log/secure. Se si aggiungesse una direttiva come ad esempio FILE /var/log/xinetdlog viene creato un file di log personalizzato chiamato xinetdlog nella directory /var/log/.
- log_on_success — Indica a xinetd cosa registrare se la connessione avviene correttamente. Per default, vengono registrati l'indirizzo IP dell'host remoto e l'ID del server che elabora la richiesta.
- log_on_failure —indica a xinetd cosa registrare se la connessione fallisce o non è autorizzata.
- cps — indica a xinetd di non abilitare più di 25 connessioni al secondo verso uno specifico servizio. Quando tale limite viene raggiuto, il servizio entra in pausa per 30 secondo.

- includedir /etc/xinetd.d/ — Include le opzioni dichiarate nei file di configurazione del servizio specifico, posizionato nella directory /etc/xinetd.d/. Consultate la Sezione 17.4.2 per maggiori informazioni.

Nota Bene

Spesso le impostazioni log_on_success e log_on_failure in /etc/xinetd.conf sono maggiormente modificate nei file di registrazione specifici del servizio. Per questa ragione, piú informazioni possono apparire in una registrazione di un servizio rispetto alle informazioni date dal file /etc/xinetd.conf.Consultare la Sezione 17.4.3.1 per maggiori informazioni.

17.4.2. La directory /etc/xinetd.d/

La directory /etc/xinetd.d/ contiene i file di configurazione per ogni servizio gestito da xinetd ed i nomi dei file relativi al servizio. Come con xinetd.conf, questa directory viene letta solo quando il servizio xinetd é avviato. Per confermare qualsiasi cambiamento, l'amministratore deve riavviare il servizio xinetd.

Il formato dei file nella directory /etc/xinetd.d/ usa le stesse convenzioni di /etc/xinetd.conf. La ragione principale per la quale la configurazione di ogni servizio viene conservata in file separati, é quella di permettere una personalizzazione piú facile con minore probabilitá di condizionare altri servizi.

Per avere una idea di come questi file sono strutturati, considerate il file /etc/xinetd.d/telnet:

```
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = yes
}
```

Queste righe controllano vari aspetti del servizio vsftpd

- service — Definisce il nome del servizio, generalmente usando un nome elencato nel file /etc/services.
- flags — Imposta un numero di attributi per il collegamento. REUSE indica a xinetd di usare nuovamente il socket per un collegamento Telnet.
- socket_type — Imposta il tipo di rete socket per stream.
- wait — Definisce se il servizio é singolo "single-threaded" (yes) o multiplo "multi-threaded" (no).
- user — Definisce con quale user ID verrá eseguito il processo.
- server — Definisce il binario eseguibile da lanciare.
- log_on_failure — Definisce i parametri di logging per log_on_failure in aggiunta a quelli giá definiti in xinetd.conf.
- disable — Definisce se il server é attivo.

17.4.3. Alterazione dei file di configurazione xinetd

Vi é un grande assortimento di direttive disponibili per i servizi protetti xinetd. Questa sezione evidenzia alcune delle opzioni maggiormente usate.

17.4.3.1. Opzioni di Logging

Le seguenti opzioni di logging sono disponibili per /etc/xinetd.conf e per i file di configurazione specifici del servizio nella directory /etc/xinetd.d/.

Di seguito é riportato un elenco di alcune delle opzioni di logging piú comunemente usate:

- ATTEMPT — registra i tentativi falliti di accesso (log_on_failure).
- DURATION — registra il tempo di utilizzo di un servizio da parte di un sistema remoto (log_on_success).
- EXIT — registra il segnale di chiusura del servizio (log_on_success).
- HOST — registra l'indirizzo IP dell'host remoto (log_on_failure e log_on_success).
- PID — registra l'ID del server che riceve la richiesta (log_on_success).
- USERID — registra l'utente remoto usando il metodo definito in RFC 1413 per tutti i servizi stream multi-thread (log_on_failure e log_on_success).

Per un elenco completo delle opzioni di logging, consultare la pagina man xinetd.conf.

17.4.3.2. Opzioni di controllo dell'accesso

Gli utenti dei servizi xinetd possono scegliere di usare le regole di accesso host dei wrapper TCP, fornire il controllo di accesso tramite i file di configurazione xinetd, o un insieme dei due. Informazioni relative all'uso dei file di controllo dell'accesso host dei wrapper TCP sono riportate nella Sezione 17.2.

Questa sezione affronta l'uso di xinetd per controllare l'accesso ai servizi.

Nota Bene

A differenza dei wrapper TCP, le modifiche apportate al controllo dell'accesso verranno confermate se l'amministratore di xinetd riavvia il servizio xinetd.

Inoltre, a differenza dei wrapper TCP, il controllo dell'accesso eseguito attraverso xinetd, influenzerà solo i servizi controllati da xinetd.

Il controllo dell'accesso fornito da xinetd differisce dal metodo usato dai wrapper TCP. Mentre i wrapper TCP raggruppano tutta la configurazione di accesso in due file, /etc/hosts.allow e /etc/hosts.deny, il controllo dell'accesso di xinetd viene trovato su ogni file di configurazione del servizio all'interno della directory/etc/xinetd.d/.

Le seguenti opzioni d'accesso host sono supportate da xinetd:

- only_from — Permette agli host specificati di usare il servizio.
- no_access — Impedisce a questi utenti di usare il servizio.
- access_times — specifica la fascia oraria in cui un particolare servizio può essere utilizzato. La fascia oraria deve essere specificata nel formato HH:MM-HH:MM e utilizzare le 24 ore della giornata.

Le opzioni only_from e no_access possono usare un elenco di indirizzi IP o di hostname, oppure è possibile specificare un'intera rete. Come per i wrapper TCP, se associate il controllo di accesso xinetd con una configurazione logging migliorata, potete aumentare la sicurezza, bloccando le richieste da host non autorizzati, registrando anche ogni tentativo effettuato.

Per esempio, il seguente file /etc/xinetd.d/telnet può bloccare l'accesso telnet da parte di uno specifico gruppo di rete e restringere la fascia oraria durante la quale anche gli utenti autorizzati possono collegarsi:

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        no_access       = 10.0.1.0/24
        log_on_success  += PID HOST EXIT
        access_times    = 09:45-16:15
}
```

In questo esempio, quando un sistema client dalla rete 10.0.1.0/24, come ad esempio 10.0.1.2, cerca di accedere al servizio Telnet, esso riceverá il seguente messaggio:

```
Connection closed by foreign host.
```

In aggiunta, il loro tentativo di login viene registrato in /var/log/secure:

```
May 15 17:38:49 boo xinetd[16252]: START: telnet pid=16256 from=10.0.1.2
May 15 17:38:49 boo xinetd[16256]: FAIL: telnet address from=10.0.1.2
May 15 17:38:49 boo xinetd[16252]: EXIT: telnet status=0 pid=16256
```

Quando si usano i wrapper TCP insieme ai controlli d'accesso xinetd, é importante capire il rapporto tra due meccanismi di controllo.

Di seguito viene riportato l'ordine delle operazioni seguite da xinetd quando un client richiede un collegamento:

1. Il demone xinetd accede alle regole dell'accesso host dei wrapper TCP attraverso una libreria libwrap.a. Se una regola di rifiuto "deny" corrisponde con il client host, la connessione viene passata su xinetd.
2. Il demone xinetd controlla le proprie regole di controllo dell'accesso sia per il servizio xinetd che per il servizio richiesto. Se una regola di rifiuto "deny" corrisponde con il client host, la connessione viene terminata. Altrimenti, xinetd avvia un esempio del servizio richiesto passando il controllo della connessione al servizio stesso.

Importante

Prestare attenzione quando si usano i controlli d'accesso dei wrapper TCP insieme con i controlli dell'accesso xinetd. Una configurazione errata puó causare degli effett indesiderati.

17.4.3.3. Opzioni di collegamento e ridirezionamento

I file di configurazione dei servizi di xinetd supportano anche il collegamento dei servizi a particolari indirizzi IP e il ridirezionamento delle richieste in entrata ad altri indirizzi IP, nomi host o porte.

Il binding è controllato tramite l'opzione bind nei file di configurazione dei servizi, collega un servizio a un particolare indirizzo IP usato sul sistema. Una volta configurata, l'opzione bind permette l'accesso al servizio solo alle richieste che utilizzano tale indirizzo IP. In questo modo i servizi diversi possono essere inviati alle interfacce di rete in base all'esigenza.

Questo è particolarmente utile per sistemi con più adattatori di rete e indirizzi IP. Su tale sistema, i servizi non sicuri, come Telnet, possono essere configurati in solo ascolto sull'interfaccia collegata ad una rete privata e non con una interfaccia collegata con Internet.

L'opzione redirect, che accetta un indirizzo IP o un nome host seguito da un numero di porta, indica al servizio di ridirezionare tutte le richieste per il servizio verso la posizione specificata. Questa funzione può essere usata per puntare verso un altro numero di porta sullo stesso sistema, ridirezionare la richiesta verso altri indirizzi IP sulla stessa macchina, inviare la richiesta a un numero di porta e sistema completamente diverso oppure a una combinazione di queste opzioni. In questo modo, un utente che si collega a un servizio su un sistema può essere instradato verso un altro sistema senza causare problemi.

Il demone xinetd è in grado di compiere questo ridirezionamento creando un processo che rimane attivo durante la connessione tra la macchina client che svolge la richiesta e l'host che effettivamente fornisce il servizio e che trasferisce i dati fra i due sistemi.

La vera forza delle opzioni bind e redirect si nota quando queste vengono usate insieme. Collegando un servizio a un indirizzo IP su un sistema e ridirezionando successivamente la richiesta per il servizio a una seconda macchina che può essere vista solo dalla prima macchina, potete usare un sistema interno che fornisce servizi a una rete totalmente diversa. Altrimenti, le due opzioni possono essere usate per limitare l'esposizione di un servizio su una macchina multihome a un indirizzo IP conosciuto, e ridirigere tutte le richieste per il servizio verso un'altra macchina appositamente configurata.

Per esempio, esaminate un sistema usato come firewall i cui parametri per il servizio Telnet sono:

```
service telnet
{
        socket_type  = stream
        wait   = no
        server   = /usr/sbin/in.telnetd
        log_on_success  += DURATION USERID
        log_on_failure  += USERID
        bind                    = 123.123.123.123
        redirect                = 10.0.1.13 23
}
```

Le opzioni bind e redirect contenute in questo file assicurano che il servizio Telnet della macchina sia collegato all'indirizzo IP esterno (123.123.123.123), quello rivolto verso Internet. Inoltre, tutte le richieste per il servizio telnet inviate a 123.123.123.123 vengono ridirezionate tramite un altro adattatore di rete a un indirizzo IP interno (10.0.1.13) accessibile solo dal firewall e dai sistemi interni. Il firewall invia in seguito la comunicazione tra i due sistemi e il sistema in collegamento crede di essere collegato a 123.123.123.123 mentre in realtà è collegato a un'altra macchina.

Questa funzione è particolarmente utile per gli utenti con collegamenti veloci e un unico indirizzo IP fisso. Quando viene utilizzato il (NAT) Network Address Translation, i sistemi dietro la macchina gateway che utilizzano solo indirizzi IP interni, non sono disponibili all'esterno del sistema gateway. Tuttavia, quando alcuni servizi controllati da xinetd sono configurati con le opzioni bind e redirect, la macchina gateway può agire come un proxy fra i sistemi esterni e una macchina interna configurata per fornire il servizio. Inoltre, le varie opzioni di controllo dell'accesso e di loggin dixinetd sono disponibili per una protezione aggiuntiva.

17.4.3.4. Opzioni di amministrazione delle risorse

Il demone `xinetd` puó aggiungere un livello basico di protezione per attacchi Denial of Service (DoS). Di seguito viene riportata una lista di direttive che possono aiutare a limitare gli effetti di tali attacchi:

- `per_source` — Definisce il numero massimo di istanze per un servizio per indirizzo IP della sorgente. Accetta solo numeri interi come argomento e puó essere usato in `xinetd.conf` e nei file di configurazione del servizio specifico nella directory `xinetd.d/`.
- `cps` — Definisce il numero massimo di connessioni al secondo. Questa direttiva prende due argomenti separati da uno spazio bianco. Il primo é il numero massimo di connessioni permesse al sirvizio al secondo. Il secondo é il numero dei secondi che `xinetd` deve attendere prima di abilitare nuovamente il servizio. Accetta solo numeri interi come argomento e puó essere usato in `xinetd.conf` e nei file di configurazione del servizio specifico nella directory `xinetd.d/`.
- `max_load` — Definisce l'uso del limite della CPU per un servizio. Accetta come argomento numeri 'floating point' con virgola mobile.

Ci sono altre opzioni di gestione delle risorse disponibili per `xinetd`. Consultate il capitolo intitolato *Sicurezza del server* nel *Red Hat Enterprise Linux Security Guide* per maggiori informazioni. Consultate altresì anche la pagina man `xinetd.conf`.

17.5. Risorse aggiuntive

Ulteriori informazioni relative ai wrapper TCP e `xinetd` sono disponibili nella documentazione del sistema e su internet.

17.5.1. Documentazione installata

La documentazione fornita con il sistema costituisce un'ottimo punto di partenza per cercare altre informazioni sui wrapper TCP, su `xinetd` e sulle opzioni per la configurazione del controllo di accesso.

- `/usr/share/doc/tcp_wrappers-<`*`version`*`>/` — Questa directory contiene un file `README` che affronta il funzionamento dei wrapper TCP ed i vari rischi di spoofingesistenti nell'utilizzo degli hostname e degli indirizzi host.
- `/usr/share/doc/xinetd-<`*`version`*`>/` — Questa directory contiene un file `README` che affronta i vari aspetti sul controllo dell'accesso e un file `sample.conf` che contiene diversi aspetti per la modifica dei file di configurazione specifici al servizio presenti nella directory `/etc/xinetd.d`.
- Wrapper TCP e pagine man relative a `xinetd` — Vi è un certo numero di pagine man per diversi file di configurazione e applicazioni riguardanti i wrapper TCP e `xinetd`. Di seguito vengono riportate alcune delle pagine man più importanti.

  Applicazioni del server

  - `man xinetd` — La pagina man per il demone del super service `xinetd`.

File di configurazione

- `man 5 hosts_access` — La pagina man per i file di controllo dell'accesso host dei wrapper TCP.
- `man hosts_options` — La pagina man per i campi delle opzioni dei wrapper TCP.
- `man xinetd.conf` — La pagina man che elenca le opzioni di configurazione di `xinetd`.

17.5.2. Siti Web utili

- http://www.xinetd.org — La home di `xinetd`, contenente un esempio di file di configurazione, un elenco completo di tutti i contenuti, e una informativa FAQ.
- http://www.macsecurity.org/resources/xinetd/tutorial.shtml — sito che spiega in modo dettagliato i vari modi per modificare i file di configurazione predefiniti di `xinetd` per adattarli alle proprie necessità di sicurezza.

17.5.3. Libri correlati

- *Red Hat Enterprise Linux Security Guide* ; Red Hat, Inc. — Fornisce una panoramica su workstation, server e sulla sicurezza di rete con suggerimenti specifici riguardanti i wrapper TCP e `xinetd`.
- *Hacking Linux Exposed* di Brian Hatch, James Lee, e George Kurtz; Osbourne/McGraw-Hill — Una risorsa eccellente per quanto riguarda la sicurezza, con informazioni riguardanti i wrapper TCP e `xinetd`.

Capitolo 18.

iptables

Installato con Red Hat Enterprise Linux vi sono dei tool avanzati per il *filtraggio dei pacchetti* della rete —, ovvero il processo di controllo dei pacchetti di rete, all'interno del kernel, che cercano di accedere, transitare e uscire dallo stack della rete. Le versioni del kernel precedenti alla 2.4 si affidavano al comando `ipchains` per il filtraggio e utilizzavano gli elenchi di regole applicabili ai pacchetti in ogni fase del processo stesso. Con il Kernel 2.4 è stato introdotto il comando `iptables`, (chiamato anche *netfilter*), il quale è simile a `ipchains`, ma permette di ampliare notevolmente le possibilità di controllo in fase di filtraggio dei pacchetti.

Questo capitolo si concentra sugli aspetti di base del filtraggio dei pacchetti, evidenzia le differenze tra `ipchains` e `iptables`, spiega le varie opzioni disponibili con i comandi `iptables`, e spiega come preservare le regole di filtraggio tra un riavvio del sistema e l'altro.

Se avete bisogno di istruzioni su come creare regole `iptables` o configurare un firewall basato su tali regole, consultate la Sezione 18.7.

Avvertenza

Il meccanismo di default del firewall per il kernel 2.4 è `iptables`, ma `iptables` non può essere utilizzato se `ipchains` sono già in esecuzione. Se `ipchains` è presente al momento dell'avvio, il kernel emette un messaggio di errore e non sarà in grado di avviare `iptables`.

Questo genere di errori non hanno ripercussioni sul funzionamento di `ipchains`.

18.1. Filtraggio dei pacchetti

Il kernel di Linux possiede la capacità integrata di filtrare i pacchetti, concedendo o negando loro l'accesso al sistema. Il netfilter del kernelpresenta tre *tabelle* integrate dette anche *elenchi delle regole*. Eccole riportate:

- `filter` — La tabella di default per la gestione dei pacchetti di rete.
- `nat` — Questa tabella altera i pacchetti che creano un collegamento e viene usata per il *Network Address Translation* (*NAT*).
- `mangle` — Questa tabella viene usata per l'alterazione di pacchetti specifici.

Suggerimento

In aggiunta a queste tabelle integrate, è possibile creare delle tabelle specializzate e conservate nella directory `/lib/modules/<versione-kernel>/kernel/net/ipv4/netfilter/` (dove <*versione-kernel*> corrisponde al numero della versione del kernel).

Ogni tabella ha un gruppo di *catene* integrate, che corrispondono alle azioni effettuate da netfilter sul pacchetto.

Le catene integrate per la tabella `filter` sono le seguenti:

- *INPUT* — Si applica ai pacchetti ricevuti mediante un'interfaccia di rete.

- *OUTPUT* — Si applica ai pacchetti inviati mediante la stessa interfaccia di rete che ha ricevuto i pacchetti in entrata.
- *FORWARD* — Si applica ai pacchetti ricevuti su una data interfaccia di rete e inviati mediante un'altra.

Le catene integrate per la tabella `nat` sono le seguenti:

- *PREROUTING* — Questa catena altera i pacchetti ricevuti attraverso un'interfaccia di rete al loro arrivo.
- *OUTPUT* — Altera i pacchetti di rete generati localmente, prima che gli stessi vengono inviati all'esterno.
- *POSTROUTING* — Questa catena altera i pacchetti prima che vengano inviati attraverso un'interfaccia di rete.

Le catene integrate per la tabella `mangle` sono le seguenti:

- *INPUT* — Altera i pacchetti di rete designati per l'host.
- *OUTPUT* — Altera i pacchetti di rete generati localmente, prima che gli stessi vengono inviati all'esterno.
- *FORWARD* — Altera i pacchetti di rete diretti attraverso l'host.
- *PREROUTING* — Questa catena altera i pacchetti ricevuti attraverso un'interfaccia di rete prima che vengano instradati.
- *POSTROUTING* — Questa catena altera i pacchetti prima che vengano inviati attraverso un'interfaccia di rete.

Ogni pacchetto di rete ricevuto o inviato da un sistema Linux è soggetto ad almeno una tabella. Tuttavia, un pacchetto può essere soggetto a numerose regole all'interno di ogni tabella prima di raggiungere la fine della catena. La struttura e lo scopo di queste regole possono variare, ma di norma si occupano di identificare un pacchetto proveniente da o diretto verso un determinato indirizzo IP o gruppo di indirizzi tramite un protocollo e un servizio di rete particolari.

Nota Bene

Non utilizzare i nomi del dominio qualificati all'interno delle regole del firewall salvate nei file `/etc/sysconfig/iptables` o `/etc/sysconfig/ip6tables`. Nel seguente esempio: `iptables -A FORWARD -s example.com -i eth0 -j DROP example.com` risulta essere invalido poichè il servizio `iptables`, inizia, al momento dell'avvio, prima di qualsiasi servizio relativo a DNS, tale procedura dà luogo alla presenza di un errore. Solo gli indirizzi IP risultano essere validi per la creazione delle regole del firewall.

Indipendentemente dalla sua destinazione, quando un pacchetto soddisfa una particolare regola contenuta in una delle tabelle, gli viene attribuito un determinato *target* o azione. Se la regola decide di assegnargli il target `ACCEPT`, il pacchetto può saltare i controlli legati alle restanti regole ed è autorizzato a procedere verso la sua destinazione. Se invece la regola opta per il target `DROP`, il pacchetto viene abbandonato, ossia gli viene negato l'accesso al sistema, e all'host mittente non viene rispedito indietro nulla. Se vi é una regola che specifica un target `QUEUE`, il pacchetto deve essere passato ad uno spazio-utente. Nel caso in cui la regola decida di applicare al pacchetto il target `REJECT`, il pacchetto viene comunque abbandonato, ma al nodo mittente viene recapitato un pacchetto di errore.

Ogni catena ha una policy di default per accettare `ACCEPT`, abbandonare `DROP`, rifiutare `REJECT`, o per accodarlo `QUEUE` verso lo spazio utente. Quando nessuna delle regole della catena risulta applicabile al pacchetto, è la policy di default a decidere come gestirlo.

Il comando iptables vi consente sia di configurare questi elenchi di regole, sia di impostare nuove catene e nuove tabelle.

18.2. Differenze tra iptables e ipchains

A prima vista, ipchains e iptables risultano piuttosto simili. Entrambi i metodi di filtraggio dei pacchetti si servono di una serie di regole che operano all'interno del kernel di Linux per decidere cosa fare con i pacchetti che corrispondono alla regola specificata oppure ad un set di regole. Tuttavia, iptables offre un modo molto più estensibile per filtrare i pacchetti, fornendo all'amministratore un livello di controllo maggiore senza, però, aggiungere eccessiva complessità al sistema.

Se avete familiarità con ipchains, prima di avventurarvi nell'utilizzo di iptables assicuratevi di avere ben presenti le seguenti differenze tra i due metodi:

- *Sotto iptables, ogni pacchetto filtrato viene elaborato usando le regole di una sola catena invece di catene multiple.* Per esempio, un pacchetto FORWARD che entra in un sistema usando ipchains deve passare attraverso le catene INPUT, FORWARD e OUTPUT per poter arrivare a destinazione. iptables, invece, invia i pacchetti alla catena INPUT solo se sono destinati al sistema locale e li invia alla catena OUTPUT solo se sono stati generati dal sistema locale. Per questa ragione, è importante posizionare la regola creata per catturare un pacchetto particolare, all'interno della regola che gestisce il pacchetto.
- *Il target DENY è stato cambiato in DROP.* In ipchains, ai pacchetti che soddisfavano una certa regola di una catena poteva essere assegnato il target DENY per fare in modo che venissero abbandonati. Per ottenere lo stesso effetto in iptables è stato necessario cambiare il target in DROP.
- *L'ordine è importante quando si devono collocare delle opzioni in una regola.* Con ipchains, l'ordine che viene assegnato alle varie opzioni non ha molta importanza. Il comando iptables usa una sitassi più rigida. Nei comandi iptables dovete specificare la porta sorgente o di destinazione prima aver specificato il protocollo (ICMP, TCP o UDP).
- *Quando specificate le interfacce di rete da associare a una regola, dovete usare solo interfacce di ingresso (opzione -i) con le catene INPUT o FORWARD e solo interfacce di uscita (opzione -o) con le catene FORWARD o OUTPUT.* Questo è necessario in quanto le catene OUTPUT non vengono più utilizzate dalle interfacce di ingresso e le catene INPUT non interessano i pacchetti che si muovono attraverso le interfacce di uscita.

Questo elenco presenta solo una parte dei cambiamenti apportati, anche perchè il filtro iptables è stato sostanzialmente riscritto. Per informazioni più specifiche, consultate *Linux Packet Filtering HOWTO* nella Sezione 18.7.

18.3. Opzioni utilizzate all'interno dei comandi iptables

Le regole per il filtraggio dei pacchetti vengono adottate usando il comando iptables. In questo contesto occorre utilizzare i seguenti aspetti del pacchetto come criterio di base:

- *Tipo di pacchetto* — Indica quale tipo di pacchetto viene filtrato dal comando.
- *Fonte del pacchetto/destinazione* — Indica al comando quali pacchetti filtrare in base alla loro fonte o destinazione.
- *Target* — Indica quali azioni vengono adottate sui pacchetti che rispondono ai criteri sopra elencati.

Per maggiori informazioni su opzioni specifiche le quali indirizzano questi apetti, consultare la Sezione 18.3.4 e la Sezione 18.3.5.

Perchè una regola iptables sia valida, le opzioni ad essa applicate devono essere raggruppate in modo logico, in base allo scopo e alle condizioni delle regole in generale. Il remainder di questa sezione spiega le opzioni usate più comunemente per il comando iptables.

18.3.1. Struttura delle opzioni di iptables

Molti comandi di iptables presentano la struttura seguente:

```
iptables [-t <table-name>] <command> <chain-name> <parameter-1> \
         <option-1> <parameter-n> <option-n>
```

L'opzione <*nome-tabella*> permette all'utente di selezionare una tabella diversa da quella di default filter da utilizzare con il comando. L'opzione <*comando*> ordina un'azione specifica da eseguire, come per esempio aggiungere o cancellare un regola specificata dall'opzione <*nome-catena*>. Questa opzione è seguita da coppie di parametri e opzioni che definiscono cosa accade quando un pacchetto corrisponde alla regola.

Guardando alla struttura di un comando iptables, è importante ricordare che, diversamente dalla maggior parte degli altri comandi, la lunghezza e la complessità di un comando iptables possono cambiare a seconda dello scopo prefisso. Un semplice comando per rimuovere una regola da una catena può essere molto corto, mentre un comando creato per filtrare pacchetti da una determinata sottorete per mezzo di parametri e opzioni particolari può raggiungere una discreta lunghezza. Nel creare comandi iptables, è utile tener presente che l'impiego di alcuni parametri e di alcune opzioni può richiedere la necessità per altri parametri e opzioni, di specificare in modo più dettagliato la precedente richiesta di opzione. Per creare una regola valida, dovete continuare in questo modo finchè non avrete soddisfatto tutti i parametri e tutte le opzioni in questione.

Per visualizzare un elenco completo delle strutture del comando iptables, digitate iptables -h.

18.3.2. Opzioni di comando

Le opzioni di comando indicano a iptables di svolgere un'azione specifica. Per ogni comando iptables è permesso solo una opzione di comando. Fatta eccezione per il comando help, tutti i comandi sono scritti con i caratteri maiuscoli.

I comandi di iptables sono i seguenti:

- -A — Aggiunge la regola iptables alla fine della catena specificata. Questo comando viene utilizzato per aggiungere semplicemente una regola, nei casi in cui l'ordine delle regole nella catena non ha importanza.
- -C — verifica una particolare regola prima di aggiungerla alla catena specificata dall'utente. Questo comando vi può aiutare nella creazione di regole di iptables complicate, indicandovi di volta in volta i parametri e le opzioni da aggiungere.
- -D — Cancella una regola da una determinata catena in base al numero (per esempio il 5 per cancellare la quinta regola contenuta nella catena). Potete anche digitare l'intera regola e iptables cancellerà la regola nella catena corrispondente.
- -E — Rinomina una catena definita dall'utente, senza intaccare la struttura della tabella.
- -F — svuota la catena selezionata, cancellando di fatto tutte le regole in essa contenute. Se non viene specificata alcuna catena, questo comando cancella tutte le regole di ogni catena.
- -h — Fornisce un elenco di strutture di comando molto utili e un breve compendio di parametri e opzioni.
- -I — Inserisce una nuova regola in un determinato punto specificato da un valore intero definito dall'utente. Se non specificate alcun numero, iptables inserirà il vostro comando all'inizio della catena.

Attenzione

Quando utilizzate l'opzione `-A` o `-I` siate a conoscenza che le regole all'interno di una catena sono importanti per determinare quali regole vengono applicate in base al pacchetto.

- `-L` — elenca tutte le regole contenute nella catena specificata dopo il comando. Per ottenere un elenco di tutte le regole di tutte le catene contenute nella tabella di default `filter`, non specificate alcuna catena o tabella. Per elencare tutte le regole di una specifica catena contenuta in una determinata tabella, dovete utilizzare la seguente sintassi:
  `iptables -L <chain-name> -t <table-name>`

  All'interno della Sezione 18.3.6, troverete la descrizione per le opzioni aggiuntive per l'opzione del comando `-L` che, tra l'altro, fornisce i numeri delle regole e consente descrizioni più complesse.
- `-N` — crea una nuova catena con un nome specificato dall'utente.
- `-P` — Imposta la policy di default per una determinata catena, così se un pacchetto arriva alla fine di una catena e nessuna delle regole è stata soddisfatta, il pacchetto stesso viene inviato al target specificato, come ad esempio ACCEPT o DROP.
- `-R` — Sostituisce una regola presente in una catena specificata. Dopo il nome della catena dovete inserire il numero della regola da sostituire. La prima regola presente in una catena corrisponde alla regola numero uno.
- `-X` — cancella una catena specificata dall'utente. In nessun caso è permesso cancellare una catena integrata di una tabella.
- `-Z` — Azzera i contatori byte e dei pacchetti in tutte le catene per una determinata tabella.

18.3.3. Opzioni del parametro `iptables`

Dopo aver specificato certi comandi di `iptables`, compresi quelli utilizzati per aggiungere, cancellare, inserire o sostituire delle regole all'interno di una determinata catena, vi occorrono alcuni parametri per procedere con la creazione della regola di filtraggio dei pacchetti.

- `-c` — azzera i contatori per una particolare regola. Questo parametro accetta le opzioni `PKTS` e `BYTES` per specificare quale contatore azzerare.
- `-d` — Imposta l'hostname di destinazione, l'indirizzo IP o la rete di un pacchetto che corrisponde alla regola. Nello specificare una rete, i seguenti formati di indirizzo IP/maschera di rete sono supportati:
  - *N.N.N.N/M.M.M.M* — Dove *N.N.N.N* é la portata dell'indirizzo IP e *M.M.M.M* é la maschera di rete.
  - *N.N.N.N/M* — Dove *N.N.N.N* é la portata dell'indirizzo IP e *M* é la bitmask.
- `-f` — fa sì che questa regola sia valida solo per i pacchetti frammentati.

  Usando il punto esclamativo (`!`) dopo questo parametro, solo i pacchetti non frammentati vengono soddisfatti.
- `-i` — Serve per impostare l'interfaccia di rete per i pacchetti in ingresso (per esempio `eth0` o `ppp0`), da utilizzare con una particolare regola. Con `iptables`, questo parametro opzionale può essere utilizzato solo per le catene INPUT e FORWARD se si opera nella tabella `filter` e con la catena PREROUTING se si opera nelle tabelle `nat` e `mangle`.

  Questo parametro supporta anche le seguenti opzioni speciali:
  - Punto esclamativo (`!`) — Inverte la direttiva, ciò significa che ogni interfaccia specificata viene esclusa da questa regola.

- Segno più (+) — Un carattere wildcard che viene usato per indicare tutte le interfacce che corrispondono a una determinata stringa. Per esempio, il parametro -i eth+ applica questa regola a tutte le interfacce ethernet ma esclude qualsiasi altra interfaccia, per esempio ppp0.

Se utilizzate il parametro -i senza specificare alcuna interfaccia, la regola riguarderà tutte le interfacce.

- -j — Salta direttamente su di un target specifico quando un pacchetto soddisfa una certa regola. Target validi da utilizzare dopo l'opzione -j includono le opzioni standard (ACCEPT, DROP, QUEUE e RETURN) e anche opzioni estese reperibili attraverso i moduli caricati per default con il pacchetto RPM iptables di Red Hat Enterprise Linux per esempio, LOG, MARK e REJECT, per citarne alcune. Per maggiori informazioni consultate la pagina man di iptables.

  Potete anche indirizzare un pacchetto che soddisfa questa regola ad una catena definita dall'utente al di fuori della catena attuale, questo vi permette di utilizzare altre regole per il controllo di tale pacchetto

  Se non viene specificato alcun target, il pacchetto oltrepassa la regola senza che succeda nulla. Tuttavia, il contatore per questa regola sale di una unità.

- -o — Serve per impostare l'interfaccia di rete per i pacchetti in uscita, da utilizzare con un regola. Può essere usato solo con le catene OUTPUT e FORWARD se si opera nella tabella filter e con la catena POSTROUTING se si opera nelle tabelle nat e mangle. Le opzioni di questo parametro sono le stesse del parametro relativo all'interfaccia di rete per i pacchetti in ingresso (-i).

- -p — Imposta il protocollo IP per la regola, che può essere icmp, tcp, udp o all, per coprire ogni possibile protocollo. Inoltre, si possono utilizzare anche altri protocolli meno diffusi, di cui è disponibile un elenco in /etc/protocols. Se non viene specificata questa opzione durante la creazione della regola, l'opzione di default è all.

- -s — Imposta l'indirizzo sorgente per un particolare pacchetto, utilizzando la stessa sintassi del parametro di destinazione (-d).

18.3.4. Opzioni di corrispondenza iptables

Diversi protocolli di rete forniscono speciali opzioni di corrispondenza configurabili in modo particolare per corrispondere a un determinato pacchetto che utilizza, appunto, uno di quei protocolli. Tuttavia, bisogna prima specificare il protocollo nel comando iptables, per esempio usando -p tcp<*nome-protocollo*>, (dove <*nome-protocollo*> é il protocollo target), per rendere disponibili le opzioni relative a quel protocollo.

18.3.4.1. Protocollo TCP

Le opzioni speciali disponibili per il protocollo TCP (-p tcp) sono:

- --dport — definisce la porta di destinazione per il pacchetto. Per configurare questa opzione, potete usare il nome di un servizio di rete (come www o smtp), un numero di porta o una gamma di numeri della porta. Nel file /etc/services potete trovare i nomi e gli alias dei servizi di rete e i numeri della porta utilizzati. Per specificare questa opzione potete usare anche --dport.

  Per indicare una specifica gamma di numeri della porta, scrivete i due numeri separati dai due punti (:), per esempio potete specificare -p tcp --dport 3000:3200. La gamma massima consentita è 0:65535.

  Potete anche utilizzare il punto esclamativo (!), dopo l'opzione --dport, per far corrispondere tutti i pacchetti che *non* utilizzano quel servizio di rete o quella porta.

- --sport — determina la porta sorgente del pacchetto, utilizzando le stesse opzioni di --dport. Per specificare questa opzione potete usare anche --source-port.

- `--syn` — rende la regola applicabile a tutti i pacchetti TCP adibiti all'apertura di una connessione (più noti come *pacchetti SYN*). Il punto esclamativo (`!`) posto come flag dopo l'opzione `--syn` indica che devono essere esaminati tutti pacchetti non SYN.
- `--tcp-flags` — Permette di filtrare i pacchetti TCP con una gamma di bit specifica o flag, impostati per soddisfare una regola. L'opzione `--tcp-flags` accetta due parametri. Il primo parametro è la maschera, che imposta i flag da esaminare nel pacchetto. Il secondo parametro si riferisce al flag che deve essere impostato per poter corrispondere correttamente.

  I flag possono essere:

  - `ACK`
  - `FIN`
  - `PSH`
  - `RST`
  - `SYN`
  - `URG`
  - `ALL`
  - `NONE`

  Per esempio, una regola di `iptables` contenente l'opzione `-p tcp --tcp-flags ACK,FIN,SYN SYN` corrisponde solo ai pacchetti TCP in cui è impostato il flag SYN, ma non i flag ACK e FIN.

  Il punto esclamativo (`!`) posto dopo `--tcp-flags` viene utilizzato per invertire l'effetto dell'opzione di corrispondenza (match)
- `--tcp-option` — cerca la corrispondenza con un particolare pacchetto in cui sono impostate delle opzioni TCP specifiche. Anche in questo caso si può invertire l'effetto mediante il punto esclamativo (`!`).

18.3.4.2. Protocollo UDP

Le opzioni estese disponibili per il protocollo UDP (`-p udp`) sono:

- `--dport` — Specifica la porta di destinazione del pacchetto UDP, usando il nome del servizio, un numero di porta o una gamma di numeri della porta. L'opzione di corrispondenza `--destination-port` é sinonimo di `--dport`.
- `--sport` — Specifica la porta sorgente del pacchetto UDP, utilizzando il nome del servizio, il numero della porta oppure una gamma di numeri.L'opzione di corrispondenza `--source-port` è sinonimo di`--port`.

18.3.4.3. Protocollo ICMP

Le seguenti opzioni di corrispondenza sono disponibili per l'Internet Control Message Protocol (ICMP) (`-p icmp`):

- `--icmp-type` — Imposta il nome o il numero del tipo di ICMP che soddisfa la regola. Potete riprendere un elenco di nomi ICMP validi digitando il comando `iptables -p icmp -h`.

18.3.4.4. Moduli con opzioni di corrispondenza aggiuntivi

Ulteriori opzioni speciali, si possono reperire attraverso i moduli che si caricano tramite il comando `iptables`. Per usare uno di questi moduli, dovete caricarlo per nome inserendo l'opzione `-m <nome-modulo>` (sostituendo `<module-name>` con il nome del modulo).

Molti di questi moduli sono disponibili per default. Potete persino creare moduli aggiuntivi per ottenere funzionalità aggiuntive.

Il seguente elenco riporta i moduli più comunemente usati:

- Il modulo `limit` — Vi consente di porre un limite al numero di pacchetti che soddisfano una certa regola. Questo risulta particolarmente utile insieme con il target `LOG` per ridurre la quantità di pacchetti da esaminare, onde impedire l'arrivo di un'ondata di messaggi di log e un consumo eccessivo di risorse di sistema. Consultare la Sezione 18.3.5 per maggiori informazioni sul target `LOG`.

  Il modulo `limit` abilita le seguenti opzioni:

  - `--limit` — Stabilisce il numero massimo di confronti da effettuare sui pacchetti in un determinato campo a di tempo, specificato da un numero e da una unità di tempo nel formato `<numero>/<tempo>`. Per esempio, utilizzando `--limit 5/hour` indica che in un'ora sono consentiti al massimo `5`confronti.

    Se il numero e l'unità di tempo non vengono specificati, il valore predefinito è `3/hour`.

  - `--limit-burst` — impone un limite al numero di pacchetti che possono soddisfare una determinata regola. Questa opzione va associata all'opzione `--limit` e può essere associata a un numero per impostare il limite sopracitato.

    Se non viene specificato alcun numero, soltanto cinque pacchetti potranno soddisfare tale regola.

- Il modulo `state` — Abilita la corrispondenza dello stato.

  Il modulo `state` abilita le seguenti opzioni:

  - Il modulo `--state` — prende in considerazione pacchetti con i seguenti stati di connessione:
    - `ESTABLISHED` — il pacchetto è associato ad altri pacchetti in una connessione stabilita.
    - `INVALID` — il pacchetto non corrisponde ad alcuna connessione conosciuta.
    - `NEW` — il pacchetto sta creando una nuova connessione oppure fa parte di una connessione bidirezionale non vista in precedenza.
    - `RELATED` — il pacchetto sta creando una nuova connessione in qualche modo legata a una connessione esistente.

    Questi stati di connessione possono essere combinati tra loro e usati in contemporanea. Occorre scriverli separati da una virgola, come in questo esempio: `-m state --state INVALID,NEW`.

- Il modulo `mac` — Abilita la corrispondenza dell'indirizzo dell'hardware MAC.

  Il modulo `mac` abilita la seguente opzione:

  - `--mac-source` — É il corrispondente di un indirizzo MAC della scheda dell'interfaccia di rete che ha inviato il pacchetto. Per escludere un indirizzo MAC da una regola, posizionare un punto esclamativo (`!`) dopo l'opzione `--mac-source`.

Per conoscere le altre opzioni aggiuntive reperibili attraverso i moduli, consultate la pagina man di `iptables`.

18.3.5. Opzioni relative ai target

Vi sono molti target attribuibili a un pacchetto dopo che ha soddisfato una determinata regola. Il loro compito è quello di decidere che cosa fare del pacchetto e di svolgere, se necessario, ulteriori operazioni, come per esempio registrare l'azione. Inoltre, ogni catena ha un suo target di default, che entra in gioco nel caso in cui un pacchetto non soddisfi nessuna delle regole in essa contenute o quando nessuna della regole che il pacchetto ha soddisfato specificano un target.

Ecco riportati i target standard:

- *<catena-definita-dall'utente>* — Sostituire *<catena-definita-dall'utente>* con il nome di una catena all'interno di questa tabella. Questo target invia il pacchetto alla catena del target.
- `ACCEPT` — autorizza il pacchetto a procedere verso la propria destinazione o verso un'altra catena.
- `DROP` — Abbandona il pacchetto, senza informare il richiedente. Il sistema che ha inviato il pacchetto non riceve alcun messaggio di mancata accettazione.
- `QUEUE` — accoda il pacchetto verso lo spazio utente.
- `RETURN` — arresta il controllo del pacchetto mediante le regole della catena corrente. Se un pacchetto con target `RETURN` soddisfa una regola contenuta in una catena chiamata da un'altra catena, allora viene rimandato alla prima catena, dove la regola riprende il controllo da dove l'aveva lasciato. Se la regola `RETURN` è utilizzata all'interno di una catena integrata e il pacchetto non può tornare alla catena precedente, il target predefinito per la catena corrente decide quale azione intraprendere.

In aggiunta a questi target standard vi sono altri target che si possono utilizzare con delle estensioni chiamate *moduli dei target*. Per maggiori informazioni in merito a questi ultimi, consultate la Sezione 18.3.4.4.

Vi sono numerose estensioni di moduli del target, molte delle quali si adattano solo a specifiche tabelle o situazioni. Quelli che seguono sono due dei moduli di target più diffusi, inclusi per default in Red Hat Enterprise Linux:

- `LOG` — Registra tutti i pacchetti che soddisfano questa regola. Poiché i pacchetti sono registrati dal kernel, il file `/etc/syslog.conf` determina dove vengono memorizzate queste voci di log (per default, nel file `/var/log/messages`.

  Dopo il target `LOG` si possono usare varie opzioni per determinare il modo in cui deve avvenire la registrazione:

  - `--log-level` — Stabilisce il livello di logging dell'evento.Potete trovare un elenco dei livelli di priorità nella pagina man `syslog.conf`.
  - `--log-ip-options` — Vengono registrate tutte le opzioni impostate nell'intestazione di un pacchetto IP.
  - `--log-prefix` — Antepone una stringa che puó arrivare fino a 29 caratteri. É utile anche per scrivere filtri per il syslog da usare insieme alla registrazione dei pacchetti.
  - `--log-tcp-options` — Vengono registrate tutte le opzioni impostate nell'intestazione di un pacchetto TCP.
  - `--log-tcp-sequence` — scrive nel log il numero di sequenza TCP per il pacchetto.

- `REJECT` — Rispedisce un pacchetto di errore al sistema che l'ha inviato, dopodiché abbandona il pacchetto (DROP).

  Il target `REJECT` accetta `--reject-with` *<tipo>* (dove *<tipo>* é il tipo di rigetto) il quale abilita più informazioni dettagliate da ritornare al pacchetto di errore. Il messaggio `port-unreachable` è il default del*<tipo>* di errore fornito quando non viene usata un altra

opzione. Per ottenere un elenco completo delle opzioni <*tipo*> disponibili, consultate la pagina man di iptables.

Sempre nella pagina man di iptables potete trovare altre estensioni di target, tra cui alcune molto utili per eseguire il masquerading mediante la tabella nat o per alterare i pacchetti mediante la tabella mangle.

18.3.6. Elenco delle opzioni

Il comando elenco di default, iptables -L, fornisce una panoramica di base delle catene di regole correnti della tabella predefinita filter. Altre opzioni consentono di ottenere ulteriori informazioni:

- -v — Visualizza output complessi, come per esempio il numero di pacchetti e di byte che hanno attraversato ciascuna catena, il numero di pacchetti e di byte che hanno soddisfatto ciascuna regola e le interfacce disponibili per quella regola.
- -x — espande i numeri fino a visualizzare il loro valore esatto. Se il sistema è occupato, il contatore di pacchetti e byte relativo a una certa catena mostra un output abbreviato, ponendo K (per le migliaia), M (per i milioni) o G (per i miliardi) alla fine del numero. Questa opzione impone la visualizzazione completa del numero.
- -n — visualizza gli indirizzi IP e i numeri di porta in formato numerico invece che nel formato di default (con hostname e servizio di rete).
- --line-numbers — Elenca le regole contenute in ogni catena vicino al loro ordine numerico. Questa opzione è utile se si vuole cancellare una specifica regola in una catena o stabilire in quale posizione della catena inserire una certa regola.
- -t — Specifica un nome della tabella.

18.4. Come salvare le regole iptables

Le regole create mediante il comando iptables vengono conservate solo nella memoria. Se il sistema viene riavviato prima di aver salvato l'impostazione della regola di iptables, tutte le regole verranno perdute. Per poter rendere effettive le regole netfilter attraverso il riavvio del sistema, esse devono essere salvate. Per fare ció, effettuare un log in come root e digitare:

```
/sbin/service iptables save
```

In questo modo initscript iptables viene eseguito, il quale a sua volta esegue il programma /sbin/iptables-save e salva la configurazione corrente di iptables nel file /etc/sysconfig/iptables. Il file /etc/sysconfig/iptables esistente viene salvato come /etc/sysconfig/iptables.save.

Quando il sistema effettua nuovamente un avvio, lo script init iptables applicherá le regole salvate in /etc/sysconfig/iptables usando il comando /sbin/iptables-restore.

È sempre consigliabile testare una nuova regola di iptables prima di salvarla nel file /etc/sysconfig/iptables; è anche possibile copiare in questo file delle regole di iptables provenienti dal file /etc/sysconfig/iptables di un altro sistema. Questo vi consente di distribuire vari gruppi di regole iptables a molti sistemi diversi.

Importante

Se distribuite il file /etc/sysconfig/iptables su altre macchine, per rendere effettive le nuove regole dovete digitare /sbin/service iptables restart.

18.5. Script di controllo di iptables

Ci sono due metodi di base per il controllo di iptables sotto Red Hat Enterprise Linux:

- **Strumento di configurazione del livello di sicurezza** (system-config-securitylevel) — Una interfaccia grafica per la creazione, l'attivazione, e il salvataggio delle regole di base del firewall. Per maggiori informazioni su come usare questo tool, consultare il capitolo *Configurazione del firewall di base* nella *Red Hat Enterprise Linux System Administration Guide*.
- /sbin/service iptables <*opzione*> — Un comando emesso dall'utente root capace di attivare, disattivare ed effettuare altre funzioni di iptables attraverso il proprio script init. Sostituire <*opzione*> nel comando, con una delle seguenti direttive:
  - start — Se è configurato un firewall (ciò significa se esiste /etc/sysconfig/iptables), tutti gli iptables in esecuzione vengono arrestati completamente e avviati successivamente usando il comando /sbin/iptables-restore. La direttiva start funzionerà solo se il modulo del kernel ipchains non è caricato.
  - stop — Se un firewall è in esecuzione, le regole del firewall presenti in memoria vengono cancellate, e tutti i moduli iptables e helper vengono scaricati.

    Se la direttiva IPTABLES_SAVE_ON_STOP all'interno del file di configurazione /etc/sysconfig/iptables-config è cambiata in yes rispetto al suo valore di default, le regole correnti vengono salvate su /etc/sysconfig/iptables e qualsiasi regola esistente viene spostata sul file /etc/sysconfig/iptables.save.

    Consultate la Sezione 18.5.1 per maggiori informazioni sul file iptables-config.
  - restart — Se un firewall è in esecuzione, le regole del firewall vengono cancellate, e lo stesso viene avviato nuovamente se configurato in /etc/sysconfig/iptables. La direttiva restart funziona solo se il modulo del kernel ipchains non è caricato.

    Se la direttiva IPTABLES_SAVE_ON_RESTART all'interno del file di configurazione /etc/sysconfig/iptables-config è cambiata in yes rispetto al suo valore di default, le regole correnti vengono salvate su /etc/sysconfig/iptables e qualsiasi regola esistente viene spostata sul file /etc/sysconfig/iptables.save.

    Consultate la Sezione 18.5.1 per maggiori informazioni sul file iptables-config.
  - status — Mostra sul prompt della shell lo stato del firewall e un elenco delle regole attive. Se nessuna regola del firewall viene caricata o configurata, esso viene indicato eseguendo questo comando.

    Un elenco di regole attive contenenti l'indirizzo IP all'interno delle regole elencate, a meno che il valore di default per IPTABLES_STATUS_NUMERIC sia cambiato in no all'interno del file di configurazione /etc/sysconfig/iptables-config. Ciò modifica l'output in informazioni riguardanti l'hostname ed il dominio. Consultate la Sezione 18.5.1 per maggiori informazioni sul file iptables-config.
  - panic — Elimina tutte le regole del firewall. La policy di tutte le tabelle configurate è impostata su DROP.
  - save — Salva le regole del firewall su /etc/sysconfig/iptables usando iptables-save. Consultare la Sezione 18.4 per maggiori informazioni.

Suggerimento

Per usare gli stessi comandi initscript per controllare netfilter per IPv6, sostituire `ip6tables` per `iptables` nei comandi `/sbin/service` elencati in questa sezione. Per maggiori informazioni su IPv6 e netfilter, consultare la Sezione 18.6.

18.5.1. File di configurazione degli script di controllo di `iptables`

Il comportamento degli initscript `iptables` è controllato dal file di configurazione `/etc/sysconfig/iptables-config`. Il seguente rappresenta un elenco delle direttive contenute all'interno di questo file:

- `IPTABLES_MODULES` — Specifica un elenco di moduli `iptables` aggiuntivi, separato da uno spazio vuoto, da caricare quando un firewall viene attivato. Questo può includere il controllo del collegamento e gli helper NAT.
- `IPTABLES_MODULES_UNLOAD` — Scarica i moduli durante il processo di avvio o di arresto. Questa direttiva accetta i seguenti valori:
  - `yes` — Il valore di default. Questa opzione deve essere impostata per poter ottenere uno stato corretto durante l'avvio o l'arresto di un firewall.
  - `no` — Questo valore deve essere impostato solo se si verificano alcuni problemi durante il processo di scaricamento dei moduli netfilter.

- `IPTABLES_SAVE_ON_STOP` — Salva le regole del firewall corrente su `/etc/sysconfig/iptables` quando il firewall viene arrestato. Questa direttiva accetta i seguenti valori:
  - `yes` — Salva le regole esistenti su `/etc/sysconfig/iptables` quando il firewall viene arrestato, spostando la versione precedente sul file `/etc/sysconfig/iptables.save`.
  - `no` — Il valore di default. Non salva le regole esistenti quando il firewall viene arrestato.

- `IPTABLES_SAVE_ON_RESTART` — Salva le regole del firewall correnti quando il firewall viene riavviato. Questa direttiva accetta i seguenti valori:
  - `yes` — Salva le regole esistenti su `/etc/sysconfig/iptables` quando il firewall viene riavviato, spostando la versione precedente sul file `/etc/sysconfig/iptables.save`.
  - `no` — Il valore di default. Non salva le regole esistenti quando il firewall viene avviato nuovamente.

- `IPTABLES_SAVE_COUNTER` — Salva e ripristina tutti i contatori del byte e del pacchetto in tutte le catene e le regole. Questa direttiva accetta i seguenti valori:
  - `yes` — Salva i valori del contatore.
  - `no` — Il valore di default. Non salva i valori del contatore.

- `IPTABLES_STATUS_NUMERIC` — Esegue un output degli indirizzi IP in un output dello stato invece di un dominio o di hostname. Questa direttiva accetta i seguenti valori:
  - `yes` — Il valore di default. Ritorna solo gli indirizzi IP all'interno dell'output dello stato.
  - `no` — Ritorna il dominio o gli hostname all'interno di un output.

18.6. ip6tables e IPv6

Se il pacchetto iptables-ipv6 è installato, netfilter sotto Red Hat Enterprise Linux è in grado di filtrare la generazione successiva di protocollo Internet IPv6. Il comando usato per manipolare il netfilter IPv6 è ip6tables. Molte direttive per questo comando, sono identiche a quelle usate per iptables, ad eccezione della tabella nat che non è ancora supportata. Questo significa che non è ancora possibile effettuare compiti di traduzione dell'indirizzo di rete IPv6 , come ad esempio masquerading e la ridirezione del traffico da una porta di un host a un'altra (port forwarding).

Le regole salvate per ip6tables sono conservate nel file /etc/sysconfig/ip6tables. Le vecchie regole salvate dagli initscript ip6tables sono salvate nel file /etc/sysconfig/ip6tables.save.

Il file di configurazione per initscript ip6tables è /etc/sysconfig/ip6tables-config ed i nomi per ogni direttiva variano leggermente. Per esempio, la direttiva iptables-config IPTABLES_MODULES è IP6TABLES_MODULES nel file ip6tables-config.

18.7. Risorse aggiuntive

Per maggiori informazioni circa il filtraggio di pacchetti con iptables, consultate le fonti riportate qui di seguito.

18.7.1. Documentazione installata

- man iptables — Contiene la descrizione di iptables e un elenco completo di target, opzioni e delle corrispondenze delle estensioni.

18.7.2. Siti Web utili

- http://www.netfilter.org/ — La home del progetto netfilter/iptables. Contiene informazioni su iptables, tra cui una sezione FAQ relativa ai problemi specifici che potete incontrare, e svariate guide molto utili a cura di Rusty Russel, il responsabile dell'implementazione del firewall IP di Linux. I documenti HOWTO contenuti in questo sito si occupano di argomenti quali i concetti di base relativi al networking, le configurazioni di NAT e del filtraggio dei pacchetti con il kernel.
- http:// www.linuxnewbie.org/nhf/Security/IPtables_Basics.html — Una descrizione essenziale e generica di come si muovono i pacchetti attraverso il kernel di Linux e un'introduzione su come creare semplici comandi di iptables.
- http://www.redhat.com/support/resources/networking/firewall.html — Contiene link aggiornati a numerose risorse di filtraggio dei pacchetti.
- *Red Hat Enterprise Linux Security Guide*; Red Hat, Inc. — Contiene un capitolo sul ruolo dei firewall all'interno di una strategia di sicurezza e sulle strategie per la creazione delle regole del firewall.
- *Red Hat Enterprise Linux System Administration Guide*; Red Hat, Inc. — Contiene un capitolo sulla configurazione dei firewall usando **Strumento di configurazione del livello di sicurezza**.

Capitolo 19.

Kerberos

Il sistema di sicurezza e l'integrità all'interno di una rete possono rappesentare un problema complesso. Numerosi amministratori possono essere impegnati per controllare i servizi eseguiti su di una rete e il modo con il quale essi vengono usati. L'autenticazione di un utente può essere pericolosa se fatta con protocolli insicuri, esempio il trasferimento in chiaro attraverso la rete di una password usando protocolli Telnet e FTP. L'uso di Kerberos può rappresentare un modo per eliminare il bisogno di usare protocolli che permettono l'uso di metodi poco sicuri di autenticazione, aumentandone così la sicurezza di rete.

19.1. Che cos'è Kerberos?

Kerberos è un protocollo di autenticazione dei servizi di rete creato da MIT che si serve della crittografia a chiave segreta [1] per autenticare gli utenti per i servizi di rete — eliminando così la necessità di inviare le password attraverso la rete. Autenticare mediante Kerberos impedisce agli utenti non autorizzati di intercettare le password inviate attraverso la rete.

19.1.1. Vantaggi di Kerberos

La maggior parte dei sistemi di rete convenzionali usa uno schema di autenticazione basato sulle password. Quando un utente effettua una autenticazione per accedere a un server di rete deve fornire un nome utente ed una password. Sfortunatamente, la trasmissione delle informazioni di autenticazione per molti servizi non é criptata. Per essere sicuri in uno schema di questo tipo, la rete non deve essere accessibile dall'esterno e tutti i computer e gli utente sulla rete, devono essere fidati.

Anche in questo caso, una volta che una rete è collegata a Internet, non si potrà più assumere che la rete sia sicura. Qualunque aggressore che ha accesso alla rete e che può utilizzare un analizzatore di pacchetti di rete (solitamente chiamato packet sniffer) può intercettare le password e i nomi utente che attraversano la rete, compromettendo cosí gli account dell'utente e l'integritá della sicurezza dell'infrastruttura.

Lo scopo principale di Kerberos è quello di eliminare la trasmissione delle informazioni di autenticazione attraverso la rete. Il corretto utilizzo di Kerberos vi permette di ridurre drasticamente la possibilità di intercettazione da parte dei packet sniffer.

19.1.2. Svantaggi di Kerberos

Tramite Kerberos si riesce a proteggere la rete dagli attacchi più comuni. Tuttavia, potrebbe risultare complesso da implementare, per varie ragioni:

- Migrare le password utente da un database delle password di UNIX standard, per esempio `/etc/passwd` o `/etc/shadow`, a quello di Kerberos può essere noioso, in quanto non esiste alcun meccanismo automatico che consenta di fare questo. Per maggiori informazioni a riguardo, consultate la domanda numero 2.23 nella sezione FAQ di Kerberos,

  http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html

1. Un sistema dove sia il client che il server, condividono una chiave comune usata per cifrare e decifrare le comunicazioni di rete

- Kerberos è solo in parte compatibile con il sistema PAM (Pluggable Authentication Modules) usato dalla maggior parte dei server Red Hat Enterprise Linux. Per maggiori informazioni, consultate la Sezione 19.4.
- Kerberos parte dal presupposto che ogni utente sia fidato e che stia usando un host non fidato su di una rete non fidata. Il suo obiettivo principale è di impedire che le password non cifrate vengano inviate attraverso questa rete. Tuttavia, se qualcuno diverso dall'utente effettivo ha accesso fisico a uno degli host, specialmente quello che emette i ticket usati per l'autenticazione —, chiamato *key distribution center* (*KDC*) —l'intero sistema di autenticazione di Kerberos è a rischio.
- Affinchè una applicazione possa usare Kerberos, è necessario modificare il suo codice sorgente per effettuare le chiamate alle librerie Kerberos. Le applicazioni modificate in questo modo, vengono considerate essere *kerberizzati*. Per alcune applicazioni, questo può essere un pò problematico a causa della misura dell'applicazione o del suo modello. Per altre applicazioni incompatibili, occorre effettuare dei cambiamenti in modo tale che il client e il server possano comunicare. Ed ancora ciò può comportare molta programmazione. Le applicazioni a sorgente chiusa che non supportano Kerberos di default, risultano quelle più problematiche.
- Kerberos è una soluzione che non prevede vie di mezzo. Se decidete di utilizzare Kerberos sulla rete, dovete ricordarvi tutte le password trasferite a un servizio che non lo supporta, poichè l'autenticazione rischia di essere intercettata dai packet sniffer. In questo caso, la rete può ottenere nussun beneficio nell'uso di kerberos. Per proteggere una rete con Kerberos, è necessario che una di essa utilizzi una versione kerberizzata di *tutte* le applicazioni client/server che inviano password non cifrate, oppure è necessario evitare *qualsiasi* applicazione di questo tipo.

19.2. Terminologia di Kerberos

Come ogni altro sistema, anche Kerberos ha una propria terminologia per definire i vari aspetti del servizio. Prima di descriverne il funzionamento, vi elenchiamo i termini utilizzati:

authentication server (AS)

Un server che emette i ticket per un servizio desiderato, che a turno, vengono conferiti agli utenti per l'accesso al servizio. L'AS risponde alle richieste provenienti dai client che non hanno o non inviano credenziali insieme con una richiesta. Viene usato generalmente per ottenere accesso al servizio ticket-granting server (TGS), emettendo un ticket-granting ticket (TGT). AS generalmente viene eseguito sullo stesso host del Key Distribution Center (KDC).

ciphertext

Dati cifrati.

client

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

credenziali

Una serie di credenziali elettroniche temporanee che verificano l'identità di un client per un particolare servizio. Chiamato anche ticket.

credential cache o file del ticket

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

crypt hash

Un hash a senso unico per l'autenticazione degli utenti. Pur essendo più sicuro di dati non cifrati, è comunque piuttosto semplice da decifrare per i cracker più esperti.

GSS-API

Il Generic Security Service Application Program Interface (definito in RFC-2743 pubblicato da Internet Engineering Task Force) rappresenta un insieme di funzioni le quali sono in grado di fornire servizi di sicurezza. Questo API viene usato dai client e dai servizi per la loro rispettiva autenticazione, senza avere una conoscenza specifica di come viene effettuata tale procedura. Se un servizio di rete (come ad esempio cyrus-IMAP) usa GSS-API, esso puó eseguire una autenticazione usando Kerberos.

hash

Un numero generato dal testo e usato per assicurare che i dati trasmessi non siano stati alterati.

key

Dati usati per cifrare e decifrare le informazioni. Le informazioni cifrate non possono essere decifrate senza la chiave corretta o senza un fiuto infallibile.

key distribution center (KDC)

Un servizio che emette i ticket di Kerberos, generalmente eseguito sullo stesso host del ticket granting server (TGS).

keytab (o tabella di conversione)

Un file che contiene un elenco non cifrato di principal e delle chiavi. I server recuperano le chiavi di cui necessitano dai file keytab invece di utilizzare il comando `kinit`. Il file keytab di default é `/etc/krb5.keytab`. Il server di gestione di KDC, `/usr/kerberos/sbin/kadmind`, é l'unico servizio che usa qualsiasi altro file (esso usa `/var/kerberos/krb5kdc/kadm5.keytab`).

`kinit`

Il comando `kinit` permette ad un principal, che ha giá effettuato la registrazione, di ottenere e depositare il ticket granting ticket (TGT) iniziale. Per maggiori informazioni sull'uso del comando `kinit`, controllare la sua pagina man.

principal (o nome principale)

Il principal é il nome unico di un utente o un servizio abilitato per l'autenticazione usando Kerberos. Il nome di un principal ha la seguente forma: `root[/instance]@REALM`. Per un utente tipico il valore root è uguale all'ID di login.`instance` è opzionale. Se il principal presenta una istanza, è separato da root con ("/"). La stringa vuota ("") è una istanza valida (che differisce dall'istanza di default `NULL`), ma il suo utilizzo può causare confusione. Tutti i principal in un realm hanno la propria chiave, essa è derivata da una password o impostata in modo casuale per i servizi.

realm

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

service

Un programma accessibile tramite la rete.

ticket

Una serie di credenziali elettroniche temporanee che verificano l'identità di un client per un particolare servizio. Chiamate anche credenziali.

ticket granting server (TGS)

Un server che emette i ticket per un servizio desiderato, i quali vengono dati a turno, agli utenti per l'accesso al servizio. Solitamente il TGS viene eseguito sullo stesso host del KDC.

ticket granting ticket (TGT)

Un ticket speciale che permette al client di ottenere ulteriori ticket senza richiederli al KDC.

password non criptata

Un testo chiaro, password leggibile.

19.3. Funzionamento di Kerberos

Kerberos differisce dai metodi di autenticazione del tipo nome utente/password perchè invece di eseguire un'autenticazione di ogni utente per ogni servizio di rete, Kerberos utilizza la cifratura simmetrica e un sistema fidato di terze parti, noto come KDC,per autenticare gli utenti per una suite di servizi di rete.Avvenuta l'autenticazione, Kerberos invia un ticket specifico per quella sessione sul computer dell'utente, e tutti i servizi kerberizzati, per effettuare l'autenticazione, invece di chiedere la password all'utente cercheranno direttamente il ticket in questione.

Quando un utente su di una rete kerberizzata si collega alla propria workstation,il suo principal viene inviato al KDC in una richiesta per il TGT da AS. Questa richiesta può essere inviata dal programma di login in modo trasparente o dal programma `kinit` una volta che l'utente ha eseguito il suo log in.

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

Il programma di login sulla macchina client o `kinit` decodifica il TGT utilizzando la chiave (che ricava dalla password dell'utente). La chiave dell'utente é usata solo sul dispositivo del client e *non* é inviata attraverso la rete.

Il TGT scade dopo un determinato periodo (generalmente dieci ore) ed è immagazzinata in una cache delle credenziali del dispositivo del client. La data di scadenza viene impostata in modo che un TGT compromesso possa essere utilizzato solo per un periodo limitato. Una volta emesso il TGT, l'utente non dovrá inserire nuovamente la propria password fino a quando non scadrá il TGT o quando l'utente si scollega per poi collegarsi nuovamente.

Quando un utente ha necessità di accedere ad un servizio di rete, il software del client utilizza il TGT per richiedere al TGS un nuovo ticket per un determinato servizio. Il ticket del servizio verrá usato per autenticare l'utente in modo trasparente nei confronti del servizio specifico stesso.

Attenzione

Il sistema Kerberos può risultare compromesso ogni volta che l'autenticazione di un utente per un servizio che non utilizza Kerberos avviene per mezzo dell'invio di una password di testo. Pertanto, non è consigliato utilizzare servizi che non prevedono Kerberos, come per esempio Telnet e FTP. È invece accettabile l'utilizzo di protocolli cifrati,come i servizi sicuri SSH o SSL, anche se non é ideale.

Chiaramente, la spiegazione sopra riportata non è che una panoramica sul funzionamento dell'autenticazione da parte di Kerberos. Se desiderate approfondire l'argomento, consultate la Sezione 19.7.

Nota Bene

Kerberos dipende da alcuni servizi di rete per poter funzionare correttamente. Kerberos richiede una sincronizzazione approssimativa degli orologi delle macchine sulla rete. Si consiglia, pertanto, di impostare sulla rete un programma di sincronizzazione degli orologi, come per esempio `ntpd`. Per maggiori informazioni su come configurare `ntpd`, controllare `/usr/share/doc/ntp-`*<numero-versione>*`/index.htm` per l'impostazione dei server del Network Time Protocol (sostituire *<numero-versione>* con il numero della versione del pacchetto `ntp` installato sul sistema).

Inoltre, alcuni aspetti di Kerberos si basano sul DNS (Domain Name Service), per questo motivo accertatevi che le entry e gli host DNS presenti sulla rete, siano configurati in modo corretto. Consultate la *Guida degli amministratori di Kerberos V5 System*, presente in formato PostScript e HTML nella directory `/usr/share/doc/krb5-server-`*<numero-versione>* per maggiori informazioni (sostituire *<numero-versione>* con il numero della versione del pacchetto `krb5-server` installato sul sistema).

19.4. Kerberos e PAM

Attualmente, i servizi kerberizzati non utilizzano i Pluggable Authentication Modules (PAM) — i server kerberizzati evitano completamente il sistema PAM. Tuttavia le applicazioni che usano PAM possono comunque utilizzare Kerberos per l'autenticazione se il modulo `pam_krb5` (fornito nel pacchetto `pam_krb5`) è installato. Il pacchetto `pam_krb5` contiene alcuni file d'esempio per la configurazione che consente a servizi quali `login` e `gdm` di autenticare gli utenti e ricavare le credenziali iniziali dalla loro password. Se l'accesso ai server di rete è effettuato sempre tramite servizi kerberizzati o servizi che utilizzano GSS-API, come IMAP, la rete può essere considerata sufficientemente sicura.

Suggerimento

Gli amministratori devono prestare attenzione a non permettere agli utenti di autenticare i servizi di rete usando le password di kerberos. Molti protocolli usati da questi servizi non cifrano la password prima di inviarla attraverso la rete, distruggendo tutti i benefici del sistema kerberos. Per esempio, gli utenti non dovrebbero essere autorizzati ad autenticare usando le proprie password attraverso Telnet.

19.5. Configurazione di un server Kerberos 5

Nel configurare Kerberos, installate prima il server. Se avete necessità di impostare dei server slave, troverete tutti i dettagli su come impostare i rapporti tra server master e server slave nella *Kerberos 5 Installation Guide* all'interno della directory `/usr/share/doc/krb5-server-`*<numero-versione>* (sostituire *<numero-versione>* con il numero della versione del pacchetto `krb5-server` installato sul sistema).

Per configurare un server Kerberos di base, eseguite quanto segue:

1. Assicuratevi che la sincronizzazione dell'orologio e il DNS stiano funzionando su tutte le macchine del server e dei client, prima di configurare Kerberos 5. Prestate particolare attenzione alla sincronizzazione tra il server Kerberos e i suoi client. Se gli orologi del server e del client differiscono di oltre cinque minuti (in kerberos 5 è possibile impostare un intervallo di tempo predefinito), i client Kerberos non potranno essere autenticati. La sincronizzazione degli orologi è importante per impedire a eventuali aggressori di utilizzare un vecchio ticket di Kerberos per farsi passare come utente valido.

Si consiglia di impostare una rete client/server compatibile con Network Time Protocol (NTP), anche se non si sta utilizzando Kerberos. Red Hat Enterprise Linux comprende il pacchetto `ntp`, per questo scopo. Consultate `/usr/share/doc/ntp-<numero-versione>/index.htm` per informazioni su come impostare i server Network Time Protocol e http://www.eecis.udel.edu/~ntp per informazioni aggiuntive su NTP.

2. Installate i pacchetti `krb5-libs`, `krb5-server` e `krb5-workstation` sulla macchina su cui verrà eseguito il vostro KDC. Tale dispositivo deve essere molto protetto — se possibile, non eseguite altri servizi al di fuori di KDC.

   Se è necessario utilizzare una interfaccia grafica per gestire Kerberos, dovete installare anche il pacchetto `gnome-kerberos`. Essocontiene `krb5`, un tool grafico della GUI per la gestione di ticket.

3. Modificate i file di configurazione `/etc/krb5.conf` e `/var/kerberos/krb5kdc/kdc.conf` per riflettere il nome del realm e le mappature del dominio al realm. Si può creare un realm semplice sostituendo l'istanza di *`EXAMPLE.COM`* e *`example.com`* con il vostro nome di dominio corretto — facendo attenzione al formato delle lettere, maiuscole e le minuscole,— cambiando il KDC da *`kerberos.example.com`* al nome del server Kerberos. Per convenzione, tutti i nomi di realm sono scritti in lettere maiuscole mentre tutti gli hostname DNS e i nomi di dominio sono in formato minuscolo. Per maggiori dettagli sul formato di questi file consultate le rispettive pagine man.

4. Create il database tramite l'utility `kdb5_util` al prompt della shell:
   ```
   /usr/kerberos/sbin/kdb5_util create -s
   ```

   Il comando `create` crea il database che sarà utilizzato per conservare le chiavi per il realm Kerberos. L'interruttore `-s` impone la creazione di un file *stash* che conserverà la chiave del server master. Se non esiste alcun file stash da cui leggere la chiave, a ogni avvio il server Kerberos (`krb5kdc`) richiederà all'utente la password del server master (utilizzabile per rigenerare la chiave).

5. Modificate il file `/var/kerberos/krb5kdc/kadm5.acl`. Questo file è utilizzato da `kadmind` per stabilire quali principal hanno accesso amministrativo al database di Kerberos nonchè al loro livello di accesso. Generalmente, sarà sufficiente una sola riga:
   ```
   */admin@EXAMPLE.COM  *
   ```

   La maggior parte degli utenti saranno rappresentati nel database, da un solo principal (con una istanza *NULL*, o vuota, come per esempio *joe@EXAMPLE.COM*). Con questa configurazione gli utenti che hanno un secondo principal con un esempio di *admin* (per esempio, *joe/admin@EXAMPLE.COM*) avranno pieni poteri sul database del realm di Kerberos.

   Una volta che `kadmind` viene avviato sul server, qualunque utente è in grado di accedere ai suoi servizi eseguendo `kadmin` su qualunque client o server presente nel realm. Tuttavia, solo gli utenti elencati nel file `kadm5.acl` avranno il permesso di modificare a loro piacimento il database ma non potranno cambiare le proprie password.

   

   Nota Bene

   L'utility `kadmin` comunica con il server `kadmind` attraverso la rete e utilizza Kerberos per gestire l'autenticazione. Per questa ragione, il primo principal deve essere già esistente, prima di potersi connettere al server attraverso la rete per amministrarlo. Create il primo principal usando il comando `kadmin.local`, il quale è concepito proprio per essere utilizzato sullo stesso host di KDC e non si serve di Kerberos per l'autenticazione.

   Per creare il primo principal, digitate il seguente comando `kadmin.local` al terminale di KDC:
   ```
   /usr/kerberos/sbin/kadmin.local -q "addprinc username/admin"
   ```

6. Avviate Kerberos mediante i comandi seguenti:

```
/sbin/service krb5kdc start
/sbin/service kadmin start
/sbin/service krb524 start
```

7. Aggiungete altri principal per gli utenti, usando il comando `addprinc` con `kadmin`. `kadmin` e `kadmin.local` sono interfacce della linea di comando per il KDC. Dopo aver lanciato il programma `kadmin` si rendono disponibili molti comandi. Per maggiori informazioni, consultate la pagina man di `kadmin`.
8. Verificate che il vostro server stia emettendo i ticket. Anzitutto, eseguite `kinit` per ottenere un ticket e immagazzinatelo in un credential cache (o file dei ticket). Successivamente utilizzate `klist` per visualizzare l'elenco delle credenziali nella vostra cache e usate `kdestroy` per eliminare la cache e le credenziali in essa contenute.

Nota Bene

Per default, `kinit` cerca di effettuare l'autenticazione utilizzando lo stesso nome utente di login del sistema (non il server Kerberos). Se il nome utente non corrisponde al principal contenuto nel database di Kerberos, `kinit` emetterà un messaggio di errore. In tal caso, assegnate a `kinit` il nome del vostro principal come argomento per la linea di comando (`kinit` *`principal`*).

Una volta completate queste operazioni, il server Kerberos dovrebbe essere attivo e funzionante.

19.6. Configurazione di un client Kerberos 5

La configurazione di un client Kerberos 5 è meno impegnativa rispetto a quella del server. Dovete, come minimo, installare i pacchetti client e fornire a ciascun client un file di configurazione `krb5.conf` valido. Le versioni kerberizzate di `rsh` e `rlogin` necessitano anche di alcune modifiche.

1. Assicuratevi che il client kerberos e il KDC siano sincronizzati. Per maggiori informazioni in merito, consultate la Sezione 19.5. Accertatevi, inoltre, che il DNS funzioni correttamente sul client Kerberos prima di configurare i programmi relativi al client di Kerberos.
2. Installate i pacchetti `krb5-libs` e `krb5-workstation` su tutte le macchine client. Dovete anche fornire un file `/etc/krb5.conf` valido per ciascun client (in genere, si può utilizzare lo stesso `krb5.conf` usato dal KDC).
3. Prima che una workstation presente nel realm possa consentire agli utenti di collegarsi utilizzando versioni Kerberizzate di `rsh` e `rlogin`, occorre installarvi il pacchetto `xinetd` ed è necessario che il principal host sia incluso nel database di Kerberos. Anche per i programmi del server`kshd` e `klogind`, sarà necessario l'accesso alle chiavi per i principal dei loro servizi.

   Utilizzando `kadmin`, aggiungete un principal host alla workstation sul KDC. L'istanza, in questo caso, sarà l'hostname della postazione. Potete utilizzare l'opzione `-randkey` per `addprinc` appartenente al comando `kadmin` per creare il principal e assegnargli una chiave casuale:

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

   Una volta creato il principal, potete estrarre le chiavi per la workstation eseguendo `kadmin` *direttamente sulla workstation* e utilizzare il comando `ktadd` all'interno di `kadmin`:

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

4. Se desiderate utilizzare altri servizi di rete Kerberizzati, essi devono esseri prima avviati. Di seguito viene riportato un elenco dei servizi kerberizzati piú comuni e le istruzioni su come abilitarli:

   - `rsh` e `rlogin` — Per utilizzare la versione Kerberizzata di `rsh` e `rlogin`, dovete abilitare `klogin`, `eklogin` e `kshell`.

- Telnet — Per usare la versione kerberizzata di Telnet, dovete abilitare `krb5-telnet`.
- FTP — Per l'accesso FTP, create ed estraete una chiave per un principal con una root di `ftp`. Assicurarsi di impostare l'istanza sull'hostname qualificato del server FTP, abilitate poi `gssftp`.
- IMAP — Per utilizzare un server IMAP kerberizzato, il pacchetto `cyrus-imap` usa Kerberos 5 solo se è stato installato il pacchetto `cyrus-sasl-gssapi`. Il pacchetto `cyrus-sasl-gssapi` contiene i plugin Cyrus SASL i quali supportano l'autenticazione GSS-API. Cyrus IMAP dovrebbe funzionare correttamente con kerberos, fino a quando l'utente `cyrus` è in grado di trovare la chiave corretta in `/etc/krb5.keytab`, e root per il principal, è impostato su `imap` (creato con `kadmin`).

  Il pacchetto `dovecot` contiene altresì un server IMAP alternativo a `cyrus-imap`, il quale è incluso con Red Hat Enterprise Linux, ma non supporta, per ora, GSS-API e Kerberos.
- CVS — Per utilizzare un server CVS kerberizzato, `gserver` utilizza un principal con un root di `cvs` ed è identico al `pserver` del CVS.

Per maggiori dettagli su come abilitare i servizi, controllare il capitolo intitolato *Controllo dell'accesso ai servizi* nel *Red Hat Enterprise Linux System Administration Guide*.

19.7. Risorse aggiuntive

Per maggiori informazioni su Kerberos, consultate le seguenti risorse.

19.7.1. Documentazione installata

- La directory `/usr/share/doc/krb5-server-<numero-versione>` — la *Guida all'installazione di Kerberos V5* e la *Guida dell'Amministratore di sistema del Kerberos V5* disponibili nei formati PostScript e HTML. È necessario installare il pacchetto `krb5-server`.
- La directory `/usr/share/doc/krb5-workstation-<numero-versione>` — La *Guida dell'utente di UNIX Kerberos V5*, nei formati PostScript e HTML. Il pacchetto `krb5-workstation` deve essere installato.
- Pagine man di Kerberos — Con l'implementazione di Kerberos si ottengono uno svariato numero di pagine man per i file di configurazione e per le applicazioni. Quanto segue, rappresenta un elenco delle pagine man più importanti.

  Applicazioni del client

  - `man kerberos` — Una introduzione al sistema di Kerberos, il quale descrive il funzionamento delle credenziali e fornisce dei consigli per ottenere e distruggere i ticket di Kerberos. La parte inferiore della pagina man, si riferisce alle relative pagine man.
  - `man kinit` — Descrive come usare questo comando per ottenere e depositare un ticket-granting ticket.
  - `man kdestroy` — Descrive come usare questo comando, per distruggere le credenziali di Kerberos.
  - `man klist` — Descrive come usare questo comando per elencare le credenziali di Kerberos depositate.

Applicazioni amministrative

- `man kadmin` — Descrive come usare questo comando per amministrare il database V5 di Kerberos.
- `man kdb5_util` — Descrive come usare questo comaando, per creare ed effettuare delle funzioni amministrative di basso-livello, sul databaase V5 di Kerberos.

Applicazioni del server

- `man krb5kdc` — Descrive le opzioni disponibili della linea di comando per il Kerberos V5 KDC.
- `man kadmind` — Descrive le opzioni della linea di comando disponibili per il server di gestione V5 di Kerberos.

File di configurazione

- `man krb5.conf` — Descrive il formato e le opzioni disponibili all'interno del file di configurazione per la libreria V5 di Kerberos.
- `man kdc.conf` — Descrive il formato e le opzioni disponibili all'interno del file di configurazione per Kerberos V5 AS e KDC.

19.7.2. Siti Web utili

- http://web.mit.edu/kerberos/www — home page di *Kerberos: Il Network Authentication Protocol* sul sito del MIT.
- http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html — sezione FAQ (Frequently Asked Questions) di Kerberos.
- ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS — link a una versione in Postscript del libro intitolato *Kerberos: An Authentication Service for Open Network Systems* di Jennifer G. Steiner, Clifford Neuman e Jeffrey I. Schiller. Si tratta della prima documentazione prodotta su Kerberos.
- http://web.mit.edu/kerberos/www/dialogue.html — *Designing an Authentication System: a Dialogue in Four Scenes* creato da Bill Bryant nel 1988, modificato da Theodore Ts'o nel 1997. Racconta di una conversazione tra due programmatori che stanno progettando di creare un sistema di autenticazione Kerberos. Lo stile informale della discussione agevola coloro che non conoscono assolutamente Kerberos.
- http://www.ornl.gov/~jar/HowToKerb.html — *Come "kerberizzare" il vostro sito* é un ottimo riferimento per "kerberizzare" una rete.
- http://www.networkcomputing.com/netdesign/kerb1.html — *Manuale del modello di rete di Kerberos* offre una panoramica approfondita sul sistema Kerberos.

Capitolo 20.

Protocollo SSH

SSH™ (o *S*ecure *SH*ell) è un protocollo che facilita i collegamenti sicuri tra due sistemi, usando un'architettura del tipo client/server permettendo agli utenti di registrarsi in sistemi host server, in modo remoto. A differenza di altri protocolli remoti di comunicazione, come FTP o Telnet, SSH cripta la sessione di login, impedendo alle persone non autorizzate di ottenere le password in chiaro.

SSH è stato progettato per sostituire applicazioni precedenti, meno sicure utilizzate per l'accesso a sistemi remoti come **telnet** o **rsh**. Un programma chiamato `scp` sostituisce i programmi meno recenti per copiare i file tra host, quali **rcp**. Poichè queste applicazioni non cifrano le password tra il client e il server, si consiglia di utilizzarle il meno possibile. Se usate dei metodi sicuri per collegarvi ad altri sistemi remoti, correte meno rischi per la sicurezza del vostro sistema e del sistema a cui vi collegate.

20.1. Caratteristiche di SSH

Il protocollo SSH fornisce le seguenti misure di protezione:

- Dopo una connessione iniziale, il client verifica che il collegamento avvenga con lo stesso server, al quale ci si è collegati precedentemente.
- Il client trasmette le proprie informazioni di autenticazione al server usando una codifica a 128 bit
- Tutti i dati inviati e ricevuti durante la sessione, vengono trasferiti utilizzando una codifica a 128 bit, in questo modo è estremamente complesso decodificare e leggere le trasmissioni.
- Il client può inoltrare le applicazioni X11 [1] applicazioni dal server. Questa tecnica, chiamata *X11 forwarding*, fornisce una applicazione grafica sicura da usare attraverso la rete.

Poichè il protocollo SSH codifica tutto ciò che invia e riceve, esso può essere usato per cifrare protocolli che altrimenti non sarebbero sicuri. Se usate la tecnica chiamata *port forwarding*, un server SSH può diventare un condotto per rendere sicuri protocolli non sicuri, come POP, aumentando la sicurezza dei dati e del sistema in generale.

Red Hat Enterprise Linux include il pacchetto OpenSSH generico (`openssh`), server OpenSSH (`openssh-server`) ed i pacchetti del client (`openssh-clients`). Per istruzioni sull'installazione e impiego di OpenSSH, consultate il capitolo *OpenSSH* nella *Red Hat Enterprise Linux System Administration Guide*. Notare anche che pacchetti OpenSSH richiedono l'installazione del pacchetto OpenSSL (`openssl`), il quale installa numerose librerie per la cifratura che consentono a OpenSSH di fornire comunicazioni cifrate.

20.1.1. Perché usare SSH?

Utenti maliziosi dispongono di un'ampia varietà di strumenti per interrompere, intercettare e reindirizzare il traffico di rete allo scopo di ottenere l'accesso al vostro sistema. In generale queste minacce possono essere raggruppate nel seguente modo:

- *Intercettazione delle comunicazioni tra due sistemi* — in questo scenario un aggressore può trovarsi in qualche punto della rete tra le due entità in comunicazione ed eseguire una copia delle informazioni trasmesse tra i due sistemi. L'aggressore potrebbe intercettare e conservare le informazioni, o modificarle e inviarle al destinatario originale.

1. X11 si riferisce al sistema di visualizzazione a finestre X11R6.7, generalmente conosciuto come Sistema X Window o X. Red Hat Enterprise Linux comprende XFree86, un sistema X Window Open Source.

Questo attacco può essere sventato attraverso l'utilizzo di una comune utility di rete per la rilevazione delle intrusioni, puó essere rappresentata da un pacchetto sniffer.

- *Imitazione di un host particolare* — Con questa strategia, il sistema di un aggressore finge di essere il destinatario di un messaggio. Se la strategia funziona, il sistema dell'utente non si accorge dell'inganno.

  Questo attacco può essere sventato attraverso tecniche note come DNS poisoning [2] o IPspoofing [3].

Entrambe le tecniche descritte sopra consentono l'intercettazione di informazioni potenzialmente importanti e, se l'intercettazione avviene per scopi ostili, i risultati possono essere disastrosi.

Se SSH viene usato per i login con la shell remota e per la copia dei file, le minacce alla sicurezza si riducono notevolmente. Questo perchè il server e l'SSH client utilizzano le firme digitali per verificare l'identità degli utenti. Inoltre, tutte le comunicazioni tra i sistemi client e server sono cifrate. I tentativi di assumere l'identità di uno dei due sistemi comunicanti non funzioneranno, poichè ogni pacchetto viene cifrato con un codice conosciuto solo dai sistemi locali e remoti.

20.2. Versioni del Protocollo SSH

Il protocollo SSH consente a ogni programma client e server creato in base alle specifiche del protocollo di comunicare in modo sicuro e di essere utilizzato in maniera interscambiabile.

Attualmente esistono due diverse versioni di SSH (versione 1 e versione 2). La versione 1 contiene diversi algoritmi di cifratura brevettati (anche se molti brevetti sono scaduti) ed è vulnerabile ad una violazione della sicurezza che potenzialmente permette ad un aggressore, di inserire dati nel flusso delle comunicazioni. La suite OpenSSH in Red Hat Enterprise Linux utilizza la versione 2 di SSH, in quanto questa versione presenta un algoritmo di scambio della chiave migliorato, il quale non è vulnerabile al tipo di violazione presente nella versione 1. Tuttavia, la suite OpenSSH supporta anche la versione 1 dei collegamenti.

 **Importante**

Si consiglia di utilizzare, se possibile, server e client compatibili con la versione 2.

20.3. Sequenza degli eventi di una connessione SSH

Una serie di eventi contribuisce a salvaguardare l'integrità di una comunicazione SSH tra due host.

- Viene fatta una introduzione criptografica in modo tale che il client possa verificare che stia comunicando con il server corretto.
- Il livello di trasporto del collegamento tra il client e l'host remoto, viene cifrato usando un codice simmetrico.
- Il client autentica se stesso al server.
- il client remoto interagisce con l'host remoto attraverso la connessione cifrata.

2. Il DNS poisoning si verifica quando un intruso ottiene l'accesso a un server DNS, indirizzando i sistemi client a un host duplicato.
3. L'IP spoofing si verifica quando un intruso invia pacchetti di rete che sembrano provenire da un host fidato della rete.

20.3.1. Livello di trasporto

Lo scopo primario del livello di trasporto è quello di facilitare una comunicazione sicura tra due host al momento dell'autenticazione e durante una successiva comunicazione. Il livello di trasporto, cerca di raggiungere tale scopo cifrando e decifrando i dati, e fornendo una protezione dell'integrità dei pacchetti di dati in fase di trasmissione e ricezione. Inoltre, il livello di trasporto può fornire la compressione dei dati, aumentando la velocità di trasferimento delle informazioni.

Quando un client SSH contatta un server, avviene uno scambio di informazioni in modo che i due sistemi possano creare correttamente il livello di trasporto. Durante questo scambio ecco cosa succede:

- Scambio delle chiavi
- Algoritmo della chiave pubblica
- Algoritmo della cifratura simmetrica
- Algoritmo per l'autenticazione del messaggio
- L'algoritmo hash è determinato

Durante lo scambio delle chiavi, il server si fa riconoscere dal client tramite una *chiave host* unica. Se il client non ha mai comunicato con il suddetto server, esso non à in grado di riconoscere la sua chiave e non verrà eseguito il collegamento. OpenSSH aggira questo problema accettando la chiave host del server dopo che l'utente è stato notificato, verificando l'accettazione della chiave host stessa. Nei collegamenti successivi, la chiave host del server viene verificata con una versione salvata sul client, in modo che il client sia sicuro di comunicare con il server corretto. Se in futuro la chiave host non corrisponde più, l'utente dovrà rimuovere la versione salvata nel client prima di eseguire un nuovo collegamento.

Attenzione

Un aggressore potrebbe mascherarsi da utente del server SSH durante il contatto iniziale, questo perchè il sistema locale non conosce necessariamente la differenza tra il server corretto e quello falso impostato dall'aggressore. Per evitare che questo accada, dovreste verificare l'integrità del nuovo server SSH, contattando l'amministratore del server prima di collegarvi per la prima volta o a causa di una non corrispondenza della chiave.

SSH è stato ideato per funzionare con quasi ogni tipo di algoritmo per le chiavi pubbliche o formato di codifica. Dopo lo scambio iniziale delle chiavi che genera un valore hash usato per gli scambi e un valore segreto condiviso, i due sistemi iniziano immediatamente a calcolare nuove chiavi e algoritmi per proteggere l'autenticazione e i dati futuri inviati tramite la connessione.

Dopo la trasmissione di una certa quantità di dati con l'utilizzo di una chiave e un algoritmo particolari (la quantità esatta dipende dall'implementazione di SSH), avviene un altro scambio di chiavi, che genera a sua volta una ulteriore serie di valori hash e un nuovo valore segreto condiviso. In questo modo, anche se un aggressore riuscisse a determinare tali valori, essi saranno validi solo per un determinato periodo.

20.3.2. Autenticazione

Dopo aver costruito un tunnel sicuro per inviare le informazioni da un sistema all'altro, il server indica al client i diversi metodi di autenticazione supportati, come per esempio una firma privata codificata o la digitazione di una password. Il client tenta, poi, di autenticarsi al server tramite uno dei metodi supportati.

Poichè i server SSH e i client possono essere configurati per autorizzare diversi tipi di autenticazione, questo metodo offre un ottimo controllo a entrambe le parti. Il server stabilisce i metodi di cifratura

supportati in base al proprio modello di sicurezza, e il client può scegliere l'ordine dei metodi di autenticazione da utilizzare dalle opzioni disponibili. Grazie alla sicurezza del livello di trasporto SSH, è possibile utilizzare senza problemi perfino metodi di autenticazione apparentemente non sicuri, come l'autenticazione basata sull'host o sull'uso della password.

20.3.3. Canali

Dopo un'autenticazione corretta su un livello di trasporto SSH, vengono aperti dei *canali* mediante una tecnica chiamata multiplexing[4].Ognuno di questi canali gestisce la comunicazione per una diversa sessione di terminale di informazioni X11 inviate.

Entrambi i client ed i server possono creare un nuovo canale. A ogni canale viene assegnato un numero diverso per ogni estremità del collegamento. Quando il client tenta di aprire un nuovo canale, viene inviato, insieme alla richiesta, il suo numero. Questa informazione viene archiviata sul server e utilizzata per indirizzare una particolare comunicazione di servizio per il canale in questione. In questo modo le diverse sessioni non si disturbano, ed i canali possono essere chiusi senza interrompere la connessione primaria SSH tra i due sistemi.

I canali supportano inoltre il *controllo del flusso*, che consente loro di inviare e ricevere i dati ordinatamente. In questo modo i dati non vengono inviati attraverso il canale finché il client non riceve un messaggio che lo avverte che il canale è in grado di ricevere.

Il client e il server negoziano le caratteristiche di ogni canale automaticamente, a seconda del tipo di servizio che il client richiede e del tipo di connessione di rete che l'utente usa. I diversi tipi di connessione remota possono essere gestiti in modo flessibile senza dover modificare l'infrastruttura di base del protocollo.

20.4. File di configurazione OpenSSH

OpenSSH possiede due diversi tipi di file di configurazione, uno per i programmi client (`ssh`, `scp` e `sftp`) e l'altro per il demone del server (`sshd`).

Le informazioni di configurazione SSH sono memorizzate nella directory `/etc/ssh/`:

- `moduli` — contiene gruppi Diffie-Hellman usati per lo scambio delle chiavi. In sostanza, questo consente di creare un livello di trasporto sicuro. Quando le chiavi sono scambiate all'inizio di una sessione SSH, viene creato un valore segreto e condiviso che non può essere determinato da una singola parte e viene usato per fornire l'autenticazione dell'host.
- `ssh_config` — il file di configurazione del client SSH. Viene sovrascritto se anche nella home directory dell'utente (`~/.ssh/config`) ne è presente uno.
- `sshd_config` — il file di configurazione per il demone `sshd`.
- `ssh_host_dsa_key` — la chiave privata DSA utilizzata dal demone `sshd`.
- `ssh_host_dsa_key.pub` — la chiave pubblica DSA usata dal demone `sshd`.
- `ssh_host_key` — la chiave privata RSA usata dal demone `sshd` per la versione 1 del protocollo SSH.
- `ssh_host_key.pub` — la chiave pubblica RSA usata dal demone `sshd` per la versione 1 del protocollo SSH.
- `ssh_host_rsa_key` — la chiave privata RSA usata dal demone `sshd` per la versione 2 del protocollo SSH.

4. Una connessione multiplexed è costituita da diversi segnali inviati tramite un mezzo comune condiviso. Con SSH, canali differenti vengono inviati tramite una connessione comune sicura.

- `ssh_host_rsa_key.pub` — la chiave pubblica RSA usata dal demone `sshd` per la versione 2 del protocollo SSH.

Le informazioni di configurazione SSH specifiche per l'utente sono archiviate nella sua directory home all'interno di `~/.ssh/`:

- `authorized_keys` — il file che contiene un elenco delle chiavi pubbliche "autorizzate" per i server. Quando un client si collega ad un server, lo stesso autentica il client stesso controllando la propria chiave pubblica immagazzinata all'interno di questo file.
- `id_dsa` — contiene l'identità di autenticazione DSA dell'utente.
- `id_dsa.pub` — la chiave DSA pubblica dell'utente.
- `id_rsa` — la chiave RSA pubblica usata da `ssh` per la versione 2 del protocollo SSH.
- `id_rsa.pub` — la chiave RSA pubblica usata da `ssh` per la versione 2 del protocollo SSH.
- `identity` — la chiave RSA privata usata da `ssh` per la versione 1 del protocollo SSH.
- `identity.pub` — la chiave RSA pubblica usata da `ssh` per la versione 1 del protocollo SSH.
- `known_hosts` — contiene le chiavi host DSA dei server a cui l'utente si collega tramite SSH. Questo file è importante per garantire che il client SSH si colleghi al server SSH corretto.

Importante

Se la chiave host del server SSH viene modificata, il client notificherá all'utente che la connessione non puó procedere fino a quando la chiave host é cancellata dal file `known_hosts` usando un editor di testo. Prima di fare ció, dovreste contattare l'amministratore di sistema del server SSH, per assicurarvi che il server non sia stato compromesso.

Consultate le pagine man di `ssh_config` e `sshd_config` per informazioni inerenti le diverse direttive disponibili con i file di configurazione SSH.

20.5. Shell più che sicura

Un'interfaccia a linea di comando sicura è solo uno dei tanti modi in cui è possibile usare una SSH. Considerata la larghezza di banda, le sessioni X11 possono essere indirizzate tramite un canale SSH. Oppure, utilizzando il TCP/IP forwarding, le connessioni di porta un tempo non sicure tra sistemi diversi possono essere mappate su canali SSH specifici.

20.5.1. Inoltro X11

Aprire una sessione X11 tramite una connessione SSH stabilita è facile quanto avviare un programma X su un computer locale. Quando un programma X viene eseguito dalla shell, il client e il server SSH creano un nuovo canale sicuro e i dati del programma X vengono inviati tramite questo canale al vostro client.

L'inoltro X11 può essere molto utile. Per esempio, potete usarlo per creare una sessione interattiva e sicura con l'interfaccia grafica utente `up2date` sul server per aggiornare i pacchetti. Per farlo, connettetevi al server utilizzando `ssh` e digitate:

```
up2date &
```

Dopo aver fornito la password root per il server, comparirá **Red Hat Update Agent** e permetterá all'utente remoto di aggiornare in modo sicuro il sistema remoto.

20.5.2. Port forwarding

Con SSH potete rendere sicuri i protocolli TCP/IP altrimenti insicuri mediante il port forwarding. Con questa tecnica, il server SSH diventa un passaggio cifrato al client SSH.

Il port forwarding consiste nel mappare una porta locale sul client per una porta remota sul server. SSH vi permette di mappare qualsiasi porta dal server per qualsiasi porta sul client. I numeri delle porte non devono corrispondere per permettere il funzionamento di questa tecnica.

Per creare un canale TCP/IP di port forwarding che attenda le connessioni sull'host locale, utilizzate il seguente comando:

```
ssh -L local-port:remote-hostname:remote-port username@hostname
```

Nota Bene

Per impostare il port forwarding all'ascolto su porte inferiori alla 1024 è necessario l'accesso root.

Se per esempio desiderate controllare la vostra posta su di un server chiamato `mail.example.com` utilizzando il protocollo POP tramite una connessione cifrata, potete usare il comando seguente:

```
ssh -L 1100:mail.example.com:110 mail.example.com
```

Una volta impostato il canale per il port forwarding tra la macchina del client e il mail server, potete indicare al vostro client di posta POP3 di usare la porta 1100 sul localhost per controllare l'arrivo di nuova posta. Qualsiasi richiesta inviata alla porta 1100 sul sistema client, sarà indirizzata in modo sicuro al server `mail.example.com`.

Se `mail.example.com` non esegue un demone server SSH, eseguito invece da un'altra macchina sulla stessa rete, potete ancora utilizzare SSH per rendere sicura una parte della connessione. Tuttavia è necessario un comando leggermente diverso:

```
ssh -L 1100:mail.example.com:110 other.example.com
```

In questo esempio, le richieste POP3 dalla porta 1100 sulla macchina del client, sono inviate tramite il collegamento SSH sulla porta 22 per il server SSH `other.example.com`. A questo punto, `other.example.com` si collega alla porta 110 su `mail.example.com` per permettervi di controllare l'arrivo di nuova posta. Con questa tecnica, solo collegamento tra il sistema client e il server SSH `other.example.com` è sicuro.

Il port forwarding può risultare particolarmente utile per ricevere informazioni in modo sicuro tramite i firewall di rete. Se il firewall è configurato per consentire il traffico SSH tramite la porta standard (22), ma blocca l'accesso alle altre porte, una connessione tra due host che usano porte bloccate è comunque possibile se si reindirizza la comunicazione tramite una connessione SSH.

Nota Bene

L'utilizzo del port forwarding per inoltrare connessioni in questo modo consente a qualsiasi utente sul sistema client di connettersi a quel determinato servizio.Se il sistema client viene compromesso, anche un aggressore avrà accesso ai servizi inoltrati.

Gli amministratori di sistema possono disabilitare la funzione del port forwarding sul server, specificando il parametro `No` per la riga AllowTcpForwarding nel file `/etc/ssh/sshd_config` e riavviando il servizio `sshd`.

20.6. Richiesta di SSH per le connessioni remote

Per rendere SSH davvero efficace, è necessario smettere di utilizzare tutti i protocolli di connessione non sicuri, come Telnet e FTP. Se questo non avviene, una password protetta tramite SSH può essere individuata alla prima connessione via Telnet.

Alcuni servizi da disabilitare includono:

- `telnet`
- `rsh`
- `rlogin`
- `vsftpd`

Per disabilitare i metodi di connessione poco sicuri, utilizzate il programma della linea di comando `chkconfig`, il programma basato su ncurses `ntsysv` o l'applicazione grafica **Strumento di configurazione dei servizi** (`redhat-config-services`). Per utilizzare questi strumenti dovete collegarvi come root.

Per maggiori informazioni sui runlevel e sulla configurazione di servizi con `chkconfig`, `ntsysv` e **Strumento di configurazione dei servizi**, fate riferimento al capitolo relativo al *controllo dell'accesso ai servizi* nella *Red Hat Enterprise Linux System Administration Guide*.

20.7. Risorse aggiuntive

Per maggiori informazioni su SSH, consultate le seguenti risorse.

20.7.1. Documentazione installata

- La directory `/usr/share/doc/openssh-<numero-versione>/` — Sostituire `<numero-versione>` con la versione installata del pacchetto OpenSSH. Questa directory contiene un README con informazioni basiche sul progetto OpenSSH e su di un file chiamato `RFC.nroff` con informazioni generali sul protocollo SSH.
- Pagine man relative a SSH — Ci sono diverse pagine man per svariate applicazioni e file di configurazione con SSH. Il seguente è un elenco di alcune pagine man più importanti.

  Applicazioni client

  - `man ssh` — Descrive come usare questo comando per collegarsi ad un server SSH.
  - `man scp` — Descrive come usare questo comando per copiare i file per e da un server SSH.
  - `man sftp` — Descrive come usare questo comando per copiare in modo interattivo i file per e da un server SSH.

  Applicazioni del server

  - `man sshd` — Descrive le opzioni della linea di comando disponibili per il server SSH.

File di configurazione

- `man ssh_config` — Descrive il formato e le opzioni disponibili all'interno del file di configurazione per i client SSH.
- `man sshd_config` — Descrive il formato e le opzioni disponibili all'interno del file di configurazione per il server SSH.

20.7.2. Siti web utili

- http://www.openssh.com — La pagina penSSH FAQ, i bug report, le mailing list, gli obbiettivi del progetto, e molte spiegazioni tecniche sui contenuti della sicurezza.
- http://www.openssl.org — La pagina penSSH FAQ, i bug report, le mailing list, e una descrizione degli obbiettivi del progetto.
- http://www.freessh.org — Software client SSH per altre piattaforme.

20.7.3. Libri correlati

- *Red Hat Enterprise Linux System Administration Guide* Red Hat, Inc. — l capitolo *OpenSSH* spiega come impostare un server SSH e come usare il software client SSH fornito con la suite OpenSSH degli strumenti. Inoltre spiega come generare una coppia di chiavi RSA (o DSA), le quali abilitano a delle registrazioni senza l'uso di password.

Capitolo 21.

SELinux

Security-Enhanced Linux, o *SELinux*, rappresenta un'architettura creata per aumentare la sicurezza del vostro sistema, ed è integrata all'interno del kernel di 2.6.*x* utilizzando *linux security modules* (LSM). È un progetto ideato dalla United States National Security Agency (NSA) e dalla community SELinux. L'integrazione di SELinux su Red Hat Enterprise Linux è stata resa possibile grazie allo sforzo congiunto tra la NSA e Red Hat.

21.1. Introduzione a SELinux

SELinux fornisce un sistema *mandatory access control* (MAC) flessibile, ideato all'interno del kernel di Linux. Sotto lo standard di Linux, *discretionary access control* (DAC), un'applicazione o un processo in esecuzione come un utente (UID o SUID) possiede i permessi dell'utente stesso che la esegue, questo vale per esempio per i file, i socket ed altri processi. L'esecuzione di un kernel MAC di SELinux, protegge il sistema da applicazioni maliziose in grado di poter danneggiare o persino distruggere il sistema stesso. SELinux definisce i diritti di accesso e di transito per ogni utente, applicazione, processo e file presenti sul sistema. SELinux è in grado di governare l'interazione di questi *soggetti* e *oggetti*, utilizzando una *policy* di sicurezza in grado di specificare la restrittività o la permissività di una installazione di Red Hat Enterprise Linux.

Per la maggior parte dei casi, SELinux è quasi completamente invisibile agli utenti del sistema. Solo gli amministratori devono preoccuparsi d'impiegare una policy restrittiva per i propri ambienti server. Tale policy può essere restrittiva o permissiva a seconda delle necessità, ed è in grado di essere molto dettagliata. Questi dettagli conferiscono al kernel di SELinux, un controllo granulare completo su tutto il sistema.

Quando un'applicazione cerca di accedere un oggetto come ad esempio un file, il server responsabile all'applicazione della policy presente nel kernel, controlla un *access vector cache* (AVC), dove i permessi degli oggetti e dei soggetti vengono conservati. Se non è possibile prendere una decisione in base ai dati contenuti nella AVC, la richiesta continua fino ad arrivare al server di sicurezza, il quale, a sua volta, controlla il *contesto di sicurezza* dell'applicazione e del file con una matrice. A quel punto il permesso può essere garantito oppure rifiutato, con un messaggio `avc: denied`, riportato in `/var/log/messages`. I soggetti e gli oggetti ottengono il proprio contesto di sicurezza tramite una policy installata, la quale fornisce altresì le informazioni per poter popolare la matrice del server di sicurezza.

In aggiunta all'esecuzione in modalità *enforcing*, SELinux può essere eseguito in modalità *permissiva*, dove l'AVC viene controllato, e tutti gli accessi rifiutati vengono registrati, è da ricordare comunque che SELinux di per sè, non applica alcuna policy.

Per maggiori informazioni sul funzionamento di SELinux, consultare la Sezione 21.3.

21.2. File relativi a SELinux

Le seguenti sezioni descrivono i file di configurazione di SELinux insieme ai file system correlati.

21.2.1. Lo pseudo-File System `/selinux/`

Lo pseudo-file system `/selinux/` contiene i comandi maggiormente utilizzati dal sottosistema del kernel. Questo tipo di file system è simile allo pseudo-file system `/proc/`.

In molti casi gli amministratori e gli utenti non hanno bisogno di manipolare il suddetto componente, al contrario di altri file e directory di SELinux.

Il seguente esempio mostra i contenuti della directory `/selinux/`:

```
-rw-rw-rw-  1 root root 0 Sep 22 13:14 access
dr-xr-xr-x  1 root root 0 Sep 22 13:14 booleans
--w-------  1 root root 0 Sep 22 13:14 commit_pending_bools
-rw-rw-rw-  1 root root 0 Sep 22 13:14 context
-rw-rw-rw-  1 root root 0 Sep 22 13:14 create
--w-------  1 root root 0 Sep 22 13:14 disable
-rw-r--r--  1 root root 0 Sep 22 13:14 enforce
-rw-------  1 root root 0 Sep 22 13:14 load
-r--r--r--  1 root root 0 Sep 22 13:14 mls
-r--r--r--  1 root root 0 Sep 22 13:14 policyvers
-rw-rw-rw-  1 root root 0 Sep 22 13:14 relabel
-rw-rw-rw-  1 root root 0 Sep 22 13:14 user
```

Per esempio, l'esecuzione del comando `cat` sul file `enforce`, può rivelare un valore `1` per la modalità di enforcing, oppure `0` per la modalità permissiva.

21.2.2. File di configurazione di SELinux

Le seguenti sezioni descrivono i file di configurazione e la policy di SELinux, insieme ai file system correlati presenti nella directory `/etc/`.

21.2.2.1. Il file di configurazione `/etc/sysconfig/selinux`

Sono presenti due diversi modi per poter configurare SELinux con Red Hat Enterprise Linux: utilizzando **Strumento di configurazione del livello di sicurezza** (`system-config-securitylevel`), oppure manualmente modificando il file di configurazione (`/etc/sysconfig/selinux`).

Il file `/etc/sysconfig/selinux` rappresenta il file di configurazione primario per l'abilitazione o la disabilitazione di SELinux, e per l'impostazione ed il modo di applicazione della policy da utilizzare sul sistema.

Nota Bene

`/etc/sysconfig/selinux` contiene un link simbolico per il file di configurazione attuale, `/etc/selinux/config`.

Di seguito viene riportato un sottoinsieme completo di opzioni, disponibili per la configurazione:

- `SELINUX=<enforcing|permissive|disabled>` — Definisce lo stato superiore di SELinux su di un sistema.
  - `enforcing` — La policy di sicurezza di SELinux è stata applicata.
  - `permissive` — Il sistema SELinux visualizza alcuni avvertimenti senza applicare tale policy. Questo processo risulta utile per il debugging e per il troubleshooting. In modalità permissiva, verranno registrati un numero maggiore di negazioni, man mano che gli utenti porteranno avanti le proprie azioni, tale permessività è compromessa se si utilizza la modalità enforcing. Per esempio, se si cerca di percorrere tutti i livelli di una directory, tale operazione originerà dei messaggi `avc: denied` multipli per ogni livello letto, al contrario di un kernel in modalità enforcing che non farà altro che arrestare tale azione, evitando quindi la visualizzazione dei suddetti massaggi.

- `disabled` — SELinux risulta essere completamente disabilitato. Le funzioni di SELinux vengono disabilitate dal kernel e lo pseudo-file system risulta non registrato.

Suggerimento

Le azioni eseguite mentre SELinux risulta essere disabilitato, possono causare un annullamento di un contesto sicuro per il file system interessato. L'esecuzione di `fixfiles relabel` prima di abilitare SELinux, non farà altro che eseguire un relabel del file system, in modo da far funzionare correttamente SELinux una volta abilitato. Per maggiori informazioni consultare la pagina man (8) di `fixfiles`.

Nota Bene

Se si lasciano spazi aggiuntivi alla fine di una riga di configurazione, oppure righe extra alla fine del file, si possono verificare dei comportamenti inaspettati. Per essere sicuri, rimuoveri tutti gli spazi presenti.

- `SELINUXTYPE=<targeted|strict>` — Specifica la policy usata da SELinux.
  - `targeted` — Solo i demoni di rete selezionati risultano essere protetti.

Importante

I seguenti demoni risultano essere protetti usando la policy di default: `dhcpd`, `httpd (apache.te)`, `named`, `nscd`, `ntpd`, `portmap`, `snmpd`, `squid`, e `syslogd`. Il resto dei sistemi viene eseguito nel dominio `unconfined_t`.

I file della policy per questi demoni sono disponibili in `/etc/selinux/targeted/src/policy/domains/program`, e sono soggetti a modifiche a seconda delle versioni disponibili di Red Hat Enterprise Linux.

L'applicazione della policy per i suddetti demoni, può essere abilitata oppure disabilitata utilizzando i valori Boolean controllati dallo **Strumento di configurazione del livello di sicurezza** (`system-config-securitylevel`). Variando un valore Boolean per un determinato demone, si è in grado di disabilitare la transizione della sua policy, la quale previene, per esempio, `init` di passare su `dhcpd` dal dominio `unconfined_t` al dominio specificato in `dhcpd.te`. Il dominio `unconfined_t` permette ai soggetti e agli oggetti con quel determinato contesto di sicurezza, di essere eseguiti sotto uno standard di sicurezza di Linux.

  - `strict` — Protezione SELinux completa per tutti i demoni. I contesti di sicurezza vengono definiti per tutti i soggetti e gli oggetti, e ogni singola azione viene processata dal server responsabile all'attuazione della policy.

21.2.2.2. La directory `/etc/selinux/`

La directory `/etc/selinux/` rappresenta il luogo primario per tutti i file della policy, insieme al file di configurazione primario.

Il seguente esempio mostra i contenuti della directory `/etc/selinux/`:

```
-rw-r--r--  1 root root  448 Sep 22 17:34 config
drwxr-xr-x  5 root root 4096 Sep 22 17:27 strict
drwxr-xr-x  5 root root 4096 Sep 22 17:28 targeted
```

Le due directory `strict/` e `targeted/`, sono le directory specifiche dove vengono contenuti i rispettivi file della policy (es. restrittivi e selezionati).

Per maggiori informazioni sulla policy SELinux e sulla sua configurazione, consultate Red Hat SELinux Policy Writing Guide.

21.2.3. Utility SELinux

Le seguenti sono le utility maggiormente utilizzate con SELinux:

- `/usr/bin/setenforce` — Modifica in tempo reale la modalità eseguita da SELinux. Eseguendo `setenforce 1`, SELinux viene selezionato in modalità enforcing. Eseguendo `setenforce 0`, SELinux viene selezionato in modalità permissiva. Per disabilitare SELinux, dovreste impostare il parametro in `/etc/sysconfig/selinux`, oppure passare il parametro `selinux=0` al kernel, sia in `/etc/grub.conf` oppure al momento dell'avvio.
- `/usr/bin/sestatus -v` — Permette di ottenere lo stato completo di un sistema che esegue SELinux. Il seguente esempio mostra un output `sestatus`:

```
SELinux status:         enabled
SELinuxfs mount:        /selinux
Current mode:           enforcing
Policy version:         18
```

- `/usr/bin/newrole` — Esegue una nuova shell in un nuovo contesto o ruolo. La policy deve permettere la transizione al nuovo ruolo.
- `/sbin/restorecon` — Imposta il contesto di sicurezza di uno o più file, segnando gli attributi estesi con il file appropriato o con un contesto di sicurezza.
- `/sbin/fixfiles` — Controlla o corregge il database del contesto di sicurezza sul file system.

Consultate la pagina man associata con queste utility per maggiori informazioni.

Per maggiori informazioni su tutte le utility binarie disponibili, consultate i contenuti dei pacchetti `setools` o `policycoreutils`, eseguendo `rpm -ql <package-name>`, dove `<package-name>` rappresenta il nome del pacchetto specifico.

21.3. Risorse aggiuntive

Le seguenti sezioni vi permettono di approfondire le vostre conoscenze su SELinux.

21.3.1. Documentazione installata

- `/usr/share/doc/setools-<version-number>/` — La documentazione completa per le utility contenute nel pacchetto `setools`. Questo include tutti gli script d'aiuto, i file di configurazione e la documentazione.

21.3.2. Documentazione di Red Hat

- *Red Hat SELinux Policy Writing Guide*; — Spiega come creare e configurare una policy SELinux.
- *Red Hat SELinux Application Development Guide*; — Per lo sviluppo delle applicazioni in un sistema SELinux.

21.3.3. Siti web utili

- http://www.nsa.gov/selinux/ — La homepage per il team di sviluppo SELinux NSA. Sono presenti numerose risorse in formato HTML e PDF. Anche se la maggior parte di questi link non sono specifici di Red Hat Enterprise Linux, alcuni concetti possono essere validi.
- http://fedora.redhat.com/docs/ — La homepage per il Fedora documentation project, contiene i materiali specifici per il Fedora Core, tutti molto aggiornati poichè il ciclo delle release è molto più breve.
- http://selinux.sourceforge.net — La homepage per la community di SELinux.

IV. Appendici

Sommario

A. Parametri generali e moduli..... 333

Appendice A.

Parametri generali e moduli

Questa appendice illustra *alcuni* dei possibili parametri disponibili per alcuni *driver* di dispositivi hardware comuni [1] che sotto Red Hat Enterprise Linux vengono chiamati *moduli* del kernel. In molti casi, i parametri di default funzioneranno. Tuttavia si potranno presentare dei casi dove parametri extra del modulo sono necessari per un dispositivo in modo da funzionare correttamente, oppure se dovete sovrascrivere i parametri di default del sistema per il dispositivo.

Durante l'installazione, Red Hat Enterprise Linux utilizza un sottoinsieme limitato di driver del dispositivo per creare un ambiente di installazione stabile. Anche se il programma di installazione supporta l'installazione di molti tipi di hardware, alcuni driver (incluso quelli per gli adattatori SCSI e di rete, non sono inclusi nel kernel di installazione). Essi devono essere caricati come moduli dall'utente al momento dell'avvio. Per informazioni su moduli extra del kernel durante il processo di installazione, consultate la sezione inerente i diversi metodi di avvio presente nel capitolo *Preparazione all'avvio* nella *Red Hat Enterprise Linux Installation Guide*.

Completando l'installazione avrete a disposizione un supporto per numerosi dispositivi attraverso i moduli del kernel.

Importante

Red Hat fornisce un gran numero di driver del dispositivo non supportato in pacchetti chiamati `kernel-unsupported-<kernel-version>`, `kernel-smp-unsupported-<kernel-version>`, e `kernel-hugemem-unsupported-<kernel-version>`. Sostituire `<kernel-version>` con la versione del kernel installato sul sistema. Questi pacchetti non sono installati dal programma di installazione di Red Hat Enterprise Linux, e i moduli forniti non sono supportati da Red Hat, Inc..

A.1. Come specificare i parametri del modulo

In alcune situazioni può essere necessario fornire i parametri ad un modulo, in quanto viene caricato per un corretto funzionamento.

Per esempio, per abilitare pienamente un duplex ad una velocità di collegamento pari a 100Mbps per una scheda Ether Express/100, caricare il driver `e100` con l'opzione `e100_speed_duplex=4`.

Attenzione

Quando un parametro presenta delle virgole, assicuratevi di *non* inserire alcuno spazio dopo la virgola.

1. Un driver è un tipo di software che permette a Linux di usare un particolare dispositivo hardware. Senza il driver, il kernel potrebbe non sapere come accedere correttamente il dispositivo.

Suggerimento

Il comando `modinfo` è utile per elencare le diverse informazioni riguardanti il modulo del kernel, come ad esempio le informazioni sulla versione, le dipendenze, le opzioni di parametro e gli alias.

A.2. Parametri SCSI

Hardware	Modulo	Parametri
Controller dei dischi 3ware	`3w-xxxx.o`	
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
Adaptec AACRAID	`aacraid.o`	
Adaptec 28xx, R9xx, 39xx AHA-284x, AHA-29xx, AHA-394x, AHA-398x, AHA-274x, AHA-274xT, AHA-2842, AHA-2910B, AHA-2920C, AHA-2930/U/U2, AHA-2940/W/U/UW/AU/, U2W/U2/U2B/, U2BOEM, AHA-2944D/WD/UD/UWD, AHA-2950U2/W/B, AHA-3940/U/W/UW/, AUW/U2W/U2B, AHA-3950U2D, AHA-3985/U/W/UW, AIC-777x, AIC-785x, AIC-786x, AIC-787x, AIC-788x , AIC-789x, AIC-3860	`aic7xxx.o`	
Controller RAID ICP	`gdth.o`	
ServeRAID IBM	`ips.o`	
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	
Qlogic 1280	`qla1280.o`	

Tabella A-1. Parametri SCSI

A.3. Parametri Ethernet

Importante

Molte network interface cards (NIC) basate su Ethernet, non necessitano di alcun parametro del modulo, per poter alterare le impostazioni. Al contrario, esse possono essere configurate utilizzando `ethtool` o `mii-tool`. Solo dopo che questi tool non hanno avuto esito positivo, allora sarà neces-

sario modificare i suddetti parametri. È possibile visualizzare detti parametri, utilizzando il comando `modinfo`.

Nota Bene

Per informazioni sull'utilizzo di questi tool, consultate le pagine man di `ethtool`, `mii-tool`, e `modinfo`.

Hardware	Modulo	Parametri
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	full_duplex= *0* è off *1* è on
RTL8139, SMC EZ Card Fast Ethernet, schede RealTek che utilizzano chipset RTL8129, o RTL8139 Fast Ethernet	`8139too.o`	
Intel Ether Express/100 driver	`e100.o`	e100_speed_duplex=*X* *Se X* = 0 = autodetect speed and duplex 1 = 10Mbps, half duplex 2 = 10Mbps, full duplex 3 = 100Mbps, half duplex 4 = 100Mbps, full duplex
Intel EtherExpress/1000 Gigabit	`e1000.o`	
Driver Intel i82557/i82558 PCI EtherExpressPro	`eepro100.o`	
NatSemi DP83815 Fast Ethernet	`natsemi.o`	
AMD PCnet32 e AMD PCnetPCI	`pcnet32.o`	
SIS 900/701G PCI Fast Ethernet	`sis900.o`	
ThunderLAN	`tlan.o`	

Hardware	Modulo	Parametri
Schede Digital 21x4x Tulip PCI Ethernet SMC EtherPower 10 PCI(8432T/8432BT) SMC EtherPower 10/100 PCI(9332DST) DEC EtherWorks 100/10 PCI(DE500-XA) DEC EtherWorks 10 PCI(DE450) DEC QSILVER's, Znyx 312 etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	io=*porta_io*
Schede Ethernet Fast VIA Rhine PCI con PCI VIA VT86c100A Rhine-II o 3043 Rhine-I D-Link DFE-930-TX 10/100	`via-rhine.o`	

Tabella A-2. Parametri del modulo Ethernet

A.3.1. Utilizzo di schede Ethernet multiple

Potete utilizzare più schede Ethernet su una macchina. Per ogni scheda ci deve essere un `alias` e, possibilmente, delle righe `options` per ogni scheda in `/etc/modules.conf`. Consultate il capitolo *Moduli del kernel* nella *Red Hat Enterprise Linux System Administration Guide* per maggiori informazioni.

Per maggiori informazioni sull'uso di più schede Ethernet, consultate *Linux Ethernet-HOWTO* online su http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

A.3.2. Il modulo Channel Bonding

Red Hat Enterprise Linux permette agli amministratori di unire i NIC ad un canale unico usando il modulo del kernel `bonding`, e una interfaccia di rete speciale chiamata *channel bonding interface*. Il Channel bonding abilita due o più interfacce di rete ad agire come se fossero una, allo stesso tempo aumentando la larghezza della banda e fornendo una certa ridondanza.

Per eseguire un channel bond di interfacce di rete multiple, l'amministratore deve eseguire le seguenti fasi:

1. Aggiungere la seguente riga a `/etc/modules.conf`:
   `alias bond<`*N*`> bonding`

   Sostituire <*N*> con il numero dell'interfaccia, come ad esempio `0`. Per ogni interfaccia channel bonding configurata, ci deve essere una entry corrispondente in `/etc/modules.conf`.
2. Configurare una interfaccia channel bonding come riportato nella Sezione 8.2.3.
3. Per aumentare le prestazioni, correggere le opzioni disponibili del modulo, per cercare la combinazione migliore. Prestate molta attenzione ai parametri `miimon` o `arp_interval` e `arp_ip_target`. Consultate la Sezione A.3.2.1 per un elenco di opzioni disponibili.
4. Dopo aver eseguito una prova, posizionare le opzioni preferite del modulo in `/etc/modules.conf`.

A.3.2.1. Direttive del modulo `bonding`

Prima di finalizzare le impostazioni per il modulo `bonding`, è consigliabile provare quale impostazione funziona meglio. Per fare questo, aprire un prompt della shell come utente root e digitare:

```
tail -f /var/log/messages
```

Aprire un altro prompt della shell e usare il comando `/sbin/insmod` per caricare il modulo `bonding` con parametri diversi, mentre osservate i messaggi di errore del kernel.

Il comando `/sbin/insmod` viene emesso nel seguente formato:

```
/sbin/insmod bond<N> <parameter=value>
```

Sostituire *<N>* con il numero della interfaccia bonding. Sostituire *<parameter=value>* con un elenco separato da uno spazio di parametri desiderati per l'interfaccia.

Una volta accertato che non ci sono più errori e dopo aver verificato la prestazione dell'interfaccia bonding, aggiungere i parametri del modulo `bonding` appropriato su `/etc/modules.conf`.

Il seguente è un elenco dei parametri disponibili per il modulo `bonding`:

- `mode=` — Specifica una delle quattro policy permesse al modulo `bonding`. I valori accettabili per questo parametro sono:
  - `0` — Imposta una policy del tipo round-robin per il bilanciamento del carico e per il fault tolerance. Le trasmissioni vengono ricevute e inviate in modo sequenziale, su ogni interfaccia slave di tipo 'bonded', iniziando con la prima disponibile.
  - `1` — Imposta una policy del tipo active-backup per il fault tolerance. Le trasmissioni vengono ricevute e inviate tramite la prima interfaccia slave di tipo 'bonded'. Un'altra interfaccia slave di tipo 'bonded' viene usata solo se la prima interfaccia non ha un esito sperato.
  - `2` — Imposta una policy del tipo XOR (exclusive-or) per il bilanciamento del carico e di fault tolerance. Usando questo metodo l'interfaccia eguaglia l'indirizzo MAC della richiesta in entrata, con l'indirizzo MAC per uno dei NIC slave. Una volta stabilito questo collegamento, le trasmissioni vengono inviate in modo sequenziale iniziando con la prima interfaccia disponibile.
  - `3` — Imposta una policy di trasmissione per il fault tolerance. Tutte le trasmissioni vengono inviate su tutte le interfacce di tipo slave.
  - `4` — Imposta una policy del tipo IEEE 802.3ad dynamic link aggregation. Crea gruppi d'aggregazione che condividono la stessa velocità e impostazioni duplex. Trasmette e riceve su tutte le interfacce slave nell'aggregator attivo. Necessita un interruttore compatibile con 802.3ad.
  - `5` — Imposta una policy Transmit Load Balancing (TLB) per il fault tolerance e per il bilanciamento del carico. Il traffico in uscita viene distribuito a seconda del carico su ogni interfaccia slave. Il traffico in ingresso viene ricevuto dall'interfaccia slave corrente. Se lo slave ricevente fallisce, un altro al suo posto assume il controllo dell'indirizzo MAC.
  - `6` — Imposta una policy Active Load Balancing (ALB)per il fault tolerance e per il bilanciamento del carico. Include la trasmissione e la ricezione del bilanciamento del carico per il traffico IPV4. La ricezione del bilanciamento del carico viene raggiunta grazie ad un ARP negotiation.

- `miimon=` — Specifica (in millisecondi) la frequenza di controllo del link MII. Questo è utile se è richiesta una disponibilità elevata in quanto MII viene usato per verificare che il NIC sia attivo. Per controllare che il driver per un NIC particolare supporta il tool MII, digitare il seguente comando come root:
  ```
  ethtool <interface-name> | grep "Link detected:"
  ```

In questo comando, sostituire *<interface-name>* con il nome dell'interfaccia del dispositivo, come ad esempio `eth0`, non l'interfaccia `bond`. Se MII è supportato, il comando ritorna:

```
Link detected: yes
```

Se si usa una interfaccia di tipo 'bonded' per una maggiore disponibilità, il modulo per ogni NIC deve supportare MII.

Impostando il valore su `0` (il default), si disabilita questa caratteristica. Quando si configura questa impostazione, un buon punto di partenza per questo parametro è `100`.

- `downdelay=` — Specifica (in millesecondi) quanto bisogna attendere dopo il fallimento del link prima di disabilitarlo. Il valore deve essere un multiplo di quello specificato nel parametro `miimon`. Il valore è impostato su `0` per default, il quale lo disabilita.
- `updelay=` — Specifica (in millesecondi) quanto bisogna attendere prima di abilitare un link. Il valore deve essere un multiplo di quello specificato nel parametro `miimon`. Il valore è impostato su `0` per default, il quale lo disabilita.
- `arp_interval=` — Specifica (in millisecondi) la frequenza di controllo ARP.

  Se si usa questa impostazione quando siete in `mode 0` o `2` (le due modalità di bilanciamento del carico) l'interruttore della rete deve essere configurato in modo da distribuire i pacchetti in modo uniforme attraverso i NIC. Per maggiori informazioni su come eseguire tale operazione, consultate `/usr/share/doc/kernel-doc-<kernel-version>/Documentation/networking/bonding.txt`.

  Per default il valore è impostato su `0`, il quale lo disabilita.
- `arp_ip_target=` — Specifica l'indirizzo IP target delle richieste ARP quando il parametro `arp_interval` è abilitato. Si possono specificare fino a 16 indirizzi IP in un elenco separato da una virgola.
- `primary=` — Specifica il nome dell'interfaccia, come ad esempio `eth0`, del dispositivo primario. Il dispositivo `primary` è il primo delle interfacce di tipo 'bonding' da usare, e non viene abbandonato fino a quando non presenta un errore. Questa impostazione è particolarmente utile quando un NIC nell'interfaccia 'bonding' è più veloce, e perciò, in grado di gestire un carico maggiore.

  Questa impostazione è valida solo quando l'interfaccia 'bonding' è in modalità active-backup. Per maggiori informazioni consultate `/usr/share/doc/kernel-doc-<kernel-version>/Documentation/networking/bonding.txt`.
- `multicast=` — Specifica un valore intero per il supporto multicast desiderato.

  Valori accettabili per questo parametro sono:

  - `0` — Disabilita il supporto multicast.
  - `1` — Abilita il supporto multicast, ma solo sullo slave attivo.
  - `2` — Abilita il supporto multicast su tutti gli slave (il default).

Importante

È importante che i parametri `arp_interval` e`arp_ip_target` o `miimon` siano specificati. In caso contrario si può verificare una degradazione delle prestazioni della rete in caso di presenza di un errore del link.

Consultate:

`/usr/share/doc/kernel-doc-<kernel-version>/Documentation/networking/bonding.txt`

per informazioni più dettagliate sulle interfacce bonding.

Indice

Simboli

.fetchmailrc, 178
  opzioni del server, 180
  opzioni globali, 179
  opzioni utente, 180
.procmailrc, 182
/etc/named.conf
  (Vd. BIND)
/etc/pam.conf, 267
  (Vd. Anche PAM)
/etc/pam.d, 267
  (Vd. Anche PAM)
/lib/security/, 267
  (Vd. Anche PAM)
/lib64/security/, 267
  (Vd. Anche PAM)

A

aboot, 3
AccessFileName
  direttiva di configurazione di Apache, 154
Action
  direttiva di configurazione di Apache, 159
AddDescription
  direttiva di configurazione di Apache, 158
AddEncoding
  direttiva di configurazione di Apache, 159
AddHandler
  direttiva di configurazione di Apache, 159
AddIcon
  direttiva di configurazione di Apache, 158
AddIconByEncoding
  direttiva di configurazione di Apache, 158
AddIconByType
  direttiva di configurazione di Apache, 158
AddLanguage
  direttiva di configurazione di Apache, 159
AddType
  direttiva di configurazione di Apache, 159
Alias
  direttiva di configurazione di Apache, 157
Allow
  direttiva di configurazione di Apache, 153
AllowOverride
  direttiva di configurazione di Apache, 153
ambienti desktop
  (Vd. X)
Apache
  (Vd. Server HTTP Apache)
arresto, 8
  (Vd. Anche interruzione)
attacco Denial of Service
    (Vd. Attacco Denial of Service)
  definizione di, 74
attivazione della vostra sottoscrizione, vii
autofs, 127
  (Vd. Anche NFS)

B

Basic Input/Output System
  (Vd. BIOS)
Berkeley Internet Name Domain
  (Vd. BIND)
BIND
  caratteristiche, 208
    IPv6, 209
    miglioramenti DNS, 208
    sicurezza, 209
    visualizzazioni multiple, 209
  configurazione di
    direttive dei file zone, 201
    esempi di file zone, 204
    esempi di istruzione zone, 199
    informazione sulla risorsa del file zone, 202
    risoluzione nomi inversa, 205
  demone named, 194
  errori comuni, 209
  file di configurazione
    /etc/named.conf, 194, 195
    directory /var/named/, 194
    file zone, 201
  introduzione, 193, 193
  programma rndc, 206
    /etc/rndc.conf, 207
    configurazione delle chiavi, 207
    configurazione di named per l'uso di, 206
    opzioni della linea di comando, 207
  risorse aggiuntive, 210
    documentazione installata, 210
    libri correlati, 211
    siti Web utili, 211
  server dei nomi
    definizione di, 193
  server dei nomi root
    definizione di, 193
  tipi di server dei nomi
    caching-only, 194
    forwarding, 194
    master, 194
    slave, 194
  zone
    definizione di, 193
BIOS
  definizione di, 1
    (Vd. Anche processo di avvio)

boot loader, 9
(Vd. Anche GRUB)
definizione di, 9
tipi di
ELILO, 9
GRUB, 9
OS/400, 9
YABOOT, 9
z/IPL, 9
BrowserMatch
direttiva di configurazione di Apache, 160

C

Cache TLB
(Vd. hugepage)
CacheNegotiatedDocs
direttiva di configurazione di Apache, 155
channel bonding
configurazione del modulo , 336
direttive del modulo, 337
interfaccia
configurazione di, 111
chkconfig, 8
(Vd. Anche servizi)
comando init, 3
(Vd. Anche processo di avvio)
accesso ai runlevel da parte del, 7
file di configurazione
/etc/inittab, 7
i runlevel
directory utilizzate da, 7
ruolo nel processo di avvio, 3
(Vd. Anche processo di avvio)
SysV init
definizione di, 7
Comando ldapadd, 215
(Vd. Anche LDAP)
Comando ldapdelete, 215
(Vd. Anche LDAP)
Comando ldapmodify, 215
(Vd. Anche LDAP)
Comando ldappasswd, 215
(Vd. Anche LDAP)
Comando ldapsearch, 215
(Vd. Anche LDAP)
comando setserial
configurazione, 6
Comando slapadd, 215
(Vd. Anche LDAP)
Comando slapcat, 215
(Vd. Anche LDAP)
Comando slapd, 215
(Vd. Anche LDAP)
Comando slapindex, 215
(Vd. Anche LDAP)
Comando slappasswd, 215
(Vd. Anche LDAP)
Comando slurpd, 215
(Vd. Anche LDAP)
configurazione
host virtuali, 164
Server HTTP Apache, 147
configurazione SSL, 162
controllo dell'accesso, 277
convenzioni
documento, iv
copiare e incollare testi
usando X, ix
CustomLog
direttiva di configurazione di Apache, 156

D

DefaultIcon
direttiva di configurazione di Apache, 158
DefaultType
direttiva di configurazione di Apache, 155
demone named
(Vd. BIND)
Denial of Service
prevenzione nell'uso di xinetd, 290
(Vd. Anche xinetd)
Deny
direttiva di configurazione di Apache, 154
directory
/boot/, 20
/dev/, 20
/etc/, 20
/lib/, 20
/media/, 20
/mnt/, 20
/opt/, 21
/proc/, 21
/sbin/, 21
/srv/, 22
/sys/, 22
/usr/, 22
/usr/local/, 23
/var/, 23
direttiva di configurazione di Apache, 152
directory /boot/, 20
directory /etc/sysconfig/
(Vd. directory sysconfig)
directory /usr/local/, 23
directory /var/spool/up2date/, 24
directory dev, 20
directory etc, 20
Directory initrd, 24
directory lib, 20

directory media, 20
directory mnt, 20
directory opt, 21
directory proc, 21
(Vd. filesystem proc)
directory public_html, 154
directory sbin, 21
directory srv, 22
directory sys, 22
directory sysconfig, 24
/etc/sysconfig/amd, 28
/etc/sysconfig/apmd, 28
/etc/sysconfig/arpwatch, 29
/etc/sysconfig/authconfig, 29
/etc/sysconfig/autofs, 29
/etc/sysconfig/clock, 30
/etc/sysconfig/desktop, 30
/etc/sysconfig/devlabel, 31
/etc/sysconfig/dhcpd, 31
/etc/sysconfig/exim, 31
/etc/sysconfig/firstboot, 31
/etc/sysconfig/gpm, 32
/etc/sysconfig/harddisks, 32
/etc/sysconfig/hwconf, 32
/etc/sysconfig/init, 33
/etc/sysconfig/ip6tables-config, 33
/etc/sysconfig/iptables, 302
/etc/sysconfig/iptables-config, 34
/etc/sysconfig/irda, 34
/etc/sysconfig/keyboard, 35
/etc/sysconfig/kudzu, 35
/etc/sysconfig/mouse, 35
/etc/sysconfig/named, 36
/etc/sysconfig/netdump, 36
/etc/sysconfig/network, 36
/etc/sysconfig/ntpd, 37
/etc/sysconfig/pcmcia, 37
/etc/sysconfig/radvd, 37
/etc/sysconfig/rawdevices, 38
/etc/sysconfig/samba, 38
/etc/sysconfig/selinux, 38
/etc/sysconfig/sendmail, 38
/etc/sysconfig/spamassassin, 38
/etc/sysconfig/squid, 39
/etc/sysconfig/system-config-securitylevel , 39
/etc/sysconfig/system-config-users, 39
/etc/sysconfig/system-logviewer, 39
/etc/sysconfig/tux, 39
/etc/sysconfig/vncservers, 39
/etc/sysconfig/xinetd, 40
directory /etc/sysconfig/apm-scripts, 40
directory /etc/sysconfig/cbq, 40
directory /etc/sysconfig/network-scripts, 107, 40
(Vd. Anche rete)
directory /etc/sysconfig/networking, 40
directory /etc/sysconfig/rhn, 40
i file trovati nella, 27
informazione addizionale per, 27
risorse addizionali, 41
documentazione installata, 41
sottodirectory nella, 40
directory usr, 22
directory var, 23
directory var/lib/rpm/, 24
DirectoryIndex
direttiva di configurazione di Apache, 154
direttive della cache per Apache, 161
direttive di configurazione, Apache, 147
AccessFileName, 154
Action, 159
AddDescription, 158
AddEncoding, 159
AddHandler, 159
AddIcon, 158
AddIconByEncoding, 158
AddIconByType, 158
AddLanguage, 159
AddType, 159
Alias, 157
Allow, 153
AllowOverride, 153
BrowserMatch, 160
CacheNegotiatedDocs, 155
configurazione SSL, 162
CustomLog, 156
DefaultIcon, 158
DefaultType, 155
Deny, 154
Directory, 152
DirectoryIndex, 154
DocumentRoot, 152
ErrorDocument, 160
ErrorLog, 155
ExtendedStatus, 150
Group, 151
HeaderName, 158
HostnameLookups, 155
IfDefine, 150
IfModule, 148
Include, 150
IndexIgnore, 159
IndexOptions, 157
KeepAlive, 148
(Vd. Anche KeepAliveTimeout)
risoluzione dei problemi, 148
KeepAliveTimeout, 148
LanguagePriority, 159
Listen, 149
LoadModule, 150
Location, 160
LogFormat
opzioni del formato, 155

LogLevel, 155
MaxClients, 149
MaxKeepAliveRequests, 148
MaxRequestsPerChild, 149
MaxSpareServers, 149
MaxSpareThreads, 149
MinSpareServers, 149
MinSpareThreads, 149
NameVirtualHost, 161
Options, 153
Order, 153
per la funzionalità della cache, 161
PidFile, 147
Proxy, 161
ProxyRequests, 161
ReadmeName, 158
Redirect, 157
ScriptAlias, 157
ServerAdmin, 151
ServerName, 152
ServerRoot, 147
ServerSignature, 156
SetEnvIf, 162
StartServers, 148
SuexecUserGroup, 141, 151
ThreadsPerChild, 149
Timeout, 147
TypesConfig, 155
UseCanonicalName, 152
User, 151
UserDir, 154
VirtualHost, 162
display managers
(Vd. X)
dispositivi a blocchi, 47
(Vd. Anche /proc/devices)
definizione di, 47
dispositivi a carattere, 47
(Vd. Anche /proc/devices)
definizione di, 47
dispositivi, locali
proprietà dei, 274
(Vd. Anche PAM)
dispositivo frame buffer, 48
(Vd. Anche /proc/fb)
DNS, 193
(Vd. Anche BIND)
introduzione, 193
documentazione
guru, iv
ricerca, ii
utenti esperti, iv
utenti inesperti, ii
newsgroup, iii
siti Web, iii
DocumentRoot
direttiva di configurazione di Apache, 152
modifica, 164
modifica della condivisione, 166
DoS
(Vd. Denial of Service)
drag-and-drop, ix
driver
(Vd. moduli del kernel)
DSO
caricamento, 164

E

e-mail
Fetchmail, 178
Postfix, 176
Procmail, 181
protocolli, 169
IMAP, 170
POP, 170
SMTP, 169
risorse aggiuntive, 189
documentazione installata, 189
libri correlati, 191
siti Web utili, 190
Sendmail, 172
sicurezza, 188
client, 188
server, 188
spam
filtrare, 187
storia di, 169
tipi
Mail Delivery Agent, 172
Mail Transfer Agent, 171
Mail User Agent, 172
tipi di programmi, 171
ELILO, 3, 9
(Vd. Anche boot loader)
epoca, 59
(Vd. Anche /proc/stat)
definizione di, 59
ErrorDocument
direttiva di configurazione di Apache, 160
ErrorLog
direttiva di configurazione di Apache, 155
Ethernet
(Vd. rete)
exec-shield
attivazione, 70
introduzione, 70
ExtendedStatus
direttiva di configurazione di Apache, 150

F

Fetchmail, 178
  opzioni di comando, 181
    informative, 181
    speciali, 181
  opzioni di configurazione, 178
    opzioni del server, 180
    opzioni globali, 179
    opzioni utente, 180
  risorse aggiuntive, 189
FHS, 19, 19
  (Vd. Anche filesystem)
  (Vd. Anche filesystem)
file di accesso degli host
  (Vd. wrapper TCP)
file virtuali
  (Vd. filesystem proc)
file, fylesystem proc
  cambiare, 44, 79
  visualizzazione, 43, 79
filesystem
  FHS standard, 19
  gerarchia, 19
  organizzazione, 19
  struttura, 19
  virtuale
    (Vd. filesystem proc)
filesystem proc
  /proc/apm, 45
  /proc/buddyinfo, 45
  /proc/cmdline, 46
  /proc/cpuinfo, 46
  /proc/crypto, 47
  /proc/devices
    dispositivi a blocchi, 47
    dispositivi a carattere, 47
  /proc/dma, 48
  /proc/execdomains, 48
  /proc/fb, 48
  /proc/filesystems, 49
  /proc/interrupts, 49
  /proc/iomem, 50
  /proc/ioports, 51
  /proc/kcore, 51
  /proc/kmsg, 51
  /proc/loadavg, 52
  /proc/locks, 52
  /proc/mdstat, 52
  /proc/meminfo, 53
  /proc/misc, 54
  /proc/modules, 55
  /proc/mounts, 55
  /proc/mtrr, 56
  /proc/partitions, 56
  /proc/pci
    visualizzazione mediante lspci, 57
  /proc/slabinfo, 58
  /proc/stat, 59
  /proc/swaps, 60
  /proc/sysrq-trigger, 60
  /proc/uptime, 60
  /proc/version, 60
  directory /proc/bus/, 63
  directory /proc/driver/, 63
  directory /proc/fs/, 64
  directory /proc/ide/, 64
    directory dei dispositivi, 64
  directory /proc/irq/, 65
  directory /proc/net/, 66
  directory /proc/scsi/, 67
  directory /proc/self/, 62
  directory /proc/sys/, 68, 79
      (Vd. Anche sysctl)
    /proc/sys/kernel/exec-shield, 70
    /proc/sys/kernel/sysrq
      (Vd. tasto SysRq)
    directory /proc/sys/dev/, 69
    directory /proc/sys/fs/, 70
    directory /proc/sys/kernel/, 70
    directory /proc/sys/net/, 74
    directory /proc/sys/vm/, 76
  directory /proc/sysvipc/, 78
  directory /proc/tty/, 78
  directory del processo, 61
  file nel, di livello superiore, 44
  introduzione, 43
  modifica dei file nel, 44, 68, 79
  risorse aggiuntive, 79
    documentazione installata, 79
    siti Web utili, 80
  sottodirectory nel, 60
  visualizzazione dei file nel, 43
filesystem virtuale
  (Vd. filesystem proc)
filtraggio di pacchetti
  (Vd. iptables)
formati degli eseguibili, 48
    (Vd. Anche /proc/execdomains)
  definizione di, 48
FrontPage, 145
fstab, 127
  (Vd. Anche NFS)
FTP, 251
      (Vd. Anche vsftpd)
  definizione di , 251
  introduzione, 251
  modalità attiva, 251
  modalità passiva, 251
  porta dati, 251
  porta di comando, 251
  software del server

Red Hat Content Accelerator, 252
vsftpd, 252

G

gerarchia, filesystem, 19
GNOME, 90
(Vd. Anche X)
Group
direttiva di configurazione di Apache, 151
GRUB, 9, 2
(Vd. Anche boot loader)
(Vd. Anche boot loaders)
caratteristiche, 10
comandi, 14
definizione di, 9
file di configurazione
/boot/grub/grub.conf, 16
struttura, 16
file di configurazione del menu, 16
direttive, 16
installazione, 11
interfacce, 13
a menu, 13
editor voci di menu, 13
linea di comando, 13
ordine di, 14
Modifica dei runlevel all'avvio, 17
modifica dei runlevel con, 13
processo di avvio, 9
risorse aggiuntive, 18
documentazione installata, 18
libri correlati, 18
siti Web utili, 18
ruolo nel processo di avvio, 2
terminologia, 11
dispositivi, 11
file, 12
root file system, 13
grub.conf, 16
(Vd. Anche GRUB)
gruppi
directory condivise, 86
GID, 81
introduzione, 81
risorse aggiuntive, 87
documentazione installata, 87
libri relativi, 88
standard, 83
strumenti per la gestione di
groupadd, 81, 85
redhat-config-users, 85
Utente Manager, 81
utenti privati, 85

H

HeaderName
direttiva di configurazione di Apache, 158
host virtuali
basati sul nome, 164
comando Listen, 165
configurazione, 164
include lato server, 159
Options, 153
HostnameLookups
direttiva di configurazione di Apache, 155
hosts.allow
(Vd. wrapper TCP)
hosts.deny
(Vd. wrapper TCP)
httpd.conf
(Vd. direttive di configurazione, Apache)
hugepage
configurazione di , 76

I

i runlevel
(Vd. comando init)
configurazione di, 8
(Vd. Anche servizi)
IfDefine
direttiva di configurazione di Apache, 150
ifdown, 115
IfModule
direttiva di configurazione di Apache, 148
ifup, 115
Include
direttiva di configurazione di Apache, 150
include lato server, 153, 159
IndexIgnore
direttiva di configurazione di Apache, 159
IndexOptions
direttiva di configurazione di Apache, 157
interruzione, 8
(Vd. Anche arresto)
introduzione, i
ip6tables
introduzione, 305
script di controllo
arresto, 303
inizio, 303
panic, 303
riavvio, 303
salvare, 303
stato, 303
ipchains
(Vd. iptables)
IPsec
(Vd. rete)

iptables
/sbin/iptables-restore, 302
/sbin/iptables-save, 302
catene
target, 293
concetti base sul filtraggio dei pacchetti, 293
elenco delle regole, 293
file di configurazione
/etc/sysconfig/iptables, 302
/etc/sysconfig/iptables-config, 304
/etc/sysconfig/iptables.save, 302
opzioni, 295
comandi, 296
elenco, 302
parametri, 297
struttura di, 296
target, 301
opzioni estese, 298
moduli, 300
panoramica su, 293
paragonato a ipchains, 295
protocolli
ICMP, 299
TCP, 298
UDP, 299
risorse aggiuntive, 305
documentazione installata, 305
siti Web utili, 305
salvataggio delle regole, 302
script di controllo
arresto, 303
inizio, 303
panic, 303
riavvio, 303
salvare, 302, 303
stato, 303
tabelle, 293

K

KDE, 90
(Vd. Anche X)
KeepAlive
direttiva di configurazione di Apache, 148
KeepAliveTimeout
direttiva di configurazione di Apache, 148
Kerberos
Authentication Server (AS), 310
configurazione del server, 311
configurazione di client, 313
definizione di, 307
e PAM, 311
funzionamento, 310
Key Distribution Center (KDC), 310
Risorse aggiuntive, 314
Documentazione installata, 314
siti Web utili, 315
svantaggi di, 307
terminologia, 308
Ticket granting Service(TGS), 310
Ticket granting Ticket (TGT), 310
vantaggi di, 307
kernel
ruolo nel processo di avvio, 3
kwin, 90
(Vd. Anche X)

L

LanguagePriority
direttiva di configurazione di Apache, 159
LDAP
aggiornamento delle directory, 222
applicazioni
ldapadd, 215
ldapdelete, 215
ldapmodify, 215
ldappasswd, 215
ldapsearch, 215
slapadd, 215
slapcat, 215
slapd, 215
slapindex, 215
slappasswd, 215
slurpd, 215
Suite OpenLDAP, 215
utility, 215
applicazioni del client, 217
Contenuti di OpenLDAP, 213
definizione di , 213
demoni, 215
file di configurazione
/etc/ldap.conf, 217
/etc/openldap/ldap.conf, 217
/etc/openldap/slapd.conf, 217, 219
directory /etc/openldap/schema/, 217, 218
impostazione, 218
migrazione delle directory più vecchie, 222
LDAPv2, 213
LDAPv3, 213
LDIF
formato di , 214
risorse aggiuntive, 222
documentazione installata, 222
libri correlati, 224
siti Web utili, 223
terminologia, 214
utilizzato con NSS, 216
utilizzato con PAM, 216
utilizzato con PHP4, 216

utilizzato con Server HTTP Apache, 216
utilizzo per l'autenticazione, 220
impostazione dei client, 220
modifica di /etc/ldap.conf, 220
modifica di /etc/nsswitch.conf, 220
modifica di /etc/openldap/ldap.conf, 220
modifica di slapd.conf, 220
pacchetti, 220
PAM, 221
Strumento di Configurazione per l'Autenticazione, 220
vantaggi di , 213
Lightweight Directory Access Protocol
(Vd. LDAP)
LILO, 2
(Vd. Anche boot loaders)
ruolo nel processo di avvio, 2
Listen
direttiva di configurazione di Apache, 149
LoadModule
direttiva di configurazione di Apache, 150
Location
direttiva di configurazione di Apache, 160
LogFormat
direttiva di configurazione di Apache, 155
LogLevel
direttiva di configurazione di Apache, 155
lspci, 57

M

Mail Delivery Agent
(Vd. e-mail)
Mail Transfer Agent
(Vd. e-mail)
Mail User Agent
(Vd. e-mail)
Master Boot Record
(Vd. MBR)
(Vd. MBR)
MaxClients
direttiva di configurazione di Apache, 149
MaxKeepAliveRequests
direttiva di configurazione di Apache, 148
MaxRequestsPerChild
direttiva di configurazione di Apache, 149
MaxSpareServers
direttiva di configurazione di Apache, 149
MaxSpareThreads
direttiva di configurazione di Apache, 149
MBR
definizione di, 1, 1
(Vd. Anche boot loaders)
(Vd. Anche processo di avvio)
MDA
(Vd. Mail Delivery Agent)
metacity, 90
(Vd. Anche X)
MinSpareServers
direttiva di configurazione di Apache, 149
MinSpareThreads
direttiva di configurazione di Apache, 149
moduli
(Vd. moduli del kernel)
(Vd. moduli del kernel)
Apache
caricamento, 164
personali, 164
predefiniti, 163
moduli del kernel
introduzione, 333
Moduli Ethernet
parametri, 334
supporto schede multiple, 336
moduli SCSI
parametri, 334
parametri del modulo
specificare, 333
tipi di, 333
moduli di autenticazione
(Vd. PAM)
moduli di Server HTTP Apache, 163
Moduli Ethernet
(Vd. moduli del kernel)
moduli NIC
(Vd. moduli del kernel)
moduli SCSI
(Vd. moduli del kernel)
mouse
utilizzo, viii
MTA
(Vd. Mail Transfer Agent)
MUA
(Vd. Mail User Agent)
mwm, 90
(Vd. Anche X)

N

named.conf
(Vd. BIND)
NameVirtualHost
direttiva di configurazione di Apache, 161
netfilter
(Vd. iptables)
Network File System
(Vd. NFS)
NFS
arresto, 122
avvio, 122
client
/etc/fstab, 127
autofs, 127
configurazione, 126
opzioni di montaggio, 128
come funziona, 119
condrestart, 122
configurazione del server, 123
/etc/exports, 123
comando exportfs, 125
comando exportfs con NFSv4, 126
introduzione, 119
portmap, 121
riavvio, 122
ricaricare, 122
risorse aggiuntive, 131
documentazione installata, 132
libri correlati, 132
siti web utili, 132
servizi richiesti, 120
sicurezza, 130
accesso host, 130
accesso host NFSv2/NFSv3, 130
accesso host NFSv4, 131
permessi dei file, 131
stato, 122
TCP, 119
UDP, 119
ntsysv, 8
(Vd. Anche servizi)

O

oggetti, dinamicamente condivisi
(Vd. DSO)
OpenLDAP
(Vd. LDAP)
OpenSSH, 317
(Vd. Anche SSH)
file di configurazione per, 320
Options
direttiva di configurazione di Apache, 153
Order
direttiva di configurazione di Apache, 153
OS/400, 9
(Vd. Anche boot loader)

P

PAM
definizione di, 267
file di configurazione, 267
file di configurazione di esempio, 270
file di servizio, 267
Kerberos e, 311
moduli, 268
argomenti, 269
componenti, 268
creazione, 272
interfacce, 268
percorsi dei, 269
stacking, 268, 270
opzioni di controllo, 269
pam_console
definizione di, 274
pam_timestamp
definizione di, 272
direttive, 273
eliminazione dei timestamp, 273
icona di autenticazione e , 272
pam_timestamp_check
eliminare il timestamp usando , 273
password shadow, 270
risorse aggiuntive, 275
documentazione installata, 275
siti Web utili, 275
vantaggi di, 267
pam_console
(Vd. PAM)
pam_timestamp
(Vd. PAM)
pam_timestamp_check
(Vd. PAM)
parametri del modulo
(Vd. moduli del kernel)
password, 270
(Vd. Anche PAM)
password shadow, 270
shadow, 86
password Shadow
panoramica di, 86
PidFile
direttiva di configurazione di Apache, 147
pool di slab
(Vd. /proc/slabinfo)
porte seriali
(Vd. comando setserial)
portmap, 121

(Vd. Anche NFS)
NFS, 121
rpcinfo, 121
stato, 122
Postfix, 176
installazione predefinita, 177
prefdm
(Vd. X)
processo di avvio, 1, 1
(Vd. Anche boot loaders)
caricamento a catena, 9
caricamento diretto, 9
fasi del, 1, 1
BIOS, 1
boot loader, 2
comando /sbin/init, 3
kernel, 3
shell EFI, 1
per x86, 1
Procmail, 181
configurazione, 182
regole, 183
azioni speciali, 185
condizioni speciali, 185
distribuzione, 184
esempi, 185
file di lock locali, 185
flag, 184
non distribuzione, 184
SpamAssassin, 187
risorse aggiuntive, 189
programma findsmb, 242
programma make_smbcodepage, 243
programma make_unicodemap, 243
programma net, 243
programma nmblookup, 244
programma pdbedit, 244
programma rpcclient, 245
programma smbcacls, 245
programma smbclient, 245
programma smbcontrol, 245
programma smbgroupedit, 246
programma smbmount, 246
programma smbpasswd, 246
programma smbspool, 246
programma smbstatus, 246
programma smbtar, 246
programma testparm, 247
programma testprns, 248
programma wbinfo, 248
programmi
esecuzione all'avvio, 6
protocollo SSH, 317
autenticazione, 319
caratteristiche di, 317
file di configurazione, 320
inoltro X11, 321
livelli di
canali, 320
livello di trasporto, 319
pericoli per la sicurezza, 317
Port forwarding, 322
protocolli non sicuri e, 323
richiesta per le connessioni remote, 323
risorse aggiuntive, 323
documentazione installata, 323
libri relativi, 324
siti web utili, 324
sequenza di connessione, 318
version 1, 318
version 2, 318
Proxy
direttiva di configurazione di Apache, 161
ProxyRequests
direttiva di configurazione di Apache, 161

R

rc.local
modifica, 6
rc.serial, 6
(Vd. Anche comando setserial)
ReadmeName
direttiva di configurazione di Apache, 158
Red Hat Enterprise Linux-posizione specifica dei file
/etc/sysconfig/, 24
(Vd. Anche directory sysconfig)
/var/lib/rpm/, 24
/var/spool/up2date/, 24
Redirect
direttiva di configurazione di Apache, 157
registrazione della sottoscrizione, vii
registrazione della vostra sottoscrizione, vii
rete
comandi
/sbin/ifdown, 115
/sbin/ifup, 115
/sbin/service network, 115
configurazione, 108
funzioni, 116
interfacce, 108
alias, 112
channel bonding, 111
clone, 112
dialup, 113
Ethernet, 108
IPsec, 110
risorse addizionali, 116
script, 107
risoluzione dei problemi
log degli errori, 155

rpcinfo, 121
runlevel
  modifica con GRUB, 13

S

Samba
    (Vd. Samba)
  Abilità, 225
  Backend del database compatibili all'indietro, 238
  Browsing, 239
  Browsing della rete, 239
    Browsing del Dominio, 241
    Browsing del Workgroup, 239
    WINS, 241
  Database d'informazione sull'account, 238
    ldapsam, 239
    ldapsam_compat, 238
    mysqlsam, 239
    smbpasswd, 238
    tdbsam, 239
    Testo normale, 238
    xmlsam, 239
  demone, 226
    nmbd, 226
    panoramica, 226
    smbd, 226
    winbindd, 226
  Introduzione, 225
  Modalità di sicurezza, 236
    Modalità di Sicurezza del Dominio, 237
    Modalità di sicurezza del server, 237
    Modalità di sicurezza dell'Active Directory, 237
    Share-Level Security, 237
    User Level Security, 236
  Nuovi Backend del database, 239
  Programmi, 242
    findsmb, 242
    make_smbcodepage, 243
    make_unicodemap, 243
    net, 243
    nmblookup, 244
    pdbedit, 244
    rpcclient, 245
    smbcacls, 245
    smbclient, 245
    smbcontrol, 245
    smbgroupedit, 246
    smbmount, 246
    smbpasswd, 246
    smbspool, 246
    smbstatus, 246
    smbtar, 246
    testparm, 247
    testprns, 248
    wbinfo, 248
  Riferimento, 225
  Risorse aggiuntive, 248
    documentazione installata, 248
    libri correlati, 248
    Risorse di Red Hat, 248
    siti web utili, 248
  servizio
    arresto, 226
    avvio , 226
    riavvio, 226
    riavvio condizionato, 226
    ricarica, 226
  smb.conf, 227
    BDC usando LDAP, 235
    Esempio di Active Directory Member Server, 230
    Esempio di file sicuro e di server di stampa, 229
    Esempio di Lettura/Scrittura anonima, 228
    Esempio di server di stampa anonimo, 229
    Esempio di sola-lettura anonima, 228
    Esempio di un membro del dominio stile NT4, 231
    PDC usando LDAP, 234
    PDC usando tdbsam, 232
    PDC utilizzando Active Directory, 236
  Supporto di stampa CUPS, 241
    CUPS smb.conf, 241
  Tipi di server, 227
    Controller del Dominio, 232
    Membro del Dominio, 230
    Stand Alone, 228
  WINS, 241
script CGI
  al di fuori della direttiva ScriptAlias, 159
  esecuzione dei programmi esterni a cgi-bin, 152
ScriptAlias
  direttiva di configurazione di Apache, 157
SELinux, 325
  file correlati, 325
    /etc/sysconfig/selinux, 326
    configurazione, 326
    Directory /etc/selinux/, 327
    pseudo-file system /selinux/, 325
    utilities, 328
  introduzione, 325
  risorse aggiuntive, 328
    documentazione, 328
    documentazione installata, 328
    siti web, 329
Sendmail, 172
  alias, 174
  con UUCP, 174
  installazione predefinita, 173
  LDAP e, 176
  limiti, 172

masquerading, 174
modifiche comuni alla configurazione, 174
risorse aggiuntive, 189
scopo, 172
spam, 175
server dei nomi
(Vd. BIND)
server dei nomi caching-only
(Vd. BIND)
server dei nomi forwarding
(Vd. BIND)
server dei nomi master
(Vd. BIND)
server dei nomi root
(Vd. BIND)
server dei nomi slave
(Vd. BIND)
Server HTTP Apache
1.3
migrazione alla 2.0, 135
2.0
caratteristiche di, 133
direttive MPM specifiche, 148
migrazione dalla 1.3, 135
modifiche ai pacchetti, 134
modifiche al filesystem, 134
avvio, 146
chiusura, 146
configurazione, 147
file di log
/var/log/httpd/error_log, 147
formato del file di log combinato, 155, 156
formato di , 155
risoluzione dei problemi con, 147, 148
usare i tool analayzer di log con, 155
introduzione, 133
lavorare in modalità non sicura, 164
migrazione alla 2.0, 135
configurazione dell'host virtuale, 140
dimensione del pool del server, 136
Direttiva UserDir, 138
direttive rimosse, 137
error documents, 139
Indicizzare la directory, 139
LDAP, 145
logging, 138
modifiche al modulo del sistema, 140
mod_auth_db, 142
mod_auth_dbm, 142
mod_include, 142
mod_perl, 143
mod_proxy, 142
mod_ssl, 141
negoziazione del contenuto, 139
PHP, 144
porte e indirizzi bind, 135
SuexecUserGroup, 141, 151
Supporto DSO, 137
Moduli di processazione multipla
attivazione dell'MPM worker, 136
prefork, 136
worker, 136
report sullo stato del server, 160
riavvio, 146
ricaricamento, 146
risoluzione dei problemi, 147
risorse aggiuntive, 166
libri correlati, 166
siti Web utili, 166
server proxy, 161, 161
ServerAdmin
direttiva di configurazione di Apache, 151
ServerName
direttiva di configurazione di Apache, 152
ServerRoot
direttiva di configurazione di Apache, 147
ServerSignature
direttiva di configurazione di Apache, 156
servizi
configurazione con chkconfig, 8
configurazione con ntsysv, 8
configurazione con Strumento di configurazione dei servizi, 8
SetEnvIf
direttiva di configurazione di Apache, 162
shadow
(Vd. password)
shell EFI
definizione di, 1
(Vd. Anche processo di avvio)
shell Extensible Firmware Interface
(Vd. shell EFI)
sicurezza
eseguire Apache senza, 164
sistema X Window
(Vd. X)
SpamAssassin
usare con Procmail, 187
StartServers
direttiva di configurazione di Apache, 148
startx
(Vd. X)
Strumento di configurazione dei servizi, 8
(Vd. Anche servizi)
Strumento di Configurazione per l'Autenticazione e LDAP, 220, 221
stunnel, 188
SuexecUserGroup
direttiva di configurazione di Apache, 141, 151
suggerimenti
come contattarci per inviarci informazioni, ix
sysctl

configurazione con /etc/sysctl.conf/, 79
controllo con /proc/sys/, 79
SysRq
(Vd. tasto SysRq)
System Request Key
definizione di, 68
impostazione del timing per , 70
SysV init
(Vd. comando init)

T

tasto SysRq
attivazione, 68
ThreadsPerChild
direttiva di configurazione di Apache, 149
Timeout
direttiva di configurazione di Apache, 147
twm, 90
(Vd. Anche X)
TypesConfig
direttiva di configurazione di Apache, 155

U

UseCanonicalName
direttiva di configurazione di Apache, 152
User
direttiva di configurazione di Apache, 151
user private group
(Vd. gruppi)
e directory condivise, 86
UserDir
direttiva di configurazione di Apache, 154
utenti
/etc/passwd, 82
directory HTML personali, 154
introduzione, 81
risorse aggiuntive, 87
documentazione installata, 87
libri relativi, 88
standard, 82
strumenti per la gestione di
useradd, 81
Utente Manager, 81
UID, 81
utility Apache APXS, 164

V

VirtualHost
direttiva di configurazione di Apache, 162
vsftpd, 252
(Vd. Anche FTP)
arresto, 253
avvio, 253
avvio di copie multiple di , 254
condrestart, 253
configurazione multihome, 254
contenuti sulla sicurezza, 252
file di configurazione
/etc/vsftpd/vsftpd.conf, 255
controlli d'accesso, 256
formato di , 255
opzioni del demone, 256
opzioni del trasferimento del file, 260
opzioni dell'utente locale, 258
opzioni della directory, 259
opzioni della rete, 261
opzioni di Logging, 260
opzioni di login, 256
opzioni per l'utente anonimo, 257
riavvio, 253
risorse aggiuntive, 263
documentazione installata, 263
libri correlati, 264
siti web utili, 264
RPM
file installati da , 253
stato, 253

W

Web server non sicuro
disabilitazione, 166
webmaster
indirizzo e-mail per, 151
window manager
(Vd. X)
wrapper TCP, 285
(Vd. Anche xinetd)
definizione di, 278
file di configurazione
/etc/hosts.allow, 278, 278
/etc/hosts.deny, 278, 278
campi di opzione, 282
caratteri jolly, 280
espansioni, 284
file di accesso degli host, 278
formattazione delle regole all'interno, 279
modelli, 281
operatori, 282
opzione del comando della shell, 283
opzione di controllo d'accesso, 283

opzione di registrazione, 282
spawn opzione, 283
twist opzione, 283
introduzione, 277
risorse aggiuntive, 290
documentazione installata, 290
libri correlati, 291
siti Web utili, 291
vantaggi di, 278

X

X
/etc/X11/xorg.conf
Device, 95
DRI, 97
Etichetta Section, 91
introduzione, 91
Monitor, 94
Screen, 96
sezione Files, 93
sezione InputDevice, 94
sezione Module, 93
sezione ServerFlags, 92
sezioni ServerLayout, 92
struttura di, 91
valori boolean per, 91
ambienti desktop
GNOME, 90
KDE, 90
client X, 89, 90
ambienti desktop, 90
commandstartx, 100
commandxinit, 100
window manager, 90
display managers
configurazione preferita, 101
definizione di, 101
GNOME, 101
KDE, 101
script prefdm, 101
xdm, 101
file di configurazione
/etc/X11/xorg.conf, 91
directory /etc/X11/, 91
opzioni del server, 91
opzioni incluse nei, 91
font
configurazione xfs, 99
Estensione X Render, 97
Fontconfig, 97
Fontconfig, aggiunta di font a, 98
FreeType, 97
introduzione, 97
sottosistema del core X font, 99
X Font Server, 99
xfs, 99
xfs, aggiungere font a, 100
Xft, 97
introduzione, 89
risorse aggiuntive, 102
documentazione installata, 102
libri correlati, 103
siti Web utili, 102
runlevel
3, 100
5, 101
runlevel e, 100
Server X, 89
caratteristiche di, 89
utilities
system-config-display, 89
window manager
kwin, 90
metacity, 90
mwm, 90
twm, 90
X.500
(Vd. LDAP)
X.500 Lite
(Vd. LDAP)
xinetd, 285
(Vd. Anche wrapper TCP)
attacchi DoS e, 290
file di configurazione, 285
/etc/xinetd.conf, 285
directory /etc/xinetd.d/, 286
Opzioni di amministrazione delle risorse, 290
opzioni di collegamento, 289
Opzioni di controllo dell'accesso, 287
opzioni di logging, 285, 286, 287
opzioni di ridirezionamento, 289
introduzione, 277, 285
rapporto con i wrapper TCP, 287
risorse aggiuntive
documentazione installata, 290
libri correlati, 291
siti Web utili, 291
xinit
(Vd. X)
Xorg
(Vd. Xorg)

Y

YABOOT, 9
(Vd. Anche boot loader)

Z

z/IPL, 9
(Vd. Anche boot loader)

Colophon

I manuali sono scritti in formato DocBook SGML v4.1. I formati HTML e PDF vengono prodotti usando i fogli stile DSSSL personali e script wrapper jade personali. I file SGML DocBook sono scritti in **Emacs** con l'aiuto della modalitá PSGML.

Garrett LeSage ha creato le grafiche di ammonizione (nota, suggerimento, importante attenzione e avviso). Essi possono essere ridistribuiti liberamente con la documentazione Red Hat.

Il team di documentazione del prodotto di Red Hat é composto dalle seguenti persone:

Sandra A. Moore — Scrittore principale/Maintainer della *Red Hat Enterprise Linux Installation Guide per x86, Itanium™, AMD64, e Intel® Extended Memory 64 Technology (Intel® EM64T)*; Scrittore principale/Maintainer della *Red Hat Enterprise Linux Installation Guide per l'Architettura IBM® POWER*; Scrittore principale/Maintainer della *Red Hat Enterprise Linux Installation Guide per le architetture IBM® S/390® e IBM® eServer™ zSeries®*

John Ha — Scrittore Principale/Maintainer della *Red Hat Cluster Suite Configurazione e gestione di un Cluster*; Scrittore/Maintainer della *Red Hat Enterprise Linux Security Guide*; Maintainer delle stylesheet DocBook personali e degli script

Edward C. Bailey — Scrittore primario/Controllore della *Red Hat Enterprise Linux Introduzione al System Administration*; Scrittore primario/Controllore delle *Release Note*; Contributing Writer alla *Red Hat Enterprise Linux Installation Guide per x86, Itanium™, AMD64, e Intel® Extended Memory 64 Technology (Intel® EM64T)*

Karsten Wade — Scrittore primario/Maintainer della *Red Hat SELinux Application Development Guide*; Scrittore primario/Maintainer della *Red Hat SELinux Policy Writing Guide*

Andrius Benokraitis — Scrittore principale/Maintainer della *Red Hat Enterprise Linux Reference Guide*; Scrittore/Maintainer della *Red Hat Enterprise Linux Security Guide*; Assistente per la *Red Hat Enterprise Linux System Administration Guide*

Paul Kennedy — Scrittore principale/Mantainer della *Red Hat GFS Administrator's Guide*; Assistente alla *Red Hat Cluster Suite Configurazione e gestione di un Cluster*

Mark Johnson — Scrittore principale/Maintainer della *Red Hat Enterprise Linux Configurazione Desktop e Administration Guide*

Melissa Goldin — Scrittore principale/Maintainer della *Red Hat Enterprise Linux Guida passo dopo passo*

Il team di localizzazione del prodotto di Red Hat é composto dalle seguenti persone:

Amanpreet Singh Alam — Traduttore della versione Punjabi

Jean-Paul Aubry — Traduttore della versione francese

David Barzilay — Traduttore della versione brasiliana/portoghese

Runa Bhattacharjee — Traduttrice della versione Bengali

Chester Cheng — Traduttore della versione cinese tradizionale

Verena Fuehrer — Traduttrice della versione tedesca

Kiyoto Hashida — Traduttore della versione giapponese

N. Jayaradha — Traduttrice della versione Tamil

Michelle Jiyeen Kim — Traduttrice della versione coreana

Yelitza Louze — Traduttrice della versione spagnola

Noriko Mizumoto — Traduttrice della versione giapponese

Ankitkumar Rameshchandra Patel — Traduttore della versione Gujarati

Rajesh Ranjan — Traduttore della versione Hindi
Nadine Richter — Traduttrice della versione tedesca
Audrey Simons — Traduttrice della versione francese
Francesco Valente — Traduttore della versione italiana
Sarah Wang — Traduttrice della versione cinese semplificato
Ben Hung-Pin Wu — Traduttore della versione cinese tradizionale