

# *Red Hat Linux 9*

## **Red Hat Linux 用戶自訂手冊**



## Red Hat Linux 9: Red Hat Linux 用戶自訂手冊

版權 2003 Red Hat, Inc.



Red Hat, Inc.

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

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

Red Hat, Inc. 著作權所有© 2003。這個資料必須遵照由Open Publication License, V1.0 或之後的版本（最新的版本可在<http://www.opencontent.org/openpub/> 找到）所公佈的條款才能散佈。

在沒有著作權所有人明定允許的情況下，散佈已經實質上更改的這份文件是被禁止的。

以任何標準（紙張上）的書本形式散佈作品或衍生的作品，並用在商業用途上是被禁止的，除非已獲得著作權所有人的允許。

Red Hat、Red Hat Network、Red Hat “Shadow Man” 標誌、RPM、Maximum RPM、RPM 標誌、Linux 函式庫、PowerTools、Linux Undercover、RHmember、RHmember More、Rough Cuts、Rawhide 以及所有 Red Hat 為主的商標與標誌都是 Red Hat, Inc. 在美國與其他國家的商標或註冊商標。

Linux 是 Linus Torvalds 的一個註冊商標。

Motif 與 UNIX 是 The Open Group 的註冊商標。

Intel 與 Pentium 是 Intel Corporation 的註冊商標。Itanium 與 Celeron 是 Intel Corporation 的註冊商標。

AMD, AMD Athlon, AMD Duron 以及 AMD K6 是 Advanced Micro Devices, Inc. 的商標。

Netscape 是 Netscape Communications Corporation 在美國與其他國家的註冊商標。

Windows 是 Microsoft Corporation 的註冊商標。

SSH 與 Secure Shell 是 SSH Communications Security, Inc. 的商標。

FireWire 是 Apple Computer Corporation 的商標。

所有其他的商標與牽涉到的著作權都屬於它們所有權人的財產。

security@redhat.com 的 GPG fingerprint 金鑰為：

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

# 內容目錄

簡介 .....	i
1. 這本手冊的變更 .....	i
2. 文件中的慣用形式 .....	ii
3. 敬請期待 .....	iv
3.1. 我們需要您的寶貴意見！ .....	iv
4. 註冊以取得支援 .....	iv
<b>I. 檔案系統 .....</b>	<b>i</b>
1章ext3 檔案系統 .....	1
1.1. ext3 的特色 .....	1
1.2. 建立一個ext3 檔案系統 .....	1
1.3. 轉換為一個ext3 檔案系統 .....	2
1.4. 還原到ext2 檔案系統 .....	2
2章Swap 空間 .....	5
2.1. 什麼是Swap 空間？ .....	5
2.2. 增加Swap 空間 .....	5
2.3. 移除Swap 空間 .....	6
2.4. 移動Swap 空間 .....	7
3章磁碟陣列(RAID) .....	9
3.1. 什麼是RAID？ .....	9
3.2. 誰該使用RAID 呢？ .....	9
3.3. 硬體RAID VS. 軟體RAID .....	9
3.4. RAID 等級與線性支援 .....	10
4章邏輯磁區管理員(LVM) .....	13
5章管理磁碟儲存空間 .....	15
5.1. 檢視磁碟分割區表 .....	15
5.2. 建立一個分割區 .....	16
5.3. 移除一個分割區 .....	18
5.4. 重新調整分割區的大小 .....	18
6章實作磁碟配額 .....	21
6.1. 設定磁碟配額 .....	21
6.2. 管理磁碟配額 .....	24
6.3. 其他的資源 .....	25
<b>II. 安裝相關的資訊 .....</b>	<b>27</b>
7章Kickstart 安裝 .....	29
7.1. 到底什麼是Kickstart 安裝啊？ .....	29
7.2. 該如何執行一個Kickstart 安裝？ .....	29
7.3. 建立Kickstart 檔案 .....	29
7.4. Kickstart 的選項 .....	30
7.5. 套件選擇 .....	43
7.6. 前置安裝程式碼 .....	44
7.7. 後續安裝程式碼 .....	45
7.8. 使Kickstart 檔案可存取 .....	46
7.9. 使安裝目錄可存取 .....	48
7.10. 開始Kickstart 安裝 .....	48
8章Kickstart 設定程式 .....	51
8.1. 基本組態設定 .....	51
8.2. 安裝方式 .....	52
8.3. 開機管理程式選項 .....	53
8.4. 分割區資訊 .....	54
8.5. 網路組態設定 .....	56
8.6. 認證 .....	57
8.7. 防火牆組態設定 .....	58
8.8. X 組態設定 .....	59

8.9. 選取套件 .....	62
8.10. 前置安裝程式碼 .....	62
8.11. 後續安裝程式碼 .....	63
8.12. 儲存檔案 .....	65
9章基本的系統回復 .....	67
9.1. 一般問題 .....	67
9.2. 開機進入救援模式 .....	67
9.3. 開機進入單一使用者模式 .....	69
9.4. 開機進入緊急模式 .....	69
10章軟體RAID 設定 .....	71
11章LVM 設定 .....	75
<b>III. 網路相關的設定 .....</b>	<b>79</b>
12章網路設定 .....	81
12.1. 概要 .....	81
12.2. 建立一個乙太網路連線 .....	82
12.3. 建立一個ISDN 連線 .....	83
12.4. 建立一個數據機連線 .....	85
12.5. 建立一個xDSL 連線 .....	86
12.6. 建立一個記號環狀網路連線 .....	88
12.7. 建立一個CIPE 連線 .....	89
12.8. 建立一個無線網路連線 .....	90
12.9. 管理DNS 設定 .....	91
12.10. 管理主機 .....	92
12.11. 啟用裝置 .....	93
12.12. 使用資料檔 .....	94
12.13. 裝置別名 .....	95
13章基本的防火牆設定 .....	97
13.1. 安全等級設定工具 .....	97
13.2. <b>GNOME Lokkit</b> .....	99
13.3. 啟動iptables 服務 .....	102
14章控制服務的存取 .....	105
14.1. 執行等級 .....	105
14.2. TCP 包裹程式(Wrappers) .....	106
14.3. 系統服務設定工具 .....	106
14.4. ntsysv .....	108
14.5. chkconfig .....	108
14.6. 其他的資源 .....	109
15章OpenSSH .....	111
15.1. 為什麼要使用OpenSSH ? .....	111
15.2. 設定一個OpenSSH 伺服器 .....	111
15.3. 設定一部OpenSSH 用戶端 .....	111
15.4. 其他的資源 .....	115
16章網路檔案系統(NFS) .....	117
16.1. 為何要使用NFS ? .....	117
16.2. 掛載NFS 檔案系統 .....	117
16.3. 匯出NFS 檔案系統 .....	118
16.4. 其他的資源 .....	122
17章Samba .....	123
17.1. 為何使用Samba ? .....	123
17.2. 設定一部Samba 伺服器 .....	123
17.3. 連線到一個Samba 共享資源 .....	129
17.4. 其他的資源 .....	130
18章動態主機設定協定(DHCP) .....	131
18.1. 為什麼要使用DHCP ? .....	131
18.2. 設定一部DHCP 伺服器 .....	131

18.3. 設定一部DHCP用戶端 .....	135
18.4. 其他的資源 .....	136
19章Apache HTTP 伺服器設定 .....	137
19.1. 基本設定 .....	137
19.2. 預設設定 .....	139
19.3. 虛擬主機設定 .....	144
19.4. 伺服器設定 .....	147
19.5. 調整效能 .....	148
19.6. 儲存您的設定 .....	149
19.7. 其他的資源 .....	149
20章Apache HTTP 安全伺服器設定 .....	151
20.1. 簡介 .....	151
20.2. 關於安全性相關之套件的簡要 .....	151
20.3. 關於憑證與安全的一個概要 .....	153
20.4. 使用之前已有的金鑰與憑證 .....	153
20.5. 憑證的種類 .....	154
20.6. 產生一把金鑰 .....	154
20.7. 產生一個憑證要求以傳送給一個CA .....	156
20.8. 建立一個自我簽署的憑證 .....	157
20.9. 測試憑證 .....	158
20.10. 存取伺服器 .....	158
20.11. 其他的資源 .....	158
21章BIND 組態設定 .....	161
21.1. 新增一個正解主網域 .....	161
21.2. 新增一個反解主網域 .....	163
21.3. 新增一個次網域 .....	165
22章認證設定 .....	167
22.1. 使用者資訊 .....	167
22.2. 認證 .....	168
22.3. 命令列版本 .....	169
23章郵件傳送代理(MTA)的設定 .....	171
<b>IV. 系統組態設定 .....</b>	<b>173</b>
24章主控台存取 .....	175
24.1. 停用Ctrl-Alt-Del的關機快捷鍵 .....	175
24.2. 停用主控台中的程式存取 .....	175
24.3. 停用所有的主控台存取 .....	176
24.4. 定義主控台 .....	176
24.5. 使檔案可經由主控台存取 .....	176
24.6. 啟用其他應用程式的主控台存取 .....	177
24.7. floppy 群組 .....	178
25章使用者與群組設定 .....	179
25.1. 新增一個使用者 .....	179
25.2. 修改使用者內容 .....	180
25.3. 新增一個群組 .....	181
25.4. 修改群組內容 .....	181
25.5. 命令列設定 .....	182
25.6. 設定過程的解釋 .....	185
26章收集系統資訊 .....	187
26.1. 系統程序 .....	187
26.2. 記憶體用量 .....	189
26.3. 檔案系統 .....	190
26.4. 硬體 .....	191
26.5. 其他的資源 .....	192
27章印表機設定 .....	195
27.1. 新增一部本機印表機 .....	196

27.2. 新增一部IPP 印表機 .....	197
27.3. 新增一個遠端的UNIX (LPD) 印表機 .....	198
27.4. 新增一部Samba (SMB) 印表機 .....	199
27.5. 新增一部Novell NetWare (NCP) 印表機 .....	200
27.6. 新增一部JetDirect 印表機 .....	201
27.7. 選取印表機型號以完成設定 .....	202
27.8. 列印測試頁 .....	203
27.9. 修改既有的印表機 .....	203
27.10. 儲存設定檔案 .....	205
27.11. 命令列的設定 .....	206
27.12. 管理列印工作 .....	207
27.13. 分享一部印表機 .....	209
27.14. 轉換列印系統 .....	211
27.15. 其他的資源 .....	212
28章自動工作排程管理 .....	213
28.1. Cron .....	213
28.2. Anacron .....	215
28.3. At 與Batch .....	216
28.4. 其他的資源 .....	217
29章紀錄檔案 .....	219
29.1. 尋找紀錄檔案 .....	219
29.2. 檢視紀錄檔案 .....	219
29.3. 檢查紀錄檔案 .....	220
30章升級核心 .....	221
30.1. 2.4 版的核心 .....	221
30.2. 準備進行升級 .....	221
30.3. 下載欲升級的核心 .....	222
30.4. 執行核心升級 .....	223
30.5. 校驗初始的虛擬磁碟映像檔 .....	223
30.6. 校驗開機管理程式 .....	223
31章核心模組 .....	227
31.1. 核心模組工具程式 .....	227
31.2. 其他的資源 .....	229
<b>V. 套件管理 .....</b>	<b>231</b>
32章使用RPM 做套件管理 .....	233
32.1. RPM 設計的宗旨 .....	233
32.2. 使用RPM .....	234
32.3. 檢查一個套件的簽章 .....	238
32.4. 使用RPM 讓您的朋友對您另眼相看 .....	239
32.5. 其他的資源 .....	241
33章套件管理工具 .....	243
33.1. 安裝套件 .....	243
33.2. 移除套件 .....	244
34章Red Hat Network .....	247
<b>VI. 附錄 .....</b>	<b>251</b>
A. 建立一個自訂的核心 .....	253
A.1. 準備建立 .....	253
A.2. 建立核心 .....	253
A.3. 建立一個集成式的核心 .....	255
A.4. 其他的資源 .....	255
B. 開始使用Gnu Privacy Guard .....	257
B.1. 設定檔案 .....	257
B.2. 警告訊息 .....	257
B.3. 產生一副鑰匙對(Keypair) .....	258
B.4. 產生一個廢止的憑證 .....	260

B.5. 匯出您的公鑰.....	260
B.6. 匯入一個公鑰.....	262
B.7. 數位簽章是什麼？.....	263
B.8. 其他的資源.....	263
<b>索引.....</b>	<b>265</b>
<b>版本記錄.....</b>	<b>275</b>





歡迎使用 *Red Hat Linux* 用戶自訂手冊。

*Red Hat Linux* 用戶自訂手冊 中含有如何自訂您的 *Red Hat Linux* 系統的相關資訊。假如您需要一本以作業為導向且一步步教您設定與自訂您系統的手冊，這就是您要找的了。這本手冊將討論許多中級的主題，例如：

- 設定一個網路介面卡(NIC)
- 執行一個Kickstart的安裝
- 設定Samba的共享
- 使用RPM管理您的軟體
- 決定與您系統相關的資訊
- 升級您的核心

這本手冊劃分為以下幾個主要的類別：

- 與安裝相關的參考資料
- 與網路相關的參考資料
- 系統設定
- 套件管理

這本手冊預設您已經對 *Red Hat Linux* 系統有基本的了解，假如您需要參考資料涵蓋例如設定您的桌面或播放音效光碟等更基本的主题，請參考 *Red Hat Linux* 使用手冊。假如您需要更進階的說明文件，如 *Red Hat Linux* 檔案系統的概要，請參考 *Red Hat Linux* 參考手冊。

HTML 與PDF 版本的 *Red Hat Linux* 手冊可在說明文件光碟與網站上找到：<http://www.redhat.com/docs/>。



#### 請注意

雖然這本手冊含有目前最新的資訊，您應該閱讀 *Red Hat Linux* 的發行公告 以取得在我們的說明文件截稿之後的最新訊息。它們可以在 *Red Hat Linux CD #1* 以及線上取得：

<http://www.redhat.com/docs/manuals/linux>

## 1. 這本手冊的變更

這本手冊已經擴充來包括在 *Red Hat Linux 9* 中的新特色，以及由我們的讀者所要求的主题。這本手冊的重要變更包括了：

### 實作磁碟配額

這個新章節解釋了如何設定與管理磁碟配額。

### 認證設定

這個新的章節解釋如何使用『**網路認證設定工具**』。

## 使用者設定

這個章節已經擴充來涵蓋用來管理使用者與群組的命令列工具，以及解釋當一個新的使用者新增至系統時會發生什麼狀況。

## Samba

這個章節已經擴充來包含新的『**Samba 伺服器設定工具**』。

## 印表機設定

這個章節已經為新的『**印表機設定工具**』介面、新的『**GNOME 列印管理員**』以及位於面板上之新的拖放印表機圖示重新撰寫過了。

## Kickstart

在Red Hat Linux 9中，kickstart的選項已經更新以收錄一個新的選項，而且『**Kickstart 設定程式**』的章節也已經更新以含括一些新的特色。

## 網路設定

這個章節已經更新，以反應最新的『**網路管理工具**』介面與特色。

## 時間與日期設定

這個章節已經移至Red Hat Linux 使用手冊中。

## 2. 文件中的慣用形式

當您閱讀這本手冊時，您將會看到某些字以不同的字型、字體、大小以及比例出現。這樣的加強顯示是有系統的；不同的字以相同的形式出現來代表它們屬於一個特定的類別。以這種方式來表示的文字類型有：

### command

Linux 的指令（以及其他作業系統的指令）是以這種形式表示。這種類型表示您可以在命令列下輸入字或詞，然後再按下[Enter]來執行該指令。有時候，指令會包含以不同形式顯示的字（例如，檔名）。在這些情況下，它們被視為指令的一部分，所以整段字將會以一個指令來顯示。例如：

使用cat testfile 指令來檢視在目前工作目錄中名為testfile 的檔案內容。

### filename

檔名、目錄名、路徑以及RPM 套件名稱是以這種形式表示。這種形式指出一個特定的檔案或目錄以該名稱存在您的Red Hat Linux 系統上。例如：

在您家目錄中的.bashrc 檔案含有bash shell 的定義以及您自己使用的別名。

/etc/fstab 檔案含有關於不同系統裝置與檔案系統的資訊。

如果您想要使用一個網頁伺服器紀錄檔分析程式，請安裝webalizer RPM。

### application

這個形式向您表示這個程式是一種用戶端的應用程式（與系統軟體相對應）。例如：

使用Mozilla 來瀏覽網頁。

### [key]

鍵盤上的按鍵是以這種形式表示。例如：

要使用[Tab] 完成鍵，輸入一個字元後再按下[Tab] 鍵。您的終端機會顯示在目錄中以該字母為首的所有檔案。

## [key]-[combination]

按鍵的組合會以這種形式表示。例如：

[Ctrl]-[Alt]-[Backspace] 的按鍵組合將會離開您的圖形工作階段，並帶您回到圖形的登入畫面或主控台。

## 在GUI 介面中的文字

在GUI 介面的畫面或視窗中的標題、字或詞將會以這種形式表示。當您看到以這種形式顯示的文字，表示它被使用來代表一個特定的GUI 畫面或一個GUI 畫面的元件（例如選取盒或欄位旁的文字）。例如：

假如您希望您的螢幕保護程式終止前需要輸入密碼，請選取『**需要密碼**』的選取盒。

## GUI 畫面或視窗頂端的選單

當您看到一個此種形式的字，它代表在頂端下拉式選單中的選項。假如您點選GUI 畫面中的字，將會出現選單的其餘部份。例如：

在GNOME 終端機的『**檔案**』選單中，您將會看到『**新增終端機分頁**』項目，這個選項讓您可以在同一視窗開啟多重的shell 提示符號。

假如您需要在GUI 選單中選擇一連串的選項，它們將會以下列的例子來表示：

點選『**主選單按鈕**』（在面板上）=> 『**程式設計**』=> **Emacs** 來啟動**Emacs** 文字編輯器。

## GUI 畫面或視窗中的按鈕

這種形式指出這文字會出現在GUI 畫面中可按的按鈕。例如：

點選上一步 按鈕來回到您上一個檢視的網頁。

## computer output

當您看到以這種形式出現的文字，它代表命令列中電腦所顯示的文字。您將會看到您所輸入指令的回應、錯誤訊息以及在程式碼或程式中互動式的輸入提示等都以這種形式表示。例如：

使用ls 指令來顯示一個目錄的內容：

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

因應這個指令所產生的輸出（在這個例子，為目錄的內容）會以這種形式表示。

## prompt

一個提示符號（它是一種電腦的符號，用來表示已準備好等待您的輸入）將會以這種形式表示。例如：

```
$
#
[stephen@maturin stephen]$
leopard login:
```

## user input

使用者必須輸入的文字（不管是在命令列或在GUI 畫面的文字欄）將會以這種形式表示。下列的例子中，**text** 是以這種形式顯示：

要啟動您的系統到文字模式的安裝程式，您必須在boot: 提示符號下輸入**text** 指令。

另外，我們使用許多種不同的方法來引起您對某些資訊的注意。以這些資訊對您系統的重要性來區分，這些項目將會被標示為『請注意』、『建議』、『重要』、『警示』與『警告』。例如：

**請注意**

請記得Linux 是有分辨大小寫的。也就是說rose, ROSE 與rOsE 都是不同的。

**建議**

/usr/share/doc 目錄含有安裝在您系統上的套件之額外說明文件。

**重要**

假如您修改DHCP 設定檔，在您重新啟動DHCP 程式前，所做的變更不會生效。

**警告**

不要以root 身份執行日常工作— 請使用一個一般的使用者帳號，除非您需要使用root 帳號來做系統管理的工作。

**警告**

假如您選擇不要手動分割磁碟，伺服器的安裝方式將會移除所有硬碟上的所有既有的分割區。除非您確定沒有任何想儲存的資料，否則千萬不要選擇這種安裝方式。

## 3. 敬請期待

*Red Hat Linux* 用戶自訂手冊 是Red Hat 不斷成長之承諾的一部分，以提供有用與即時的支援給Red Hat Linux 的使用者。因為新的工具與應用程式會漸次出現，這本手冊也將持續擴充以涵蓋它們於其中。

### 3.1. 我們需要您的寶貴意見！

假如您在*Red Hat Linux* 用戶自訂手冊 中有看到印刷上的錯誤，或有任何您覺得可以改進的地方，我們很歡迎您的建言！請回報一份關於rh1-cg 的報告到Bugzilla (<http://bugzilla.redhat.com/bugzilla/>)。

當呈送一份報告時，請記得要註明這本手冊的識別標籤：

```
rh1-cg(ZH-TW)-9-Print-RHI(2003-02-20T01:08)
```

藉由您所提供的手冊識別標籤，我們將會確切地知道您所擁有之手冊的版本。

假如您有關於改善說明文件的建議，請盡量明確的說明您的想法。如果有發現錯誤，也請您指出段落號碼與一些周遭的文字，以使得我們可以更快的找到它。

## 4. 註冊以取得支援

假如您有購買Red Hat Linux 9，請記得註冊以使您成為可享應有權益的Red Hat 顧客。

您將會享有下列任何或全部的權益（取決於您所購買的Red Hat Linux 產品）：

- Red Hat 的技術支援— 從Red Hat, Inc. 的技術支援團隊取得關於您安裝問題的輔助。
- Red Hat Network — 輕易的更新您的套件，以及接收為您系統自訂的安全性提示。請至<http://rhn.redhat.com> 以取得更多詳細資訊。
- *Under the Brim* : Red Hat 的電子報 — 每個月直接從Red Hat 收到最新新聞與產品訊息。

要註冊，請至<http://www.redhat.com/apps/activate/>。在您的Red Hat Linux 盒裝中，您將會看到您的產品ID 在一張黑紅白相間的卡上。

如要閱讀關於Red Hat Linux 的技術支援，請參考在*Red Hat Linux* 安裝手冊 中的『取得技術支援』附錄。

祝您好運，並感謝您選擇Red Hat Linux ！

Red Hat 說明文件團隊敬上



# I. 檔案系統

『檔案系統』是指儲存在電腦中的檔案與目錄，一個檔案系統可以有不同的格式稱為『檔案系統類型』。這些格式決定資訊是如何儲存為檔案與目錄，有些檔案系統類型儲存多餘的資料備份，然而有些檔案系統類型使得硬碟的存取更快。這個章節將探討ext3, swap, RAID 以及LVM 檔案系統類型，還有說明一個用來管理分割區的parted 工具。

## 內容目錄

1章ext3 檔案系統 .....	1
2章Swap 空間 .....	5
3章磁碟陣列(RAID) .....	9
4章邏輯磁區管理員(LVM).....	13
5章管理磁碟儲存空間.....	15
6章實作磁碟配額 .....	21





打從Red Hat Linux 7.2 版開始，預設的檔案系統已經從較脆弱的ext2 格式更改為日誌式的ext3 檔案系統。

## 1.1. ext3 的特色

ext3 檔案系統基本上是ext2 檔案系統的加強版本，這些改革提供了下列的優點：

### 可用性

在非預期的電源中斷或系統當機（也稱為*unclean system shutdown*），每一個在機器上掛載的ext2 檔案系統都必須由e2fsck 程式檢查其一致性。這個費時的過程將會嚴重地延誤系統的開機時間，特別是在含有大量檔案的分割區上。在這個時間內，在該磁區上的任何資料都無法存取。

由ext3 檔案系統提供的日誌式功能表示在系統未正常關機的情況下，這種檔案系統的檢查已不再需要。使用ext3 檔案系統唯一需要做一致性檢查的情況在於某些少見的硬體錯誤狀況，如硬碟錯誤。在系統未正常關機之後，用來回復一個ext3 檔案系統所需的時間，並不取決於檔案系統的大小或所含檔案的數量，而是在於用來維護一致性之*journal* 的大小。取決於硬體的速率，用來回復預設大小的*journal* 只需要一秒鐘。

### 資料完整性

ext3 檔案系統在系統未正常關機的情況下提供了加強的資料完整性。ext3 檔案系統讓您您可以為您的資料選擇保護的類型與層級。預設情況下，Red Hat Linux 9 設定ext3 的磁區對於檔案系統狀態保持一個高等級的資料一致性。

### 速度

不管需要多次地寫入某些資料，ext3 在大部分情況下擁有比ext2 高的資料傳輸量，因為ext3 的日誌式功能會加速硬碟機磁頭的動作。您可以選擇三種日誌式的模式來為硬碟機加速，不過這樣反而會犧牲資料的完整性。

### 簡易的轉換

您可以很容易地將ext2 檔案系統轉換成ext3，並不需要重新格式化便可立即享有一個多功能日誌式檔案系統的好處。請看 1.3 節以取得關於如何執行這項工作的指示。

假如您執行一個Red Hat Linux 9 的完整安裝，預設指定給Linux 分割區的檔案系統為ext3，假如您是從使用ext2 分割區的Red Hat Linux 版本作升級，安裝程式會讓您有機會將這些分割區轉換為ext3 分割區而不遺失任何資料。請參閱Red Hat Linux 安裝手冊中的『升級您目前的系統』附錄以取得詳細資訊。

以下的部份將會引導您建立與調校ext3 分割區的步驟。假如您有ext2 檔案系統，並且正在執行Red Hat Linux 9，您可以跳過以下的磁碟分割與格式化步驟，直接進行 1.3 節。

## 1.2. 建立一個ext3 檔案系統

在安裝完成後，通常需要建立一個新的ext3 檔案系統，舉例來說，假如您新增一個新的磁碟機到一部Red Hat Linux 系統，您也許會想要將該磁碟做磁碟分割，並且使用ext3 檔案系統。

建立一個ext3 檔案系統的步驟如下：

1. 使用parted 或fdisk 建立分割區。
2. 使用mkfs 格式化分割區為ext3 檔案系統的格式。

3. 使用 `e2label` 將該分割區加上標籤。
4. 建立掛載點。
5. 增加該分割區到 `/etc/fstab` 檔案中。

請參考第5章 以取得執行這些步驟的更詳細資訊。

### 1.3. 轉換為一個 ext3 檔案系統

`tune2fs` 程式可以增加一個日誌到既有的 ext2 檔案系統，而不影響到分割區上既有的資料。假如在轉換過程中，該檔案系統已經被掛載，這個日誌將會出現在該檔案系統的根目錄下的 `.journal` 檔案。假如該檔案系統沒有被掛載，這個日誌將會被隱藏，並且不會出現在檔案系統中。

如要轉換一個 ext2 檔案系統為 ext3，請以 `root` 身份登入並輸入：

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

請取代以上例子中的 `/dev/hdb` 為您的裝置名稱，以及 `X` 為分割區編號。

完成後請確實更改 `/etc/fstab` 檔案中該分割區的類型為 ext3。

假如您要轉換您的根目錄檔案系統，您必須要使用一個 `initrd` 映像檔（或虛擬硬碟）來開機。如要建立這個，請執行 `mkinitrd` 程式。如需關於使用 `mkinitrd` 指令的更多資訊，請輸入 `man mkinitrd`。也請確定您的 `GRUB` 或 `LILO` 設定會載入 `initrd`。

假如您沒有做這個變更，系統還是會開機，不過檔案系統會被掛載為 ext2 而不是 ext3。

### 1.4. 還原到 ext2 檔案系統

因為 ext3 檔案系統是相當新的功能，有些磁碟工具尚未支援它。舉例來說，您也許需要使用 `resize2fs` 來縮小分割區的大小，不過它尚未支援 ext3。在這種情況下，您也許需要暫時將該檔案系統還原到 ext2。

如要還原一個分割區，首先您必須以 `root` 身份登入並輸入以下指令來卸載該分割區：

```
umount /dev/hdbX
```

在以上例子中，請以裝置名稱取代 `/dev/hdb`，以分割區編號取代 `X`。在以下的部份，範例指令將使用 `hdb1` 代表這些數值。

再來，以 `root` 身份輸入以下指令來更改檔案系統的類型為 ext2：

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

在以 `root` 身份輸入下列指令來檢查分割區的錯誤：

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

然後再輸入以下指令掛載分割區為 ext2 檔案系統：

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

在以上例子中，請以分割區的掛載點取代 `/mount/point`。

下一步請轉換到它被掛載的目錄，再輸入下列指令來移除位於該分割區根目錄下的 `.journal` 檔案：

```
rm -f .journal
```

現在您將擁有一個 ext2 分割區。

假如您想要永久性的變更分割區為 ext2，請記得要更新 `/etc/fstab` 檔案中的紀錄。



## 2.1. 什麼是Swap 空間？

在Linux 上的『Swap 空間』是在當實體記憶體(RAM)用完時才會使用到，假如系統需要更多的記憶體資源，而實體記憶體已經用完，記憶體上不活動的頁面將會被移到swap 空間。雖然swap 空間可以幫助系統增加一小部份容量的RAM，不過不能將它當作更多記憶體的替代品。Swap 空間是位於硬碟上，它的存取速度比起實體記憶體慢了很多。

Swap 空間可以是一個既定的swap 分割區（建議使用）、一個swap 檔案，或為swap 分割區與swap 檔案的結合。

swap 空間的大小必須是您電腦記憶體兩倍大的空間或者至少為32MB（視何者較大），不過不能大於2048MB(2GB)。

## 2.2. 增加Swap 空間

有時候需要在安裝後增加更多的swap 空間，舉例來說，您也許會將系統的RAM 從64MB 升級為128MB，不過swap 的空間只有128MB，如果您需要執行需要大量記憶體的應用程式或操作，這時候就有必要將swap 的空間增大至256MB。

在此您有兩種選擇：增加一個swap 分割區或增加一個swap 檔案。建議您新增一個swap 分割區，不過如果您沒有任何可用的空間，將很難做到。

如要新增一個swap 分割區（假設/dev/hdb2 為您想新增的swap 分割區），請依照下列的指示：

1. 硬碟不可以正在使用中（分割區不能被掛載中，而且不能啟用swap 空間）。要做到這樣最簡單的方法是將您的系統開機至『救援模式』，請參考第9章 以取得開機進入救援模式的指示。在提示您掛載檔案系統時，請選擇略過。

除此之外，假如該磁碟不包含任何使用中的分割區，您可以卸載它們，然後使用swapoff 指令來關閉硬碟上所有的swap 空間。

2. 可以使用parted 或fdisk 來建立swap 分割區，使用parted 會比fdisk 容易，因此在這裡只有解釋parted。如要使用parted 來建立一個swap 分割區，請遵照以下指示：
  - 以root 身份在shell 提示符號下輸入parted /dev/hdb 指令，這裡的/dev/hdb 是含有剩餘空間之硬碟的裝置名稱。
  - 在(parted) 的提示符號下輸入print 來檢視既有的分割區以及剩餘的空間。在此，起點與終點的數值是以MB 表示的，請找出硬碟上所剩餘的空間以及您要分配多少空間給新的swap 分割區。
  - 在(parted) 的提示符號下輸入mkpartfs part-type linux-swaps start end，這裡的part-type 是primary, extended 或logical 的其中一種，start 是分割區的起始點，而end 為分割區的結束點。



警告

變更將立即生效，在輸入時請特別小心。

- 輸入quit 以離開parted。
3. 現在，您的swap 分割區就建立好了，請使用mkswap 指令來設定該swap 分割區，以root 身份在shell 提示符號下輸入以下指令：

```
mkswap /dev/hdb2
```

4. 如要立即啟用該swap 分割區，請輸入以下指令：  

```
swapon /dev/hdb2
```
5. 如要在開機時啟用它，請編輯/etc/fstab 檔案以包含下列這一行：  

```
/dev/hdb2    swap          swap defaults    0 0
```

下次系統開機時，將會啟用新的swap 分割區。
6. 在新增完swap 分割區然後啟用它後，請使用cat /proc/swaps 或free 指令來檢視它們的輸出以確定它已經被啟用。

如要新增一個swap 檔案：

1. 請先決定新swap 檔案的大小，然後乘以1024 以取得磁碟區塊(block)的大小，例如64MB 之swap 檔案的區塊大小為65536。
2. 請以root 身份在shell 提示符號下輸入下列指令，並包括count 等於區塊大小的數值：  

```
dd if=/dev/zero of=/swapfile bs=1024 count=65536
```
3. 並使用以下指令來設定swap 檔案：  

```
mkswap /swapfile
```
4. 如要立即啟用swap 檔案（非開機時自動啟動），請使用下列指令：  

```
swapon /swapfile
```
5. 如要在開機時啟動它，請編輯/etc/fstab 以包含：  

```
/swapfile    swap          swap defaults    0 0
```

下次系統開機時，它將會啟用新的swap 檔案。
6. 在增加新的swap 檔案並啟用它後，請檢視cat /proc/swaps 或free 指令的輸出以確定它已經被啟用。

## 2.3. 移除Swap 空間

要移除一個swap 分割區，請依照下列的指示：

1. 硬碟不可以正在使用中（分割區不能被掛載中，而且不能啟用swap 空間）。要做到這樣最簡單的方法是將您的系統開機至『救援模式』，請參考第9章 以取得開機進入救援模式的指示。在提示您掛載檔案系統時，請選擇略過。  

除此之外，假如該磁碟不包含任何使用中的分割區，您可以卸載它們，然後使用swapoff 指令來關閉硬碟上所有的swap 空間。
2. 以root 身份在shell 提示符號下執行下列指令以確定swap 分割區已經停用了（/dev/hdb2 為swap 分割區）：  

```
swapoff /dev/hdb2
```
3. 再從/etc/fstab 檔案中移除它的紀錄項。
4. 可以使用parted 或fdisk 來移除分割區，在這裡只有解釋parted。如要使用parted 來移除分割區，請遵照以下指示：
  - 以root 身份在shell 提示符號下輸入parted /dev/hdb 指令，這裡的/dev/hdb 是含有要移除之swap 空間的硬碟裝置名稱。
  - 在(parted) 的提示符號下輸入print 來檢視既有的分割區以及找出您想要移除之swap 分割區的次碼(minor number)。
  - 在(parted) 的提示符號下輸入rm MINOR，這裡的MINOR 就是您想要移除之分割區的次碼。



警告

變更將立即生效，您必須輸入正確的密碼。

- 輸入**quit** 以離開parted。

如要移除一個swap 檔案，請遵照以下步驟：

1. 請以root 身份在shell 提示符號下執行下列指令以停用swap 檔案（/swapfile 就是swap 檔案）：  
`swapoff /swapfile`
2. 再從/etc/fstab 檔案中移除它的紀錄項。
3. 最後請移除該檔案：  
`rm /swapfile`

## 2.4. 移動Swap 空間

如要移動swap 空間到另一個位置，請先依照移除swap 空間的步驟，再進行新增swap 空間的步驟。





## 磁碟陣列(RAID)

### 3.1. 什麼是RAID ?

RAID 的基本概念是結合多個小型且便宜的磁碟機成為一個陣列，以達到一個大且昂貴的磁碟機無法做到的效能表現或多餘性的目標。這個磁碟機的陣列將會以一個單一的邏輯儲存單位或磁碟機呈現在電腦中。

RAID 是用來分散資訊到許多磁碟上的一種方法，使用例如磁碟機平行儲存(*disk striping*) (RAID Level 0)、磁碟機映射儲存(*disk mirroring*) (RAID level 1) 與其備分布式同位元檢測資料的磁碟機平行儲存(*disk striping with parity*) (RAID Level 5) 等技術來達到多餘性、較短的延遲時間亦或增加讀取或寫入到磁碟的頻寬，並且強化硬碟毀損時的回復能力。

RAID 的概念是資料可以一致地分散到陣列中的每一個磁碟，如要做到這樣，資料必須先劃分為一致大小的區塊(*chunks*) (雖然仍可能使用不同的大小，通常是32K 或64K 的大小)。根據所使用的RAID 等級，再來將會寫入每一個區塊到陣列中的硬碟。當資料要被讀取時，過程則相反，這樣將造成多個磁碟機實際上為一個大型磁碟機的假象。

### 3.2. 誰該使用RAID 呢 ?

需要保留大量資料在手邊的任何人士(如系統管理員) 都可藉由使用RAID 而受益。使用RAID 的主要原因包括了：

- 速度加快
- 使用一個單一的虛擬磁碟以增加儲存的容量
- 減少磁碟發生錯誤時的衝擊

### 3.3. 硬體RAID VS. 軟體RAID

目前有兩種實作RAID 的方法：硬體RAID 與軟體RAID。

#### 3.3.1. 硬體RAID

硬體為基礎的系統以獨立於主機之外的方式管理RAID 子系統，並且以每一個RAID 陣列中只有一個單一的磁碟呈現在主機面前。

硬體RAID 裝置的一個例子是連接到一個SCSI 控制器並且以一個單一的SCSI 磁碟機代表RAID 陣列的裝置。一個外部的RAID系統移動所有RAID 的處理“能力”到位於外部磁碟子系統的一個控制器，這整個子系統是透過一個一般的SCSI 控制器來連接到主機，並以一個單一的磁碟呈現給主機。

對作業系統來說，RAID 控制器也是以卡的形式來模擬類似一個SCSI 控制器，不過它們自己本身處理所有實際的磁碟通訊。在這些例子中，您將一個磁碟插入RAID 控制器就像是您對SCSI 控制器所做的一樣，不過您已將它們加入到RAID 控制器的組態設定中，而作業系統從未知曉發生什麼事。

### 3.3.2. 軟體RAID

軟體RAID 在核心磁碟(區塊裝置)程式碼上實作這許多種的RAID 等級, 它能提供最經濟的解決方案, 因為並不需要昂貴的磁碟控制器或熱插拔的底盤<sup>1</sup>。軟體RAID 可以使用在便宜的IDE 硬碟以及SCSI 硬碟上, 加上今日速度相當快的CPU, 軟體RAID 的效能表現已經超越硬體RAID 了。

Linux 核心中的MD 驅動程式是一種完全與硬體無關的RAID 解決方案例子。軟體為基礎之陣列的效能表現, 是依賴在伺服器的CPU 效能與負載。

如需關於在Red Hat Linux 安裝程式中設定軟體RAID 的資訊, 請參考第10章。

對於那些有興趣知道更多關於軟體RAID 所能做的事情, 這裡是最重要之特色的一個簡要清單:

- 執行緒的重建程序
- 核心為基礎的設定
- 在Linux 機器間不需重建的陣列可攜性
- 使用閒置的系統資源來背景化陣列的重建
- 支援磁碟的熱插拔
- 自動偵測CPU 以利用某些CPU 的最佳化

### 3.4. RAID 等級與線性支援

RAID 支援許多種設定, 包括0, 1, 4, 5 等模式與線性(linear)模式。這些RAID 類型定義如下:

- **Level 0** — RAID level 0, 通常稱為『平行儲存』, 它是一種以效能為導向的資料條狀分佈儲存的技術。這表示要寫入到陣列的資料會先劃分為條狀, 再寫入到陣列中的成員磁碟, 這個方法以較低的固有關支提供了相當高的I/O 存取效能, 不過並沒有任何的容錯能力。level 0 陣列的儲存容量等於硬體RAID 設定中所有成員磁碟的總容量, 也等於軟體RAID 設定中成員分割區的總容量。
- **Level 1** — RAID level 1 (映射儲存) 是所有RAID 模式中使用最長久的一種。Level 1 藉由寫入相同的資料到陣列中的每一個成員磁碟中以提供容錯能力, 這種方式將會在每一個磁碟上留下一份映射的複本。由於它的單純與相當高的資料可用性, 使得映射儲存一直都很受歡迎。Level 1 運用兩個以上的磁碟並使用平行式的存取, 以提供讀取時相當高的資料傳輸速率, 不過通常是獨立式的運作以提供快速的I/O 處理速率。Level 1 提供了相當好的資料可靠性, 並且改善了執行讀取密集之應用程式的效能, 不過相對的所需的成本是相當可觀的。<sup>2</sup> Level 1 陣列的儲存容量等於硬體RAID 設定中映射儲存硬碟中的其中一個磁碟容量, 或者是軟體RAID 設定中映射儲存分割區其中一個的容量。
- **Level 4** — Level 4 使用分布式同位元檢測資料(parity)<sup>3</sup>, 並將之存放在單一的磁碟機中以保護資料。這個方式較適用在交易式的I/O 存取, 而不適用於大型的檔案傳輸。因為這個既定的parity 磁碟機代表了一個固有的瓶頸限制, 因此在不使用回寫快取(write-back caching)技術的情況下, 很少用到level 4 模式。雖然RAID level 4 是某些RAID 磁碟分割機制的一個選擇, 不過在Red Hat Linux RAID 安裝中並沒有如此的選擇。<sup>4</sup> 硬體RAID level 4 的儲存容量等於所有成員磁碟機的容量減掉一個成員磁碟機的容量。軟體RAID level 4 的儲存容量等於成員分割區的容量減掉一個分割區的大小(假如它們是同樣大小的話)。

1. 一個熱插拔的底盤可以讓您在不開機的情況下, 也可以拔除一個硬碟機。

2. RAID level 1 的成本是很高的, 因為您會寫入相同的資訊到陣列中所有的磁碟上, 這將很浪費硬碟的空間。舉例來說, 假如您已經設定了RAID level 1, 而您的根目錄分割區(/) 存放在兩個40G 的硬碟上, 雖然您總共有80GB 的空間, 不過您只能存取80GB 中的40GB。另外的40GB 空間是用來當作第一個40GB 的映射儲存。

3. 分布式同位元檢測資料是根據陣列中其餘的成員磁碟之內容所計算出來的, 如果陣列中的一個磁碟發生錯誤時, 這些資訊可以使用來重建資料。在發生錯誤之磁碟被取出, 然後重新輸入資料於其中之前, 這些重建的資料可以被使用來滿足對該磁碟I/O 存取的要求。

4. RAID level 4 與RAID level 5 佔有相同的磁碟空間, 不過level 5 擁有較多的優點, 因此level 4 並不被支援。

- *Level 5* — 這是最普遍被使用的RAID 模式，藉由分散parity的資訊到陣列中某些或所有的成員磁碟機中，RAID level 5 減少了在level 4 中存在的寫入瓶頸。僅有的效能表現瓶頸在於parity 計算的過程，不過如果使用現今相當快的CPU 加上軟體RAID 設定，這通常不是一個很大的問題。與level 4 相同的是，結果會是不對稱的效能表現，也就是讀取的速度比起寫入速度快了很多。Level 5 通常使用回寫快取來減少這種不對稱性。硬體RAID level 5 的儲存容量等於所有成員磁碟機的容量減掉一個成員磁碟機的容量。軟體RAID level 5 的儲存容量等於成員分割區的容量減掉一個分割區的大小（假如它們是同樣大小的話）。
- 線性RAID 模式 — 線性RAID 模式是一種簡易地群組磁碟機來建立一個大型的虛擬磁碟。在線性RAID 模式設定中，空間區塊是從一個成員磁碟依序分配下來，當第一個磁碟完全填滿時，再分配到第二個磁碟，依此類推。這種群組化並沒有提供任何的效能增益，因為在成員磁碟機之間不可能會有任何分開的I/O 操作。線性的RAID 模式也沒有提供多餘性，而且說實在的它也降低了可靠性——假如任何一個成員磁碟發生錯誤，整個陣列便無法存取使用。總磁碟容量是所有成員磁碟機的容量。



## 邏輯磁區管理員(LVM)

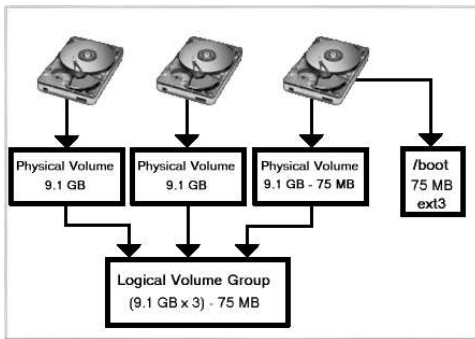
從Red Hat Linux 8.0 開始，您便可以使用邏輯磁區管理員(LVM) 來做硬碟空間的分配。

LVM 是一種分配硬碟空間到邏輯磁區的方法，這種方式比分配到分割區較容易做容量的調整。

使用LVM，硬碟或硬碟組將會被分配到一個或更多的『實體磁區』，不過一個實體磁區不可以跨越一個以上的磁碟。

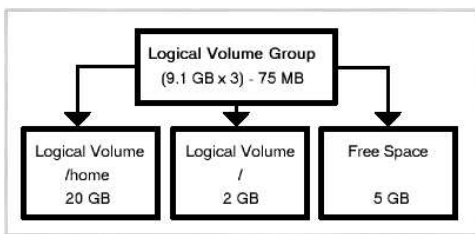
除了/boot 分割區，實體磁區會結合到『邏輯磁區群組』。/boot 分割區不可以在邏輯磁區群組中，因為開機管理程式將無法讀取到它。假如您想要根目錄/ 分割區在邏輯磁區中，您必須另外建立一個/boot 分割區，使其不屬於磁區群組的一員。

因為一個實體磁區不能跨越一個以上的磁碟，假如您想要邏輯磁區群組跨越一個以上的磁碟，您必須在每一個磁碟上建立一個以上的實體磁區。



圖形4-1. 邏輯磁區群組

邏輯磁區群組可以分割為幾個『邏輯磁區』，將會指定它們的掛載點，例如/home 與/，以及檔案系統類型，如ext3。當『分割區』的容量全滿時，邏輯磁區群組中的剩餘空間可以增加到邏輯磁區以增大分割區的大小。當系統新增一個硬碟時，可以將它增至邏輯磁區群組中，因此便可以擴展身為邏輯磁區的分割區。



圖形4-2. 邏輯磁區

以另一個角度來說，假如系統是以ext3 檔案系統做磁碟分割，且硬碟是分割為所定義大小的分割區。當一個分割區的容量用完時，要擴展該分割區的大小是很困難的，即使將該分割區移動到另一顆硬碟上，原本硬碟上的空間還是得重新分配到另一個分割區，或者先不去動它。

LVM 的支援必須編譯到核心中，Red Hat Linux 9 的預設核心是已編譯好LVM 支援的。

如要學習在Red Hat Linux 安裝過程中，如何設定LVM 的資訊，請參考第11章。

## 管理磁碟儲存空間

在您完成Red Hat Linux 系統的安裝之後，您也許會想要檢視現有的磁碟分割區表、更改分割區的大小、移除分割區或者從剩餘的空間或另一個硬碟來新增分割區。使用parted 工具可以幫您完成這些工作。這個章節討論如何使用parted 來執行檔案系統的工作。或者您可以使用fdisk 來執行大部分的這些工作（除了重新調整分割區的大小之外）。如需關於fdisk 的更多資訊，請參考fdisk 的man 或info page。

假如您想要檢視系統的磁碟空間用量或監視磁碟空間用量，請參考 26.3 節。

首先，系統必須安裝parted 套件才能使用parted 工具，如要啟動parted，請以root 身份在shell 提示符號下輸入parted /dev/hdb 指令，這裡的/dev/hdb 就是您想要設定的磁碟機裝置名稱。您將會看到一個(parted) 的提示字元，您可以輸入help 來檢視可使用指令的清單。

假如您想要建立、移除分割區或重新調整分割區的大小，該裝置不可正在使用中（分割區不可被掛載，而swap 空間不可被啟用）。最簡單的方法是啟動您的系統到救援模式。請參考第9章 以取得開機進入救援模式的指示。當提示您掛載檔案系統時，請選擇略過。

或者，假如該磁碟並不包含任何使用中的分割區，您可以使用umount 指令來卸載它們，並且使用swaponoff 關閉所有硬碟上的swap 空間。

表格5-1 含有較常用的parted 指令清單，在之後的部份將會再詳細地探討它們。

指令	說明
check minor-num	執行檔案系統的一般性檢查
cp from to	複製一個分割區的檔案系統到另一個分割區，from 與to 為分割區的次碼(minor number)
help	顯示可使用的指令清單
mklable label	建立磁碟分割區表中的一個磁碟標籤
mkfs minor-num file-system-type	建立一個類型為file-system-type 的檔案系統
mkpart part-type fs-type start-mb end-mb	建立一個分割區，而不建立新的檔案系統
mkpartfs part-type fs-type start-mb end-mb	建立一個分割區，並且建立所指定的檔案系統
move minor-num start-mb end-mb	移動分割區
print	顯示磁碟分割區表
quit	離開parted
resize minor-num start-mb end-mb	重新調整分割區大小從start-mb 到end-mb
rm minor-num	移除分割區
select device	選擇另一個裝置來設定
set minor-num flag state	設定一個分割區的旗標；state 可以是on 或off

表格5-1. parted 指令

## 5.1. 檢視磁碟分割區表

在parted 啟動後，請輸入以下指令來檢視磁碟分割區表：

```
print
```

會出現類似以下的表格：

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

第一行顯示磁碟的大小，第二行顯示磁碟的標籤類型，而其餘的輸出則顯示磁碟分割區表。在這個表格中，**Minor** 的數字就是分割區編號，例如次碼1 的分割區代表/dev/hda1。**Start** 與**End** 的數值是以MB 表示。**Type** 則是primary, extended 或logical 其中之一。**Filesystem** 就是檔案系統的類型，可以是ext2, ext3, FAT, hfs, jfs, linux-swap, ntfs, reiserfs, hp-ufs, sun-ufs 或xfs 等的其中一種類型。**Flags** 欄位會列出分割區所設定的旗標，可使用的旗標是boot, root, swap, hidden, raid, lvm 或lba。



### 建議

如要在不重新啟動parted 的情況下選取一個不同的裝置，您可以使用select 指令並在後面加上例如/dev/hdb 的裝置名稱。然後您便可以檢視它的磁碟分割區表或者開始設定它。

## 5.2. 建立一個分割區



### 警告

請勿試著在使用中的裝置上建立一個分割區！

在建立一個分割區之前，請先開機進入救援模式（或者卸載裝置上的任何分割區以及關閉裝置上的任何swap 空間）。

輸入下列指令來啟動parted，這裡的/dev/hda 就是您要用來建立分割區的裝置：

```
parted /dev/hda
```

檢視目前的磁碟分割區表以找出是否有足夠的剩餘空間：

```
print
```

假如沒有足夠的剩餘空間，您可以重新調整一個現有分割區的大小。請參考 5.4 節 以得到更詳細的指示。



### 5.2.1. 製作分割區

從磁碟分割區表上，可以找出新分割區之起始與結束的位置，以及應該是何種類型的分割區。在一個裝置上，只能有四個主分割區（不含延伸分割區），假如您需要四個以上的分割區，您可以有三個主分割區、一個延伸分割區，以及位於延伸分割區上的多個邏輯分割區。如需關於磁碟分割區的概要，請參考 *Red Hat Linux* 安裝手冊 中的『磁碟分割區的介紹』。

舉例來說，如果您要建立一個含有ext3 檔案系統的主分割區，範圍從硬碟上的1024MB 到2048MB，請輸入以下指令：

```
mkpart primary ext3 1024 2048
```



#### 建議

假如您使用mkpartfs 指令，檔案系統會在分割區建立好後建立。然而parted 並不支援建立一個ext3 檔案系統。因此假如您想要建立一個ext3 檔案系統，請使用mkpart，然後再使用如下所述的mkfs 指令建立檔案系統。mkpartfs 可使用在linux-swaps 的檔案系統類型上。

請特別注意在您按下[Enter] 鍵之後，變更會馬上生效，所以請在執行前小心地查看您的指令。

在建立分割區之後，請使用print 指令以確定該分割區在磁碟分割表上，並含有正確的分割區類型、檔案類型與大小。也請記得新分割區的次碼，所以您可以將它加上標籤，您也應該要檢視以下指令的輸出：

```
cat /proc/partitions
```

以確定核心可以辨識新的分割區。

### 5.2.2. 格式化分割區

分割區仍然還沒有建立檔案系統，請執行下列指令建立檔案系統：

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



#### 警告

格式化分割區將會永久地摧毀分割區上既有的任何資料。

### 5.2.3. 將分割區加上標籤

下一步就是將分割區加上標籤，舉例來說，假如新的分割區是/dev/hda3，而您想將它標示為/work：

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

預設情況下，Red Hat Linux 的安裝程式會使用分割區的掛載點當作該分割區的標籤，以確定該標籤是獨一無二的。不過您可以使用任何您可以想到的標籤名稱，只要不重複就好了。

### 5.2.4. 建立掛載點

以root 身份來建立掛載點：

```
mkdir /work
```

### 5.2.5. 新增至/etc/fstab

以root 身份來/etc/fstab 檔案，使其含有新分割區的資料，請加入類似以下這一行的資訊：

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

第一個欄位必須是LABEL= 加上您所給予分割區的標籤。第二個欄位應該包含新分割區的掛載點，而下一個欄位應該是檔案系統的類型（如ext3 或swap）。假如您需要關於這個檔案中所需格式的更多資訊，請使用man fstab 指令來參考它的man page。

假如第四個欄位為defaults，這個分割區將會在開機時被掛載；如果您要在不重新開機的情況下掛載這個分割區，請以root 身份輸入以下這個指令：

```
mount /work
```

## 5.3. 移除一個分割區



**警告**

請勿移除裝置上正在使用中的分割區。

在移除分割區之前，請開機進入救援模式（或是卸載裝置上任何的分割區，並關閉裝置上任何的swap 空間）。

輸入下列指令來啟動parted，這裡的/dev/hda 就是您要用來移除分割區的裝置：

```
parted /dev/hda
```

檢視目前的磁碟分割區表以找出要移除之分割區的次碼：

```
print
```

使用rm 指令來移除分割區，例如要移除次碼為3 的分割區，請輸入：

```
rm 3
```

一旦您按下[Enter] 鍵，變更將立即生效，所以請仔細查看您的指令。

在移除分割區之後，請使用print 指令以確定它已經從分割區表中移除了。您可以使用下列指令來檢視輸出

```
cat /proc/partitions
```

以確定核心知道該分割區已移除。

最後一個步驟是從/etc/fstab 檔案中移除該分割區的紀錄，請找出含有已移除分割區的該行，並將它從檔案中移除。

## 5.4. 重新調整分割區的大小



警告

請勿調整裝置上正在使用之分割區的大小。

在調整一個分割區的大小之前，請先開機進入救援模式（或是卸載裝置上的任何的分割區，並關閉裝置上任何的swap 空間）。

輸入下列指令來啟動parted，這裡的/dev/hda 就是您要用來調整分割區的裝置：

```
parted /dev/hda
```

請檢視磁碟分割區表以找出該分割區的次碼，以及該分割區開始與結束的位置：

```
print
```



警告

要調整之分割區的使用空間必須不能大於新的分割區大小。

如要調整一個分割區，請使用resize 指令再加上該分割區的次碼、以百萬位元組表示的起始位置以及結束位置。例如：

```
resize 3 1024 2048
```

在調整完分割區之後，請使用print 指令以確定該分割區已經做了正確的調整，以及是否為正確的分割區類型與檔案系統類型。

在重新啟動系統進入正常模式後，請使用df 指令以確定該分割區已經被掛載，並且含有正確的分割區大小。



## 實作磁碟配額

除了監視系統所使用磁碟空間之外（請參閱 26.3.1 節），可以藉由實作磁碟配額來限制磁碟的使用空間，因此在一個使用者用掉太多磁碟空間或一個分割區的容量太滿時，系統管理員將會收到警示訊息。

可以為單獨的使用者以及使用者群組設定磁碟配額，這種彈性設定使得我們可以給予每一個使用者小容量的定額以用來處理個人的檔案（如電子郵件與報告），而給予較充足容量的定額給他們所從事的專案（假設該專案是屬於他們自己的群組）。

除此之外，磁碟配額並不只是設定來控制所使用的磁碟區塊數目，它也控制inodes的數量。因為inodes通常都含有檔案相關的資訊，這個特色將允許控制可以建立的檔案數量。

您必須安裝quota RPM 才能實作磁碟配額。如需關於安裝RPM 套件的更多資訊，請參考 V 部。

### 6.1. 設定磁碟配額

如要實作磁碟配額，請遵照以下步驟：

1. 修改/etc/fstab 檔案來啟用每一個檔案系統的磁碟配額
2. 重新掛載檔案系統
3. 建立配額檔案以及產生磁碟用量表
4. 指定配額

每一個步驟都在以下的部份有個別詳述。

#### 6.1.1. 啟用配額

以root 身份使用您喜歡的文字編輯器，增加usrquota 亦或grpquota 選項到需要配額的檔案系統：

```
LABEL=/          /          ext3 defaults 11
LABEL=/boot      /boot      ext3 defaults 12
none             /dev/pts   devpts gid=5,mode=620 00
LABEL=/home      /home      ext3 defaults,usrquota,grpquota 12
none             /proc      proc defaults 00
none             /dev/shm   tmpfs defaults 00
/dev/hda2        swap       swap defaults 00
/dev/cdrom       /mnt/cdrom udf,iso9660 noauto,owner,kudzu,ro 00
/dev/fd0         /mnt/floppy auto noauto,owner,kudzu 00
```

在這個例子中，/home 檔案系統已經啟用使用者與群組的配額。

#### 6.1.2. 重新掛載檔案系統

在加入userquota 與grpquota 選項後，重新掛載fstab 紀錄項已經被修改的每一個檔案系統。假如該檔案系統不被任何程序使用中，請使用umount 指令再加上mount 指令來重新掛載檔案系統。假如該檔案系統目前正在使用中，重新掛載檔案系統的方法是重新啟動系統。

### 6.1.3. 建立配額檔案

在重新掛載每一個啟用磁碟配額的檔案系統後，系統上的磁碟配額機制將立即生效。然而，檔案系統本身尚未準備好支援磁碟配額。下一個步驟是執行quotacheck指令。

quotacheck指令會檢查啟用磁碟配額的檔案系統，並且建立每一檔案系統目前磁碟用量的表格。這個表格將會被使用來更新作業系統磁碟用量的資料，而且檔案系統的磁碟配額檔案也會更新。

如要在檔案系統上建立配額檔案(aquota.user與aquota.group)，請使用quotacheck指令的-c選項。舉例來說，假如在/home分割區上啟用使用者與群組的配額，請在/home目錄建立這些檔案：

```
quotacheck -acug /home
```

-a選項代表在/etc/mstab中所有已掛載的非NFS檔案系統都會檢查以查看磁碟配額是否已啟用。-c選項代表每一個已啟用磁碟配額的檔案系統都應該建立配額檔案，-u則表示要檢查使用者的磁碟配額，而-g選項表示檢查群組的磁碟配額。

假如都沒有指定-u或-g選項，將只會建立使用者的配額檔案。假如只有指定-g選項，則只會建立群組配額檔案。

在建立檔案之後，請執行下列指令以產生啟用配額之每一檔案系統的目前磁碟用量表格：

```
quotacheck -avug
```

所使用的選項如下：

- a — 檢查所有啟用配額之本機掛載的檔案系統
- v — 顯示配額檢查過程的詳細狀態資訊
- u — 檢查使用者磁碟配額資訊
- g — 檢查群組磁碟配額資訊

在quotacheck執行完成後，對應到啟用之配額（使用者亦或群組）的配額檔案將會開始加入每一個啟用配額之檔案系統（如/home）的資料。

### 6.1.4. 指定每一個使用者的磁碟配額

最後一個步驟是使用edquota指令來指定磁碟的配額。

如要設定使用者的磁碟配額，請以root身份在shell提示符號下執行以下指令：

```
edquota username
```

請對每一個您想套用磁碟配額的使用者執行這個步驟，舉例來說，假如在/etc/fstab中已經啟用/home分割區(/dev/hda3)的磁碟配額，而且已經執行了edquota testuser指令，下列的資訊將會顯示在系統預設的編輯器中：

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



#### 請注意

由EDITOR環境變數所定義的文字編輯器將會由edquota所啟動，如要變更這個編輯器，請設定EDITOR的環境變數為您選擇之編輯器的完整路徑。

第一個欄位是啟用配額之檔案系統的名稱，第二個欄位顯示目前使用者已經使用的區塊數量，旁邊的兩個欄位是用來設定檔案系統上對使用者強制性(hard)與非強制性(soft)的磁碟空間限制。inodes 欄位顯示目前使用者已使用的檔案數目(inodes)。最後兩個欄位使用來設定檔案系統上對使用者強制性與非強制性的檔案數量限制。

強制性限制是一個使用者或群組可以使用之絕對最大的磁碟空間。一旦到達這個限制，將無法使用任何的磁碟空間。

非強制性限制定義可以使用的最大磁碟空間，然而不同於強制性限制的地方在於它允許在某一段時間內超越非強制性的限制空間。這段時間稱為『寬限期』(grace period)。寬限期可以以秒、分、時、天數、週數或月份數表示。

假如任何的這些數值設為0，表示沒有設定限制。請在文字編輯器中，更改這些數值為您想要的限制值，例如：

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

如要確認已經設定好這個使用者的磁碟配額，請使用下列指令：

```
quota testuser
```

### 6.1.5. 指定每一個群組的磁碟配額

磁碟配額也可以指定給群組為單位的對象，例如您想要為devel 群組設定群組磁碟配額，請使用下列指令（在設定群組磁碟配額前，該群組必須存在）：

```
edquota -g devel
```

這個指令會在文字編輯器中顯示該群組現有的磁碟配額：

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

修改限制值，儲存檔案，然後再設定磁碟配額。

如要確認已經設定好群組的磁碟配額，請使用下列指令：

```
quota -g devel
```

### 6.1.6. 指定每一個檔案系統的磁碟配額

如要指定磁碟配額給已啟用配額機制的每一個檔案系統，請使用下列指令：

```
edquota -t
```

如同其他的edquota 指令，這個指令會在文字編輯器中開啟檔案系統目前的磁碟配額：

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

更改磁碟空間的寬限期(Block grace period)或檔案數量的寬限期(Inode grace period)，再儲存變更到檔案，然後離開文字編輯器。

## 6.2. 管理磁碟配額

假如您實作了磁碟配額，您需要做一些維護性的工作——大都是查看磁碟配額是否已超過，以及確定配額的限制是正確的。當然，假如使用者不斷地超過他們的磁碟配額限制，或者經常性的到達他們的非強制性的限制，取決於他們是何種類型的使用者以及有多少的磁碟空間衝擊他們的工作，系統管理員必須做個決定，他可以建議使用者如何使用較少的磁碟空間，或者是視需要增加該使用者的磁碟配額。

### 6.2.1. 磁碟配額的報告

您必須執行`repquota` 工具來建立一個磁碟用量的報告。例如`repquota /home` 指令會產生以下的輸出：

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

如要檢視所有啟用配額之檔案系統的磁碟用量報告，請使用以下指令：

```
repquota -a
```

雖然這個報告很容易閱讀，仍然有一些要點需要做解釋。在每一個使用者之後顯示的`--` 是用來決定是否已超過磁碟空間或檔案數量限制的一種很方便的方法。假如已超過非強制性的限制，`+` 記號會出現在相對應之`-` 的地方；第一個`-` 記號代表磁碟空間限制(Block limits)，而第二個記號代表檔案數量的限制(Inode limits)。

`grace` 欄位通常是留空的，假如已經超過非強制性的限制，這個欄位會出現一個等於寬限期所剩餘的時間，假如已經超越寬限期，這裡會出現`none`。

### 6.2.2. 保持正確的磁碟配額

每當一個檔案系統沒有按照正常程序卸載時（例如由於系統當機），便有需要執行`quotacheck` 指令。然而即使系統沒有當機，您也可以定期地執行`quotacheck`。定期地執行下列的指令將會保持更加正確的磁碟配額（所使用的選項在 6.1.1 節有詳述）：

```
quotacheck -avug
```

最簡單執行它的方法是使用`cron` 時程管理程式。您可以以`root` 身份使用`crontab -e` 指令來排成一個定期的`quotacheck`，或放置執行`quotacheck` 的一個程式碼在下列的任一個目錄中（請使用適用您需求的時間間隔）：

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

當檔案系統的分析不在使用中時，可以獲得最正確的磁碟配額資料。因此`cron` 工作應該要排定在最少使用到檔案系統的時間來執行。假如這個時間對每一個啟用磁碟配額之檔案系統都不同的話，請使用多個`cron` 工作以在不同的時間執行每一個檔案系統的`quotacheck`。

請參考第28章 以取得關於設定`cron` 的更多資訊。



### 6.2.3. 啟用與停用

在不將配額設為0的情況下也可以將它停用，如要停用所有使用者與群組的磁碟配額，請使用下列指令：

```
quotaoff -vaug
```

假如-u 或-g 選項都沒有指定，將只會停用使用者的磁碟配額。假如只指定-g，將只會停用群組的磁碟配額。

如要再次啟用磁碟配額，請使用quotaon 指令並加上相同的選項。

舉例來說，如要啟用所有檔案系統上使用者與群組的磁碟配額，請使用下列指令：

```
quotaon -vaug
```

如要啟用特定一個檔案系統（如/home）的磁碟配額：

```
quotaon -vug /home
```

假如-u 或-g 選項都沒有指定，將只會啟用使用者的磁碟配額。假如只指定-g，將只會啟用群組的磁碟配額。

## 6.3. 其他的資源

如需更多關於磁碟配額的相關資訊，請參考如下列出的有用資源。

### 6.3.1. 已安裝的說明文件

- quotacheck, edquota, repquota, quota, quotaon 與quotaoff 的man pages

### 6.3.2. 相關書籍

- *Red Hat Linux 系統管理入門* — 可在<http://www.redhat.com/docs> 與說明文件光碟上取得，這本手冊含有適用於Red Hat Linux 系統管理員新手關於儲存空間管理（包括磁碟配額）的背景資料。



## II. 安裝相關的資訊

*Red Hat Linux* 安裝手冊 中探討了Red Hat Linux 的安裝，以及一些基本的後安裝階段故障排除。然而一些進階的安裝選項則在這本手冊中有說明，這個章節提供了包括*kickstart*（一種自動化的安裝技術）、系統回復模式（假如系統無法開機進入正常的執行等級，如何啟動系統）、如何在安裝過程中設定RAID 以及LVM 等的指示。請結合這些章節與*Red Hat Linux* 安裝手冊 來執行這些任何的進階安裝工作。

### 內容目錄

7章Kickstart 安裝 .....	29
8章Kickstart 設定程式 .....	51
9章基本的系統回復 .....	67
10章軟體RAID 設定 .....	71
11章LVM 設定 .....	75



# Kickstart 安裝

## 7.1. 到底什麼是Kickstart 安裝啊？

許多系統管理員較喜歡一種自動化的安裝方式來安裝Red Hat Linux 到他們的機器上。為了要回應這樣的請求，Red Hat 創建了kickstart 的安裝方式。藉由使用kickstart，系統管理員可以建立一個單一的檔案，其中含有典型的Red Hat Linux 安裝中會詢問之所有問題的答案。

Kickstart 檔案可以保存在一部單一的伺服器上，以讓個別的電腦在安裝中讀取它。這種安裝方式可以支援使用單一的kickstart 檔案來安裝Red Hat Linux 到多部機器上，這將對網路與系統管理員造成很大的方便。

Kickstart 可幫您自動化一個Red Hat Linux 的安裝。

## 7.2. 該如何執行一個Kickstart 安裝？

Kickstart 的安裝可以使用一部本機的光碟機、硬碟機或透過NFS, FTP 或HTTP 來進行安裝。

如要使用kickstart 安裝方式，您必須：

1. 建立一個kickstart 檔案。
2. 建立一個含有kickstart 檔案的開機磁片，或使得該檔案可經由網路存取。
3. 準備好安裝目錄。
4. 開始kickstart 安裝。

這個章節將詳細地解釋這些步驟。

## 7.3. 建立Kickstart 檔案

kickstart 檔案是一個普通的文字檔案，其中含有各個關鍵字的项目清單。在Red Hat Linux 說明文件光碟中RH-DOCS 目錄下可以找到sample.ks 檔案，您可以藉由編輯這個檔案、或使用**Kickstart 設定程式** 應用程式，或者從頭撰寫這個檔案。Red Hat Linux 安裝程式也根據您在安裝過程中所選擇的選項建立了一個範例的kickstart 檔案，該檔案會存放在 /root/anaconda-ks.cfg，您也可使用任何可以儲存檔案為ASCII 文字的文字編輯器或文字處理器來編輯這個檔案。

首先，當您要建立kickstart 檔案時，請特別小心下列的事項：

- 必須以既定的順序指定各個部份，每一個部份中的項目不必以特定的順序排列（除非另外有指定），主要的順序如下：
  - 指令部份— 請參考 7.4 節 以取得kickstart 選項的清單，您必須含括必要的選項。
  - %packages 部份— 請參考 7.5 節 以取得詳細資訊。
  - %pre 與%post 部份— 這兩個部份可以是任何的順序，而且不是必要的。請參考 7.6 節 與 7.7 節 以取得詳細資訊。
- 可以忽略不必要的項目。
- 如果忽略了必要的項目，將會導致安裝程式提示使用者輸入相關項目的答案，就如同在典型的安裝中提示使用者的狀況一樣。在給予答案後，將繼續自動化的安裝程式（除非又找到另一個遺失的項目）。

- 以井字號開頭的行會被視為註解，且會忽略它。
- 至於kickstart的升級，下列的項目是必要的：
  - 語言
  - 語系支援
  - 安裝類型
  - 裝置指定（假如需要一個裝置來執行安裝）
  - 鍵盤設定
  - upgrade 關鍵字
  - 開機管理程式設定

假如尚有其他的項目被指定來做升級，那些項目將會被忽略（請注意這裡包括套件的選擇）。

## 7.4. Kickstart 的選項

下列的選項可以被放置在一個kickstart檔案中，假如您較喜歡使用圖形的介面來建立您的kickstart檔案，您可以使用**Kickstart 設定程式**，請參考第8章以取得詳細資訊。



### 請注意

假如選項後面接著一個等號(=)，必須在其後指定一個數值。在範例的指令中，括號()中的選項是該指令可選的參數。

autostep (可選的)

類似interactive，除了它將帶您進入下一個畫面，它大部分被用來做除錯。

auth或authconfig (必要的)

設定系統的認證選項，類似authconfig指令，這將會在安裝之後執行。預設情況下，通常會將密碼加密處理，而不使用shadow。

--enablemd5

使用md5的編碼方式在使用者的密碼上。

--enablenis

開啟NIS支援。預設情況下，--enablenis將使用在網路上找到的網域，不過您總是必須要手動使用--nisdomain=選項設定一個網域。

--nisdomain=

NIS服務所使用的NIS網域名稱。

--nisserver=

NIS服務所使用的伺服器（預設為廣播尋找）。

--useshadow或--enablesshadow

使用shadow密碼。

`--enableldap`

開啟 `/etc/nsswitch.conf` 檔案中的 LDAP 支援，使得您的系統從一個 LDAP 目錄擷取關於使用者的資訊 (UIDs、家目錄、shells 等等)。如要使用這個選項，您必須安裝 `nss_ldap` 套件，您也必須使用 `--ldapserver=` 與 `--ldapbasedn=` 來指定一部伺服器以及一個 base DN。

`--enableldapauth`

使用 LDAP 當作一個認證方式，這將會啟用使用一個 LDAP 目錄當作認證與更改密碼的 `pam_ldap` 模組。如要使用這個選項，您必須安裝 `nss_ldap` 套件，您也必須使用 `--ldapserver=` 與 `--ldapbasedn=` 來指定一部伺服器以及一個 base DN。

`--ldapserver=`

假如您有指定 `--enableldap` 或 `--enableldapauth`，請使用這個選項來指定欲使用的 LDAP 伺服器名稱，這個選項是設定在 `/etc/ldap.conf` 檔案中。

`--ldapbasedn=`

假如您有指定 `--enableldap` 或 `--enableldapauth`，請使用這個選項來指定欲使用的 LDAP 目錄樹中的 DN (distinguished name)，在其中儲存了使用者的資訊。這個選項是設定在 `/etc/ldap.conf` 檔案中。

`--enableldaptls`

使用 TLS (Transport Layer Security) 搜尋。這個選項使得 LDAP 在做認證之前，傳送已加密的使用者名稱與密碼到一部 LDAP 伺服器。

`--enablekrb5`

使用 Kerberos 5 來認證使用者，Kerberos 本身並不知道使用者的家目錄、UIDs 或 shells 等資訊，所以假如您要啟用 Kerberos，您則必須藉由啟用 LDAP、NIS 或 Hesiod 來使這個工作站認識使用者的帳號資訊，或者使用 `/usr/sbin/useradd` 指令。假如您要使用這個選項，您必須安裝 `pam_krb5` 套件。

`--krb5realm=`

您的工作站所隸屬的 Kerberos 5 領域 (realm) 名稱。

`--krb5kdc=`

在這個領域中伺服器要求的 KDC (或 KDCs)。假如您的領域中有多部 KDCs，請以逗號 (,) 將它們分隔開。

`--krb5adminserver=`

領域中的 KDC 也一樣執行 `kadmin`。這部伺服器將處理密碼更改以及其他的管理性要求。假如您有一個以上的 KDC，這部伺服器必須在主要的 KDC 中執行。

`--enablehesiod`

啟用 Hesiod 支援以搜尋使用者家目錄、UIDs 與 shells。更多關於在您的網路中設定與使用 Hesiod 的資訊在 `/usr/share/doc/glibc-2.x.x/README.hesiod` 檔案中 (收錄於 `glibc` 套件)。Hesiod 是 DNS 的一種延伸，它使用 DNS 紀錄來儲存關於使用者、群組以及其他許多項目的資訊。

`--hesiodlhs`

設定於 `/etc/hesiod.conf` 檔案中的 Hesiod LHS ("left-hand side") 選項。這個選項是由 Hesiod 函式庫所使用，以決定當搜尋資訊時從 DNS 搜尋的名稱為何，類似 LDAP 所使用的一個 base DN。

--hesiodrhs

設定於/etc/hesiod.conf 檔案中的Hesiod RHS ("right-hand side") 選項。這個選項是由Hesiod 函式庫所使用，以決定當搜尋資訊時從DNS 搜尋的名稱為何，類似LDAP 所使用的一個base DN。



#### 建議

如要搜尋"jim" 的使用者資訊，Hesiod 函式庫會搜尋jim.passwd<LHS><RHS>，這應該會解析為一個TXT 的紀錄，使得他的密碼紀錄就如同原本的格式一樣(jim:\*:501:501:Jungle Jim:/home/jim:/bin/bash)。至於群組，這個狀況是相同的，除了將會使用jim.group<LHS><RHS>。

以數字的方式搜尋使用者與群組是經由指定"501.uid" 為"jim.passwd" 的一個CNAME，以及指定"501.gid" 為"jim.group" 的一個CNAME 來做到。請注意當函式庫取決要搜尋的名稱時，LHS 與RHS 並不含一個句點[.] 在它們的前面，所以LHS 與RHS 通常以句點開頭。

--enablesmbauth

啟用針對一部SMB 伺服器（典型的一部Samba 或Windows 伺服器）的使用者認證。SMB 認證支援並不了解什麼是家目錄、UIDs 或shells，所以假如您要啟用它，您則必須藉由啟用LDAP、NIS 或Hesiod 來使這個工作站認識使用者的帳號資訊，或者使用/usr/sbin/useradd 指令。如要使用這個選項，您必須安裝pam\_smb 套件。

--smbservers=

用作SMB 認證的伺服器名稱，如要指定一部以上的伺服器，請以逗號(,)將它們分隔開。

--smbworkgroup=

SMB 伺服器所屬的工作群組名稱。

--enablecache

啟用nscd 服務，nscd 服務會快取儲存關於使用者、群組以及許多其他類型的資訊。假如您選擇使用NIS、LDAP 或hesiod 來透過網路散佈使用者與群組的資訊，快取的功能則相當的好用。

bootloader (必要的)

指定該如何安裝開機管理程式以及應該安裝LILO 或GRUB。不管您是執行安裝或升級，這個選項都是必要的。於升級模式，假如您沒有指定--useLilo，而且LILO 是目前的開機管理程式，開機管理程式將會變更為GRUB。如要在升級中保留LILO，請使用bootloader --upgrade。

--append=

指定核心參數，如要指定多個核心參數，請以空白字元將它們隔開，如：  
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"

--location=

指定要於何處寫入開機紀錄，有效的數值如下：mbr (預設值)、partition (安裝開機管理程式到含有核心之分割區的第一個區段)，或none (不安裝開機管理程式)。

--password=

假如使用GRUB，請以這個選項指定要設定的GRUB 開機管理程式密碼。最好使用這個選項來限制對GRUB shell 的存取，因為在其中可以傳送任意的核心參數。



`--md5pass=`

假如使用GRUB，這個選項類似`--password=`，加上密碼已經加密處理過了。

`--useLilo`

使用LILO 當作開機管理程式（而不是GRUB）。

`--linear`

假如使用LILO，您可以使用`linear LILO`的選項；這只適用於向後相容（而現在預設使用`linear`）。

`--nolinux`

假如使用LILO，您可以使用`nolinux LILO`選項；預設為`linear`。

`--lba32`

假如使用LILO，強制使用`lba32`模式，而不是自動偵測。

`--upgrade`

升級既有的開機管理程式設定，並保留舊有的紀錄。這個選項只在升級時才能使用。

#### `clearpart`（可選的）

建立新的分割區之前，移除系統中的分割區。預設情況下不會移除任何的分割區。



#### 請注意

假如使用`clearpart`指令，`--onpart`指令則不能被使用在一個邏輯分割區上。

`--linux`

移除所有的Linux 分割區。

`--all`

移除系統上所有的分割區。

`--drives=`

指定要移除分割區的磁碟機，舉例來說，下列指令將會移除主IDE 控制卡上前兩個磁碟機的分割區：

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

`--initlabel`

初始磁碟標籤為適用您主機架構的預設值（例如`msdos`代表x86，而`gpt`代表Itanium）。這使得安裝程式不詢問是否應該初始磁碟標籤（當安裝到一個全新的硬碟上時）。

#### `device`（可選的）

在大部份的PCI 系統上，安裝程式將會自動偵測乙太網路卡與SCSI 控制卡，然而在舊式的系統與某些PCI 系統上，`kickstart`需要一個暗示以找到適當的裝置。告知安裝程式來安裝額外模組的`device`指令為以下這個格式：

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

<type>

以scsi 或eth 取代之

<moduleName>

以應該要安裝的核心模組名稱取代之。

--opts=

傳送至核心模組的選項，請注意您也可以傳送多個選項，只要以雙引號將多個選項括住即可，例如：

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

deviceprobe (可選的)

強制偵測PCI 匯流排，並載入找到之所有裝置的模組（假如該模組是可用的）。

driverdisk (可選的)

可以在kickstart 安裝中使用驅動程式磁片，您必須複製驅動程式磁片的內容到系統硬碟上分割區的根目錄下，然後您便可以使用driverdisk 指令來告知安裝程式去何處找到驅動程式磁片。

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

<partition>

含有驅動程式磁片的分割區。

--type=

檔案系統類型（例如vfat 或ext2）。

firewall (可選的)

這個選項是對應到安裝程式中的『防火牆設定』畫面：

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

<securitylevel>

以下列的一種安全性等級取代之：

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

--trust=

在此列出一個裝置（例如eth0），這將使得所有來自該裝置的網路流量都可通過防火牆。如要列出一個以上的裝置，請使用--trust eth0 --trust eth1。請勿使用以逗號分開的格式，如--trust eth0, eth1。

<incoming>

請使用以下的服務名稱取代之，使得指定的服務通過防火牆。

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

--port=

您可以使用port:protocol 格式來指定允許通過防火牆的連接埠。舉例來說，如要允許IMAP存取通過您的防火牆，請指定imap:tcp。您也可以指定特定的數值連接埠，如1234:udp表示允許在1234埠號的UDP封包通過防火牆。如要指定多個連接埠，請以逗號將它們隔開。

install (可選的)

告知系統安裝一個全新的系統，而不是升級一個舊有的系統，這是預設的模式。至於安裝，您必須指定cdrom, harddrive, nfs 或url (用於ftp 或http 安裝方式) 的其中一種安裝方式。install 指令與安裝方式指令必須放在不同行。

cdrom

從系統上第一個光碟機進行安裝。

harddrive

從本機硬碟上 (必須是vfat 或ext2 檔案系統) 的一個Red Hat 安裝目錄進行安裝。

- --partition=  
安裝來源的分割區 (如sdb2)。
- --dir=  
安裝目錄中含有RedHat 子目錄的目錄名稱。

例如：

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

nfs

從所指定的NFS 伺服器進行安裝。

- --server=  
安裝來源的伺服器 (主機名稱或IP 位址)。
- --dir=  
安裝目錄中含有RedHat 子目錄的目錄名稱。

例如：

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

url

透過FTP或HTTP，從一部遠端伺服器中的安裝目錄進行安裝。

例如：

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

或：

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

interactive (可選的)

在安裝過程中使用kickstart 檔案所提供的資訊，不過卻允許您檢查與修改所給予的數值。您將會被呈現安裝程式中的每一個畫面，並且含有來自kickstart 檔案的數值，您可以藉由點選下一步 接受設定，或更改數值後點選下一步 繼續。也請您參閱autostep。

keyboard (必要的)

設定系統鍵盤類型，以下是適用於i386, Itanium 以及Alpha 機器的鍵盤類型清單：

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-nodeadkeys, dk, dk-latin1, dvorak, es, et,
fi, fi-latin1, fr, fr-latin0, fr-latin1, fr-pc, fr_CH, fr_CH-latin1,
gr, hu, hul01, is-latin1, it, it-ibm, it2, jpl06, la-latin1, mk-utf,
no, no-latin1, pl, pt-latin1, ro_win, ru, ru-cpl251, ru-ms, rul, ru2,
ru_win, se-latin1, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querly, slovene, trq, ua,
uk, us, us-acentos
```

/usr/lib/python2.2/site-packages/rhpl/keyboard\_models.py 中也含有這個清單，而它是rhpl 套件的一部分。

lang (必要的)

設定安裝過程中要使用的語言，例如要設定語言為繁體中文，kickstart 檔案中必須含有下列這一行：

```
lang zh_TW
```

/usr/share/redhat-config-language/locale-list 檔案中每一行的第一個欄位提供了有效語系碼的清單，這個檔案是redhat-config-languages 套件的一部分。

langsupport (必要的)

設定要安裝到系統的語系支援，lang 所使用的語系碼也可使用在langsupport。

如要安裝一種語言，請指定它，例如要安裝繁體中文支援(zh\_TW)：

```
langsupport zh_TW
```

```
--default=
```

假如指定多個語系支援，則必須指定一個預設的語系。

舉例來說，您想安裝英文與繁體中文，而想使用英文為預設語系：

```
langsupport --default=en_US zh_TW
```

假如您使用--default 的選項，並且只加上一種語言，這將會安裝所有語言，並以指定的語言為預設語言。

lilo (已由bootloader 所取代)



警告

這個選項已經由bootloader 所取代，而且只能用於向後相容。請參考bootloader 選項。

在此指定應該要如何安裝開機管理程式到系統上，預設情況下，LILO 將會安裝到第一磁碟機的MBR，假如有找到一個DOS 分割區的話，將會安裝一個多重開機的系統（當使用者在LILO: 提示符號輸入dos，將會啟動DOS/Windows 系統）。

--append <params>

指定核心參數。

--linear

使用linear 的LILO 選項；這只可用於向後相容（而且現在已預設使用linear）。

--nolinear

使用nolinear 的LILO 選項；現在已預設使用linear。

--location=

指定要寫入LILO 開機紀錄的位置，有效的數值如下：mbr（預設值）或partition（安裝開機管理程式到含有核心之分割區的第一個區段）。假如沒有指定位置，將不會安裝LILO。

--lba32

強制使用lba32 模式，而不是使用自動偵測。

lilocheck (可選的)

假如有設定lilocheck 的話，安裝程式將會在第一個磁碟機的MBR 上尋找LILO 的存在，假如有找到的話，將會重新啟動系統— 在這樣的情況下，將不會執行任何的安裝。這將可避免kickstart 重新安裝一個已經安裝好的系統。

logvol (可選的)

使用下列語法來建立用於邏輯磁區管理(LVM)的一個邏輯磁區：

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

先建立分割區，再建立邏輯磁區群組，然後再建立邏輯磁區，例如：

```
part pv.01 --size 3000
```

```
volgroup myvg pv.01
```

```
logvol / --vgname=myvg --size=2000 --name=rootvol
```

mouse (必要的)

設定用於圖形與文字介面模式的系統滑鼠，可使用的選項有：

--device=

滑鼠所連接的裝置介面（例如--device=ttyS0）。

--emulthree

這個選項將會使 X 視窗系統認定同時按下滑鼠的左右兩鍵為滑鼠的中間按鍵。假如您有的是兩鍵式的滑鼠，應該要使用這個選項。

在選項之後，可以在其後指定以下其中一種滑鼠類型：

```
alpsps/2, ascii, asciiips/2, atibm, generic, generic3, genericps/2,
generic3ps/2, genericwheelps/2, genericusb, generic3usb, genericwheelusb,
geniusnm, geniusnmps/2, geniusprops/2, geniusscrollps/2, geniusscrollps/2+,
```

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

您也可在 `/usr/lib/python2.2/site-packages/rhpl/mouse.py` 檔案中找到這個清單，該檔案是 `rhpl` 套件的一部分。

假如所設定的滑鼠指令沒有給予任何的引數，或是省略掉了。安裝程式將會試著自動偵測滑鼠，這個過程可使用在大部分當代的滑鼠。

network (可選的)

為系統設定網路資訊，假如 `kickstart` 安裝不需要網路連線（也就是說，它不是透過 NFS、HTTP 或 FTP 來進行安裝），則不會在系統上設定網路連線。假如安裝確實需要網路連線，而且在 `kickstart` 檔案中沒有提供任何的網路資訊，Red Hat Linux 安裝程式會假定安裝是透過 `eth0` 經由一個動態的 IP 位址 (BOOTP/DHCP) 所完成，並且設定最後安裝好的系統動態決定它的 IP 位址。`network` 的選項為透過網路的 `kickstart` 安裝過程以及安裝好的系統設定網路連線的資訊。

--bootproto=

請使用 `dhcp`, `bootp` 或 `static` 的其中一種。

預設為 `dhcp`，而 `bootp` 與 `dhcp` 被視為相同的。

DHCP 的方式使用一部 DHCP 伺服器系統來取得它的網路連線資訊，您也許會猜想，BOOTP 的方式應該是類似的，需要一部 BOOTP 伺服器以供應網路連線資訊。如要設定一部系統使用 DHCP：

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

如要設定一部系統使用 BOOTP 來取得它的網路連線設定資訊，請使用下列的資訊在 `kickstart` 檔案中：

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

靜態 (static) 的方式需要您輸入所有必要的網路連線資訊到 `kickstart` 檔案中，如名稱所示，這個資訊是靜態的，而且將會被使用在安裝過程與安裝完成後。用來設定靜態網路連線的選項比較複雜，因為您必須含括所有的網路設定資訊在一行中。您必須指定 IP 位址網路遮罩開道器與名稱伺服器，例如 (\ 符號表示這是在同一行)：

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

假如您使用靜態的方法，請注意下列的兩種限制：

- 所有靜態網路連線的資訊必須在同一行中指定，您不能使用反斜線來換行。
- 您只能在這裡指定一個名稱伺服器，然而您可以使用 `kickstart` 檔案的 `%post` 部份（在 7.7 節有說明）來增加更多的名稱伺服器（如果需要的話）。

--device=

使用來選擇一個特定的乙太網路裝置以做安裝，請注意，除非kickstart 檔案是一個本機的檔案（如ks=floppy），否則將無法使用--device= 選項，因為安裝程式必須先設定好網路才能找到該kickstart 檔案，例如：

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

--ip=

要安裝之機器的IP 位址。

--gateway=

預設閘道器的IP 位址。

--nameserver=

主要名稱伺服器的IP 位址。

--nodns

不設定任何的DNS 伺服器。

--netmask=

要安裝之系統的網路遮罩。

--hostname=

要安裝之系統的主機名稱。

part 或partition（安裝時是必要的，升級時請忽略）

為系統建立一個分割區。

假如系統上的其他分割區有存在多個Red Hat Linux 的安裝，安裝程式將會提示使用者並且詢問要升級那一個安裝。



**警告**

除非有使用--noformat 與--onpart，否則所有建立的分割區都會在安裝過程中被格式化。

<mntpoint>

<mntpoint> 是分割區將會被掛載的地方，必須是以下的其中一種形式：

- /<path>

例如/, /usr, /home

- swap

這個分割區將被視為一個swap 空間。

如要自動決定swap 分割區的大小，請使用--recommended 選項：

```
swap --recommended
```

自動產生之swap 分割區的最小空間不可小於系統中實體記憶體容量，而且不可大於系統實體記憶體的兩倍容量。

- raid.<id>

該分割區將被使用來當作軟體RAID 用途（請參考raid）。

- pv.<id>

該分割區將被使用來當作LVM用途（請參考logvol）。

`--size=`

以MB表示的最小分割區大小，請在此指定一個整數的數值，例如500。請勿在數字後面加上MB。

`--grow`

告知分割區填滿可使用的空間（如果有的話），或填滿至最大可允許的設定。

`--maxsize=`

當設定分割區的空間可增大時，在此指定最大的分割區大小。請在此指定一個整數數值，而且請勿在數值後面加上MB。

`--noformat`

告知安裝程式不格式化分割區，可與`--onpart`指令一併使用。

`--onpart=` 或 `--usepart=`

放置分割區在已經存在的裝置，例如：

```
partition /home --onpart=hdal
```

將會放置/home在/dev/hdal這個既有的裝置。

`--ondisk=` 或 `--ondrive=`

強制建立分割區在一個特定的磁碟上，例如`--ondisk=sdb`指令將會放置分割區在系統上的第二個SCSI磁碟。

`--asprimary`

強制自動分派該分割區為一個主分割區，否則磁碟分割將會失敗。

`--bytes-per-inode=`

所指定的數字代表檔案系統建立時每一個inode的位元組數量。在此必須指定一個十進制的格式，當您想要為應用程式增加檔案系統上的inode數量時，這個選項便會很有用。

`--type=`（已由fstype所取代）

這個選項已不存在，請使用fstype。

`--fstype=`

設定分割區的檔案系統類型，有效的數值為ext2, ext3, swap與vfat。

`--start=`

請指定分割區起始的磁柱位置，您也必須使用`--ondisk=`或`ondrive=`來指定一個磁碟機，也需要您使用`--end=`來指定結束磁柱的位置，或者使用`--size=`來指定分割區的大小。

`--end=`

指定分割區結束的磁柱位置，您也必須使用`--start=`來指定分割區起始的磁柱位置。

`--badblocks`

指定分割區應該要被檢查是否有損壞的磁區。





## 請注意

假如因為某種因素導致磁碟分割失敗，系統診斷訊息將會出現在虛擬主控台3。

## raid (可選的)

組合一個軟體RAID裝置，這個指令如下所示：

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

<mntpoint>

掛載RAID檔案系統的位置，假如它是/，RAID level 必須是1，除非已有一個開機分割區(/boot)，假如一個開機分割區已經存在，/boot 分割區必須是level 1，而根目錄(/) 分割區可以是任何的類型。<partitions\*> (表示可以列出多個分割區) 列出欲增加至RAID陣列的RAID標識符。

--level=

要使用的RAID level(0, 1 或5)。

--device=

要使用的RAID裝置名稱(如md0 或md1)。RAID裝置範圍從md0 到md7，而且每一個只能使用一次。

--spares=

指定分配給RAID陣列的備援磁碟機數量，備援磁碟機是當磁碟發生錯誤時用來重建陣列的。

--fstype=

設定RAID陣列的檔案系統類型，有效的數值是ext2, ext3, swap 與vfat。

--noformat

請勿格式化RAID陣列。

以下的例子顯示如何建立一個RAID level 1 的分割區給/，以及一個RAID level 5 給/usr，在此假設系統上有三個SCSI磁碟機。也會建立三個swap分割區(每一個磁碟上各建立一個)。

```
part raid.01 --size=60 --ondisk=sda
part raid.02 --size=60 --ondisk=sdb
part raid.03 --size=60 --ondisk=sdc
part swap --size=128 --ondisk=sda
part swap --size=128 --ondisk=sdb
part swap --size=128 --ondisk=sdc
part raid.11 --size=1 --grow --ondisk=sda
part raid.12 --size=1 --grow --ondisk=sdb
part raid.13 --size=1 --grow --ondisk=sdc
raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

## reboot (可選的)

安裝完成後重新開機(沒有任何引數)。通常kickstart 會顯示一個訊息，並在重新開機前等待使用者按下一個按鍵。

## rootpw (必要的)

設定系統的root密碼為<password>引數。

```
rootpw [--iscrypted] <password>
```

`--iscrypted`

假如有使用這個的話，表示密碼引數已經經過加密了。

`skipx` (可選的)

如果有這個選項的話，安裝的系統上將不設定X。

`text` (可選的)

以文字模式執行kickstart 安裝，Kickstart 安裝是預設以圖形模式執行的。

`timezone` (必要的)

設定系統的時區為`<timezone>`，它可以是`timeconfig` 指令所列出的任何時區。

`timezone [--utc] <timezone>`

`--utc`

假如使用這個選項的話，系統將假定硬體時鐘設定為UTC (格林威治標準時間) 時間。

`upgrade` (可選的)

告知系統升級一個既有的安裝，而不是安裝一個全新的系統，您必須指定`cdrom`, `harddrive`, `nfs` 或`url` (用於`ftp` 與`http` 安裝) 當作安裝目錄的位置，請參考`install` 以取得詳細資訊。

`xconfig` (可選的)

設定X 視窗系統，假如沒有給予這個選項，而有選擇安裝X，使用者則必須在安裝過程中手動地設定X；假如不要安裝X 在系統上，則不應該使用這個選項。

`--noprobe`

不偵測螢幕。

`--card=`

使用指定的顯示卡；這張顯示卡的名稱必須是來自`/usr/share/hwdata/Cards` 檔案中所列出的顯示卡清單 (來自`hwdata` 套件)。這個清單也可在**Kickstart 設定程式**的『**X 組態設定**』畫面中找到。假如在此沒有提供任何引數，安裝程式將會偵測PCI 匯流排上的介面卡，因為AGP 也是PCI 匯流排的一部分，AGP 顯示卡也會被偵測到 (假如有支援的話)。偵測的順序是由主機板上的PCI 掃描順序所決定。

`--videoram=`

指定顯示卡上的顯示記憶體容量。

`--monitor=`

使用指定的螢幕類型；螢幕名稱可以在`/usr/share/hwdata/MonitorsDB` 檔案中的螢幕清單找到 (來自`hwdata` 套件)。該螢幕清單也可在**Kickstart 設定程式**的『**X 組態設定**』畫面中找到。假如有提供`--hsync` 或`--vsync`，將會忽略這個選項。假如沒有提供任何的螢幕資訊，安裝程式將會試著自動偵測它。

`--hsync=`

指定螢幕的水平掃描頻率。

```
--vsync=
    指定螢幕的垂直掃描頻率。
```

```
--defaultdesktop=
    指定GNOME 或KDE 以設定為預設的桌面（假設GNOME 桌面環境或KDE 桌面環境已經透過%packages 安裝了）。
```

```
--startxonboot
    在安裝的系統上使用圖形的登入畫面。
```

```
--resolution=
    指定安裝系統上X 視窗系統的預設解析度，有效的數值為640x480, 800x600, 1024x768, 1152x864, 1280x1024, 1400x1050, 1600x1200。請確定有指定一個與顯示卡以及螢幕相容的解析度。
```

```
--depth=
    指定安裝系統上X 視窗系統的彩度，有效數值為8, 16, 24 與32。請確定有指定一個與顯示卡以及螢幕相容的彩度。
```

volgroup (可選的)

以下列的語法建立一個邏輯磁區管理(LVM)群組：

```
volgroup name partition
```

先建立分割區，再建立邏輯磁區群組，然後再建立邏輯磁區，舉例來說：

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

zerombr (可選的)

假如有指定zerombr，而且yes 是它主要的引數，在磁碟上找到的任何無效磁碟分割表都會被初始化，這將會摧毀含有無效磁碟分割表之磁碟的所有內容。這個指令應該是以下列的格式：

```
zerombr yes
```

沒有其他的格式是有效的。

%include

在kickstart 檔案中使用%include /path/to/file 指令來含括另一個檔案的內容，就好像該檔案的內容是在kickstart 檔案中%include 指令的位置。

## 7.5. 套件選擇

使用%packages 指令來開始一個kickstart 檔案部份用來列出您想要安裝的套件（這只適用於安裝，因為升級過程中並不支援套件選擇）。

可以使用套件群組或個別的套件名稱來指定套件，安裝程式有定義含括相關套件的許多套件群組，請參考Red Hat Linux 第一片安裝光碟中的RedHat/base/comps.xml 檔案以取得群組的清單。每一個群組都有一個id、使用者可見的數值、名稱、說明以及套件清單。在套件清單中，假如有選取該群組，標示為mandatory 的套件都會安裝，而如果該群組有被選取的話，標示為default 的套件則會被預設選取，然而即使該群組有被選取要安裝，也必須特地選取標示為optional 的套件。

大部分情況下，只需要列出群組而不是個別的套件，請注意預設都必定有選取Core 與Base 群組，所以並不需要在%packages 的部份指定它們。

這裡是`%packages` 部份的一個例子：

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

如您所見，套件群組是以一行一個來指定，先以一個`@` 符號開頭，再接上一個空白字元，然後是完整的群組名稱（如`comps.xml` 檔案中所指定的）。如要指定個別套件，請只列出該套件的名稱，不加上任何的字元（在以上例子中的`galeon` 一行，便是個別套件的例子）。

您也可以指定不安裝預設套件清單中的套件：

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

`%packages` 有兩個選項可以使用。

#### `--resolvedeps`

安裝所列出的套件，並自動解決套件相依性的問題。假如沒有指定這個選項，而安裝過程中有套件相依性的問題，自動化的安裝將會暫停，並提示使用者做相關的動作，例如：

```
%packages --resolvedeps
```

#### `--ignoredeps`

忽視未解決的相依性問題，並且安裝不含相依性問題的列出套件，例如：

```
%packages --ignoredeps
```

#### `--ignoremissing`<sup>1</sup>

在不暫停安裝以詢問安裝是否該停止或繼續的情況下，便忽視遺失的套件或群組，例如：

```
%packages --ignoremissing
```

## 7.6. 前置安裝程式碼

您可以增加在`ks.cfg` 檔案被解析後立即在系統上執行的指令，這個部份必須在`kickstart` 檔案的最後（在指令之後），而且必須以`%pre` 指令開頭。您可以在`%pre` 部份存取網路，然而在此尚未設定『名稱服務』，所以只能使用IP 位址。



### 請注意

請注意前置安裝程式碼無法在更改根目錄的環境下執行。

#### `--interpreter /usr/bin/python`

您可以指定一個不同的程式語言，例如Python，請以您所選擇之程式語言取代`/usr/bin/python`。

---

1. 這是Red Hat Linux 9 的新選項。

### 7.6.1. 範例

這裡是一個

```
pre
```

部份的範例：

```
%pre

#!/bin/sh

hds=""
mymedia=""

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

set $hds
numhd=`echo $#`

drive1=`echo $hds | cut -d' ' -f1`
drive2=`echo $hds | cut -d' ' -f2`

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

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

這個程式碼會決定系統上的硬碟數量，並以不同的磁碟分割機制來寫入一個文字檔案（取決於有一個或兩個硬碟）。您可以不用在kickstart 檔案中指定一組磁碟分割指令，只需要將以下這行加入即可：

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

將會使用在程式碼中選取的磁碟分割指令。

### 7.7. 後續安裝程式碼

您也可以選擇增加在安裝完成後要在系統上執行的指令，這個部份必須在kickstart 檔案的最後，而且必須以

```
post
```

 指令開頭，這個部份在例如安裝其他的軟體以及設定另一部名稱伺服器時相當好用。

**請注意**

假如您以靜態的IP 資訊（含有一部名稱伺服器）來設定網路，您可以在`%post` 部份存取網路並且解析IP 位址。假如您設定網路為使用DHCP，當安裝程式執行`%post` 部份時，`/etc/resolv.conf` 檔案還尚未完成。您可以存取網路，不過您無法解析IP 位址，因此假如您使用DHCP，您必須在`%post` 部份指定IP 位址。

**請注意**

後續安裝的程式碼是在`chroot` 的環境下執行的，因此執行例如從安裝媒體複製程式碼或RPMs 將無法使用。

```
--nochroot
```

使您可以指定在`chroot` 環境之外執行的指令。

以下的例子會複製`/etc/resolv.conf` 檔案到剛安裝好的檔案系統中。

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

```
--interpreter /usr/bin/python
```

使您可以指定一個不同的程式語言，例如Python，請以您所選擇的程式語言取代`/usr/bin/python`。

**7.7.1. 範例**

啟動或停止服務：

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

從一個NFS 的共享資源上執行一個名為`runme` 的程式碼：

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

新增一個使用者到系統中：

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

## 7.8. 使Kickstart 檔案可存取

kickstart 檔案必須存放在以下的其中一個位置：

- 開機磁碟片上
- 開機光碟片上
- 網路上

通常我們會複製kickstart 檔案到開機磁碟片上，或使其可在網路上被存取。網路為主的方法最常被使用，因為大部分的kickstart 安裝都是在網路連線的電腦上執行的。

現在讓我們來仔細討論一下kickstart 檔案可以放置何處。

### 7.8.1. 建立一片Kickstart 的開機磁片

如要執行一個磁片為主的kickstart 安裝，該kickstart 檔案必須命名為`ks.cfg`，而且必須放置在開機片的最上層目錄。請參考*Red Hat Linux* 安裝手冊中的『建立一片安裝程式開機磁片』一節以取得關於建立開機磁片的指示。因為Red Hat Linux 的開機磁片是MS-DOS 格式的，在Linux 下您可以很容易的使用`mcopy` 指令來複製kickstart 檔案：

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

或者您可以使用Windows 來複製檔案，您也可以在Red Hat Linux 下以`vfat` 的檔案系統類型掛載MS-DOS 的開機片，然後使用`cp` 指令來複製檔案到磁片上。

### 7.8.2. 建立一片Kickstart 的開機光碟

如要執行一個光碟為主的kickstart 安裝，kickstart 檔案必須命名為`ks.cfg`，而且必須放置在開機光碟的最上層目錄。因為光碟片是僅能讀取的，該檔案必須增加至使用來建立寫入光碟之映像檔的目錄，請參考*Red Hat Linux* 安裝手冊中的『建立一片安裝程式的開機光碟』一節以取得關於建立開機光碟的指示；然而在建立`file.iso` 映像檔案之前，請複製`ks.cfg` kickstart 檔案到`isolinux/` 目錄中。

### 7.8.3. 使Kickstart 檔案可經由網路存取

使用kickstart 的網路安裝是很常見的，因為系統管理員可以在許多網路連線的電腦上快速且簡單的執行自動安裝。一般來說，這種方法最常用在當系統管理員在區域網路中擁有一部BOOTP/DHCP 伺服器以及一部NFS 伺服器，BOOTP/DHCP 伺服器是用來提供用戶端系統它的網路連線資訊，而安裝過程中所用到的檔案，實際上是由NFS 伺服器所供應的。通常這兩部伺服器是在同一部實體機器上執行，不過這並不是必要的。

如要執行一個網路為主的kickstart 安裝，在您的網路上必須要有一部BOOTP/DHCP 伺服器，而且它必須包含您要用來安裝Red Hat Linux 機器的設定資訊。BOOTP/DHCP 伺服器將會提供用戶端它的網路連線資訊，以及kickstart 檔案的位置。

假如kickstart 檔案是由BOOTP/DHCP 伺服器所指定，用戶端系統將會試著執行一個該檔案路徑的NFS 掛載，並且將會複製指定的檔案到用戶端機器中，使用它來當作kickstart 檔案。在此所需的確實設定取決於您所使用的BOOTP/DHCP 伺服器。

這裡是來自Red Hat Linux 所收錄之DHCP 伺服器的`dhcpd.conf` 檔案中一行的範例：

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

請注意您必須以kickstart 的檔案名稱取代`filename` 之後的數值（或者kickstart 檔案所存放的目錄），以NFS 伺服器的名稱取代`next-server` 之後的數值。

假如BOOTP/DHCP 伺服器所傳回的檔名是以斜線("/")結尾，而它則被解釋為一個路徑。在這個情況下，用戶端系統使用NFS 掛載該路徑，並且搜尋一個特定的檔案，用戶端所搜尋的檔名是：

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

檔名的<ip-addr> 部份應該以用戶端的加點十進位IP 位址表示法取代，例如對擁有10.10.0.1 IP 位址的電腦之檔名應為10.10.0.1-kickstart。

請注意假如您沒有指定一個伺服器名稱，用戶端系統將會試著使用回應BOOTP/DHCP 要求的伺服器當作它的NFS 伺服器，假如您沒有<ip-addr>-kickstart 檔名搜尋kickstart 檔案。

## 7.9. 使安裝目錄可存取

kickstart 安裝需要存取一個『安裝目錄』，一個安裝目錄是含有與二進制的Red Hat Linux 光碟片相同目錄結構的一個複本。

假如您執行一個光碟片為主的安裝，請在開始kickstart 安裝前先放入Red Hat Linux 第一片光碟。

假如您執行一個硬碟的安裝，請確定二進制Red Hat Linux 光碟片的ISO 映像檔已經存放在電腦中的硬碟上了。

假如您要執行一個網路為主的安裝方式 (NFS, FTP 或HTTP)，您必須讓安裝目錄在網路上可被存取，請參考Red Hat Linux 安裝手冊 中的『準備網路安裝』一節以取得詳細資訊。

## 7.10. 開始Kickstart 安裝

如要開始一個kickstart 的安裝，您必須從Red Hat Linux 開機片、Red Hat Linux 開機光碟或Red Hat Linux 第一片光碟啟動系統，然後在開機提示符號下輸入一個特殊的開機指令。當ks 命令列參數傳送到核心後，安裝程式將會尋找kickstart 檔案的存在。

### 開機片

假如kickstart 檔案是放置在一片開機片上 (如 7.8.1 節 所述)，請使用該磁片啟動系統，然後在boot: 提示符號輸入以下指令：

```
linux ks=floppy
```

### 第一片光碟以及磁片

假如ks.cfg 檔案是放置在磁碟片上一個vfat 或ext2 檔案系統中，而且您從Red Hat Linux 第一片光碟開機，您也可以使用linux ks=floppy 指令。

另一個開機指令是從Red Hat Linux 第一片光碟開機，而且將kickstart 檔案放置在磁片上的vfat 或ext2 檔案系統中。如要如此做，請在boot: 提示符號下輸入下列指令：

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

### 使用驅動程式磁片

假如您需要在kickstart 安裝使用驅動程式磁片，請指定dd 選項。舉例來說，如要使用開機片開機，並且使用驅動程式磁片，請在boot: 提示符號下輸入下列指令：

```
linux ks=floppy dd
```

### 開機光碟

假如kickstart 檔案是放置在開機光碟上 (如 7.8.2 節 所述)，請將該光碟放入並啟動系統，然後在boot: 提示符號下輸入下列指令 (這裡的ks.cfg 就是kickstart 檔案的名稱)：

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

其他用來開始kickstart 安裝的選項如下所示：



```
ks=nfs:<server>:/<path>
```

安裝程式將會在NFS 伺服器<server> 中的<path> 路徑下尋找kickstart 檔案。安裝程式將使用DHCP 來設定乙太網路卡，舉例來說，假如您的NFS 伺服器為server.example.com，而kickstart 檔案是在NFS 共享資源的/mydir/ks.cfg，正確的開機指令將是ks=nfs:server.example.com:/mydir/ks.cfg。

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

安裝程式將會在HTTP 伺服器<server> 中的<path> 路徑下尋找kickstart 檔案。安裝程式將使用DHCP 來設定乙太網路卡，舉例來說，假如您的HTTP 伺服器為server.example.com，而kickstart 檔案是在HTTP 目錄/mydir/ks.cfg 中，正確的開機指令將是ks=http://server.example.com/mydir/ks.cfg。

```
ks=floppy
```

安裝程式將會在/dev/fd0 磁片上一個vfat 或ext2 檔案系統中尋找ks.cfg 檔案。

```
ks=floppy:/<path>
```

安裝程式將會在/dev/fd0 磁片上的<path> 路徑下尋找kickstart 檔案。

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

安裝程式將會掛載<device> 上的檔案系統（必須是vfat 或ext2），然後尋找檔案系統中的kickstart 設定檔案<file>（例如ks=hd:sda3:/mydir/ks.cfg）。



#### 請注意

第二個欄位是Red Hat Linux 9 中的語法變更。

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

安裝程式將試著從檔案系統中讀取<file> 檔案（沒有任何掛載的動作）。這通常使用在當kickstart 檔案已經是一個initrd 映像檔時。

```
ks=cdrom:/<path>
```

安裝程式將會在光碟片上尋找kickstart 檔案<path>。

```
ks
```

假如只有使用ks，安裝程式將會使用DHCP 設定系統中的乙太網路卡，系統將使用DHCP 回應中的"bootServer" 當作一部NFS 伺服器以用來讀取kickstart 檔案（預設情況下，這是與DHCP 伺服器相同的），kickstart 檔案的名稱會是以下的其中一種：

- 假如指定DHCP，而且開機檔案以/ 開頭，將會在NFS 伺服器上搜尋這個DHCP 提供的開機檔案。
- 假如指定DHCP，而且開機檔案不是以/ 開頭，將會在NFS 伺服器上的/kickstart 目錄中搜尋這個DHCP 提供的開機檔案。
- 假如DHCP 沒有指定一個開機檔案，安裝程式將會試著讀取/kickstart/1.2.3.4-kickstart 檔案（這裡的1.2.3.4 是用來安裝之機器的數值IP 位址）。

```
ksdevice=<device>
```

安裝程式將會使用網路裝置來連線到網路，例如要使用NFS 伺服器（透過eth1 裝置連線到系統）上之kickstart 檔案來開始一個kickstart 安裝，請在boot: 提示符號下輸入`ks=nfs:<server>:/<path> ksdevice=eth1` 指令。

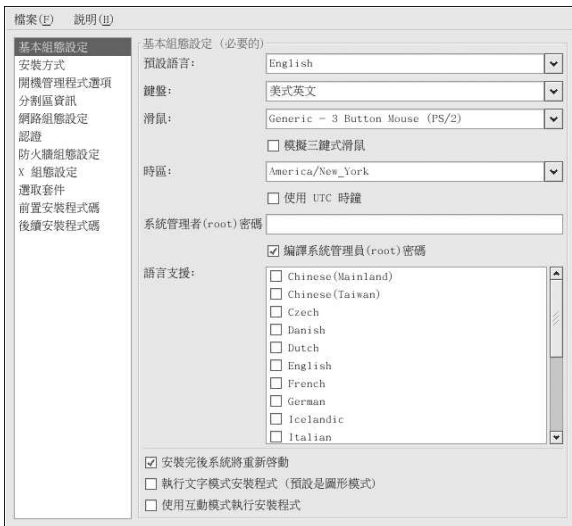
## Kickstart 設定程式

**Kickstart 設定程式** 讓您使用一個圖形使用者介面來建立一個kickstart 檔案，如此您便不用去詳記這個檔案的正確語法。

如要使用**Kickstart 設定程式**，您必須執行X 視窗系統，如要啟動**Kickstart 設定程式**，請選擇面板上的『**主選單按鈕**』=>『**系統工具**』=> **Kickstart**，或是輸入/usr/sbin/redhat-config-kickstart 指令。

當您正在建立kickstart 檔案時，您可以在任何時間選擇『**檔案**』=>『**預覽**』來檢視您目前的選項。

### 8.1. 基本組態設定



圖形8-1. 基本組態設定

從『**預設語言**』的選單中選擇在安裝過程中要使用的語言，並且當作完成安裝後系統的預設語言。

從『**鍵盤**』的選單中選擇系統鍵盤的種類。

從『**滑鼠**』的選單中選擇系統上使用的滑鼠。如果選擇**No Mouse**，將不會設定任何滑鼠；假如選擇**Probe for Mouse**，安裝程式將會試著自動偵測滑鼠的種類。這個偵測可用在大部分當代的滑鼠裝置。

假如系統上有一個兩鍵式的滑鼠，您可以選擇『**模擬三鍵式滑鼠**』的選項來模擬三鍵式的滑鼠功能。假如有選擇這個選項，同時按下滑鼠的左右兩鍵將會被當作中間按鍵來使用。

在『**時區**』的選單，您可以為系統選擇要使用的時區。如要設定系統使用UTC，請選擇『**使用UTC 時鐘**』。

請在『**Root 密碼**』的文字欄位輸入系統上的root 密碼，如要儲存密碼為一個檔案中的加密密碼，請選擇『**編譯root 密碼**』，假如有選擇加密選項的話，當檔案儲存時，您所輸入的純文字密碼將會被加密然後寫入到kickstart 檔案中，請勿輸入一個加密過的密碼，然後再選擇為其加密。

如要安裝『**語言**』選單中選取之外的語言，請在『**語言支援**』的清單中選取它們，安裝完成後將會使用『**語言**』選單中選取的語言當作預設語言；然而您仍然可以在安裝完成後使用**語言設定工具**(redhat-config-language) 來更改預設的語言。

選擇『**安裝完後系統將重新啟動**』選項，將會使得系統在安裝完後自動重新開機。

Kickstart 安裝是預設以圖形模式進行安裝的，如要強制覆寫這個預設值，而使用文字模式安裝方式，請選擇『**執行文字模式安裝程式**』的選項。

您可以以互動模式來進行kickstart 的安裝，也就是說安裝程式將使用所有在kickstart 檔案中預先設定好的選項，不過在繼續到下一個畫面前請您檢視每一個畫面的選項，如要繼續到下一個畫面，請在您確認設定或在繼續之前更改它們後，點選**下一步** 按鈕。如要選擇這種類型的安裝方式，請選取『**使用互動模式執行安裝程式**』選項。

## 8.2. 安裝方式



圖形8-2. 安裝方式

『**安裝方式**』的畫面讓您選擇是否要執行一個全新的安裝或系統升級，假如您選擇要做系統升級，『**分割區資訊**』與『**選取套件**』的選項將會失效，kickstart 的升級安裝並不支援它們。

您也可以在這個畫面選擇要執行的kickstart 安裝類型，可以選擇下列的選項：

- **光碟機** — 選擇這個選項以從Red Hat Linux 的光碟片來安裝Red Hat Linux 。
- **NFS** — 選擇這個選項以從一個NFS 的共享目錄來安裝Red Hat Linux ，將會出現可讓您輸入NFS 伺服器以及NFS 目錄的兩個文字欄位。請在NFS 伺服器的欄位輸入一個有效的網域名稱或IP 位址，至於NFS 目錄，請輸入含有安裝目錄中RedHat 目錄的NFS 目錄名稱。舉例來說，假如您的NFS 伺

伺服器含有 `/mirrors/redhat/i386/RedHat/` 目錄，請輸入 `/mirrors/redhat/i386/` 當作 NFS 的目錄。

- **FTP** — 選擇這個選項以從一部 FTP 伺服器來安裝 Red Hat Linux，將會出現可讓您輸入 FTP 伺服器以及 FTP 目錄的兩個文字欄位。請在 FTP 伺服器的欄位輸入一個有效的網域名稱或 IP 位址，至於 FTP 目錄，請輸入含有安裝目錄中 RedHat 目錄的 FTP 目錄名稱。舉例來說，假如您的 FTP 伺服器含有 `/mirrors/redhat/i386/RedHat/` 目錄，請輸入 `/mirrors/redhat/i386/` 當作 FTP 的目錄。假如該 FTP 伺服器需要一組使用者名稱與密碼，請在此指定它們。
- **HTTP** — 選擇這個選項以從一部 HTTP 伺服器來安裝 Red Hat Linux，將會出現可讓您輸入 HTTP 伺服器以及 HTTP 目錄的兩個文字欄位。請在 HTTP 伺服器的欄位輸入一個有效的網域名稱或 IP 位址，至於 HTTP 目錄，請輸入含有安裝目錄中 RedHat 目錄的 HTTP 目錄名稱。舉例來說，假如您的 HTTP 伺服器含有 `/mirrors/redhat/i386/RedHat/` 目錄，請輸入 `/mirrors/redhat/i386/` 當作 HTTP 的目錄。
- **硬碟** — 選擇這個選項以從您的硬碟來安裝 Red Hat Linux，將會出現可讓您輸入硬碟分割區與硬碟目錄的兩個文字欄位。硬碟安裝方式需要使用 ISO（或光碟）映像檔，請在開始安裝前記得要檢驗 ISO 映像檔是完整的。如要做檢驗，您可以使用 `md5sum` 程式以及在 *Red Hat Linux* 安裝手冊中所討論的 `linux mediacheck` 開機選項。請在『**硬碟分割區**』的欄位輸入含有 ISO 映像檔的硬碟分割區（例如 `/dev/hda1`），請在『**硬碟目錄**』欄位輸入含有 ISO 映像檔的目錄名稱。

### 8.3. 開機管理程式選項

檔案 (F) 說明 (H)

基本組態設定  
安裝方式  
**開機管理程式選項**  
分割區資訊  
網路組態設定  
認證  
防火牆組態設定  
X 組態設定  
選取套件  
前置安裝程式碼  
後續安裝程式碼

開機管理程式選項 (必要的)

安裝新的開機管理程式  
 不安裝開機管理程式  
 升級目前的開機管理程式

使用 GRUB 當作開機管理程式  
 使用 LILO 當作開機管理程式

GRUB 選項:

使用 GRUB 密碼:

編譯 GRUB 密碼

安裝開機管理程式在 MBR  
 安裝開機管理程式在開機磁區的第一扇區

核心參數:

圖形8-3. 開機管理程式選項

您可以選擇要安裝 GRUB 或 LILO 當作開機管理程式，假如您不想要安裝一個開機管理程式，請選擇『**不安裝開機管理程式**』，假如您選擇不安裝開機管理程式，請記得要建立一個開機片，或者您確定有其他用來啟動您系統的方式（例如其他協力廠商提供的開機管理程式）。

假如您選擇要安裝開機管理程式，您必須選擇要安裝那一個開機管理程式（GRUB 或 LILO），以及要在那裡安裝開機管理程式（MBR 或 `/boot` 分割區的第一個磁區）。假如您打算使用它當作您的開機管

理程式，請安裝開機管理程式在 MBR；假如您正在使用另一個開機管理程式，請安裝 GRUB 或 LILO 到 /boot 分割區的第一個磁區，然後設定其他的開機管理程式來啟動 Red Hat Linux。

當系統開機時如要傳送任何特殊參數到核心，請輸入到『**核心參數**』的欄位。舉例來說，假如您有一個 IDE 的光碟燒錄機，您可以輸入 `hdd=ide-scsi` 當作核心參數 (`hdd` 是該光碟燒錄機裝置)，用來告訴核心使用 SCSI 模擬驅動程式以在使用 `cdrecord` 之前將之載入。

假如您選擇 GRUB 當作開機管理程式，您可以藉由設定一個 GRUB 密碼來保護您的系統，請在『**使用 GRUB 密碼**』的文字欄位輸入一個密碼。如要在檔案中儲存該密碼為一個加密過的密碼，請選擇『**編譯 GRUB 密碼**』。假如有選擇加密選項的話，當檔案儲存時，您所輸入的純文字密碼將會被加密然後寫入到 kickstart 檔案中，請勿輸入一個加密過的密碼，然後再選擇為其加密。

假如您選擇 LILO 當作開機管理程式，請選擇是否要使用線性模式，以及您是否想強制使用 lba32 模式。

假如在『**安裝方式**』的頁面有選擇『**升級目前的安裝**』的選項，請選擇『**升級目前的開機管理程式**』來升級既有的開機管理程式設定，並保留舊有的紀錄項。

## 8.4. 分割區資訊

圖形8-4. 分割區資訊

請選擇是否要清除 MBR，您也可以選擇要移除所有既有的分割區、移除既有的 Linux 分割區，或保留既有的分割區。

您可以初始化磁碟標籤為系統架構的預設值（例如用於 x86 的 `msdos`，以及用於 Itanium 的 `gpt`）。假如您要安裝到一個全新的硬碟上，請選擇『**初始化磁碟標籤**』。

### 8.4.1. 建立分割區

如要建立一個分割區，請點選 **新增** 按鈕，『**分割區選項**』的視窗將會出現在圖形8-5。請為新的分割區選取掛載點、檔案系統類型以及分割區大小。除此之外，您也可以選擇下列的選項：

- 在『**其他的磁區大小選項**』部份，您可以選擇使分割區為一個固定大小、填滿至選擇的大小或填滿硬碟上可用的空間。假如您選擇swap 當作檔案系統類型，您可以選擇讓安裝程式以建議的大小（而不是由您指定）來建立swap 分割區。
- 強制分割區建立為主要分割區。
- 建立分割區在一個特定的硬碟。例如要在第一個IDE 硬碟上(/dev/hda)建立分割區，請指定**hda** 為磁碟機，請勿將/dev 加在磁碟名稱中。
- 使用一個既有的分割區，例如要建立分割區在第一個IDE 硬碟的第一個分割區(/dev/hda1)，請指定分割區為**hda1**，請勿將/dev 加在分割區名稱中。
- 格式化分割區為選取的檔案系統類型。

掛載點: [ ]

檔案系統類型: ext3

大小 (MB): 1

其他的磁區大小選項

固定大小

填滿最大值到 (MB): [ ]

填滿磁碟上所有的剩餘空間

使用建議的 swap 大小

強制成為主要分割區 (asprimary)

在特定磁碟機上建立分割區 (ondisk)

磁碟機: [ ] (例如: hda 或 sda)

使用現有的分割區 (onpart)

分割區: [ ] (例如: hda1 或 sda9)

格式化分割區

[X] 取消 (C) [Y] 確定 (O)

圖形8-5. 建立分割區

如要編輯一個既有的分割區，請從清單中選取該分割區，再點選**編輯**的按鈕，會出現當您選擇要新增一個分割區時相同的『**分割區選項**』視窗（如圖形8-5 所示），不過它含有選取之分割區的數值。請修改分割區的選項，再點選**確定**。

如要刪除一個既有的分割區，請從清單中選取該分割區，再點選**刪除**的按鈕。

#### 8.4.1.1. 建立軟體RAID 分割區

請參閱第3章 以取得關於RAID 以及不同RAID 模式的資訊，在此您可以設定RAID 0, 1 與5 等模式。

如要建立一個軟體RAID 分割區，請使用下列步驟：

1. 點選**RAID** 按鈕。
2. 選擇『**建立一個軟體RAID 分割區**』。
3. 如以上所述來設定分割區，不過得選擇『**軟體RAID**』當作檔案系統類型，而且您必須指定要用來建立分割區的硬碟，或指定一個既有的分割區來使用。

掛載點: [ ]

檔案系統類型: 軟體 RAID

大小 (MB): 2048

其他的磁碟大小選項

固定大小

填滿最大值到 (MB): [ 1 ]

填滿磁碟上所有的剩餘空間

使用建議的 swap 大小

強制成為主要分割區 (asprimary)

在特定磁碟機上建立分割區 (ondisk)

磁碟機: [ sda ] (例如: hda 或 sdc)

使用現有的分割區 (onpart)

分割區: [ ] (例如: hda1 或 sdc3)

格式化分割區

[ 取消 ] [ 確定 ]

圖形8-6. 建立一個軟體RAID 分割區

重複這些步驟來建立您的RAID 設定所需的所有分割區，並不是所有的分割區都一定要設定為RAID 分割區。

在建立完形成一個RAID 裝置所需的所有分割區之後，請遵照這些步驟：

1. 點選**RAID** 按鈕。
2. 選擇『**建立一個RAID 裝置**』。
3. 再來為軟體RAID 裝置選取一個掛載點、檔案系統類型、RAID 裝置名稱、RAID 等級、RAID 成員以及備援裝置的數量，還有是否要格式化RAID 裝置。

掛載點: [ /home ]

檔案系統類型: [ ext3 ]

RAID 裝置: [ md0 ]

RAID 等級: [ 0 ]

Raid 的成員

- raid.01
- raid.02

spares 的數量: [ 1 ]

格式化 RAID 裝置

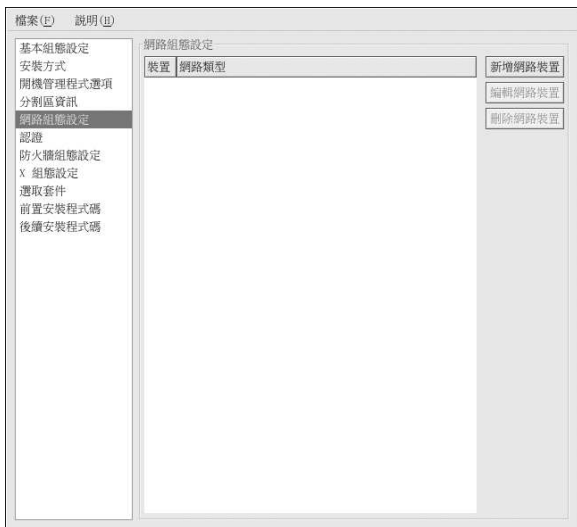
[ 取消 ] [ 確定 ]

圖形8-7. 建立一個軟體RAID 裝置

4. 點選**確定** 以增加該裝置到清單中。



## 8.5. 網路組態設定



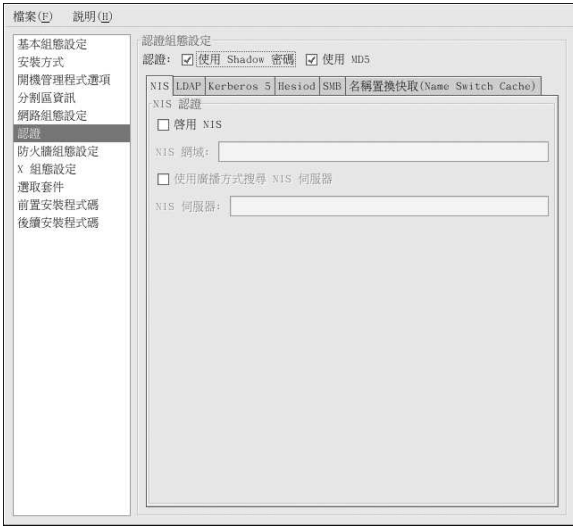
圖形8-8. 網路組態設定

假如要使用kickstart 來安裝的系統沒有乙太網路卡，請勿在『網路組態設定』頁面設定一個。

只當您選擇一種網路為主的安裝方式（NFS, FTP 或HTTP），才需要設定網路連線。不過您總是可以在安裝完成後，使用**網路管理工具**(redhat-config-network)來設定您的網路連線。請參考第12章以取得更詳細資訊。

至於系統上的每一個乙太網路卡，請點選**新增網路裝置**，然後選擇網路裝置以及該裝置所屬的網路類型。請為第一個乙太網路卡選擇**eth0** 當作網路裝置（第二個乙太網路卡為**eth1** 等等依此類推。）

## 8.6. 認證



圖形8-9. 認證

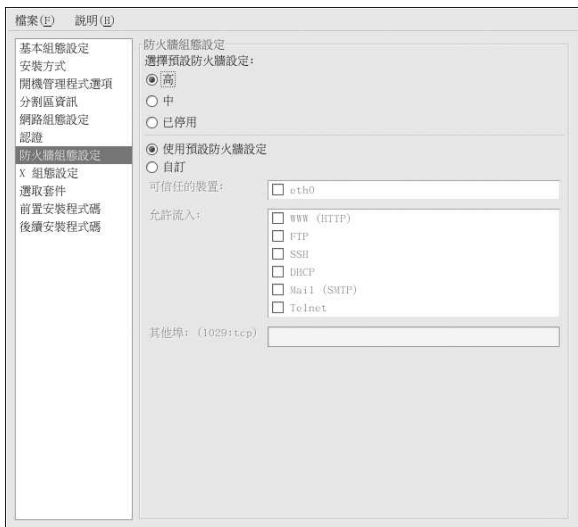
在『認證』的部份選擇是否在使用者的密碼上使用shadow 密碼以及MD5 編碼，這些選項是強烈建議且預設選取的。

『認證組態設定』中的選項讓您可以設定下列的網路認證方法：

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- 名稱置換快取

這些方式並非預設啟用的，如要啟用一個或以上的這些方法，請點選適當的標籤頁，並點選旁邊的選取盒以『啟用』，並且為認證方式輸入適當的資訊。

## 8.7. 防火牆組態設定



圖形8-10. 防火牆組態設定

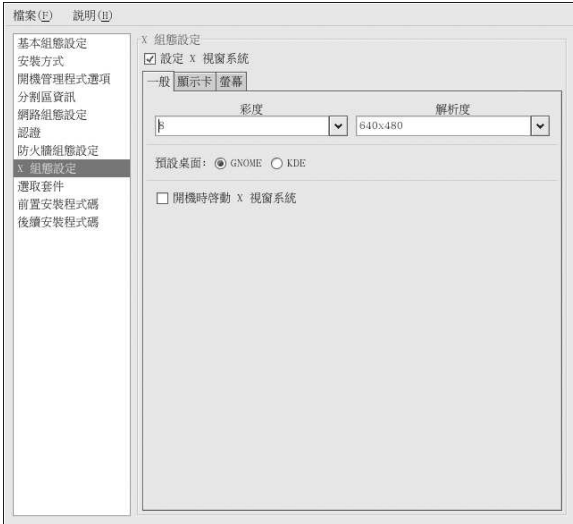
『**防火牆組態設定**』的視窗與 Red Hat Linux 安裝程式中的畫面以及**安全等級設定**工具的畫面一樣，並且含有相同的功能性。請在『**高**』、『**中**』以及『**已停用**』的安全性等級中做選擇，參考 13.1 節以取得關於這些安全性等級的詳細資訊。

## 8.8. X 組態設定

假如您要安裝 X 視窗系統，您可以在 kickstart 安裝中來設定它，只要在如圖形8-11 所示的『**X 組態設定**』視窗中選取『**設定 X 視窗系統**』的選項即可。假如沒有選擇這個選項，將會停用 X 組態設定的選項，而且將會寫入 skipx 的選項到 kickstart 檔案中。

### 8.8.1. 一般

設定 X 的第一步是選擇預設的彩度以及解析度，請從相對應的下拉式選單選取它們，請確實指定與系統顯示卡以及螢幕相容的彩度與解析度。



圖形8-11. X 組態設定- 一般

假如您要安裝GNOME 與KDE 桌面，您必須選擇一個預設的桌面環境，假如只要安裝一個桌面，請確定要選取它。當系統安裝完後，使用者可以選擇他們想要的預設桌面。如需關於GNOME 與KDE 的更多資訊，請參考*Red Hat Linux* 安裝手冊 與*Red Hat Linux* 使用手冊。

再來請選擇是否要在系統開機時啟動X 視窗系統，這個選項將會啟動系統到含有圖形登入畫面的執行等級5。在系統安裝完後，您可以修改/etc/inittab 設定檔案來更改這個設定。

### 8.8.2. 顯示卡

『偵測顯示卡』的選項是被預設選取的，請接受這個預設值來讓安裝程式於安裝中偵測顯示卡，這個偵測工作可使用在大部分現今的顯示卡。假如有選取這個選項，不過安裝程式卻無法成功偵測顯示卡，安裝程式將會停頓在顯示卡的設定畫面。如要使安裝過程繼續，請從清單中選取您的顯示卡，然後點選下一步。

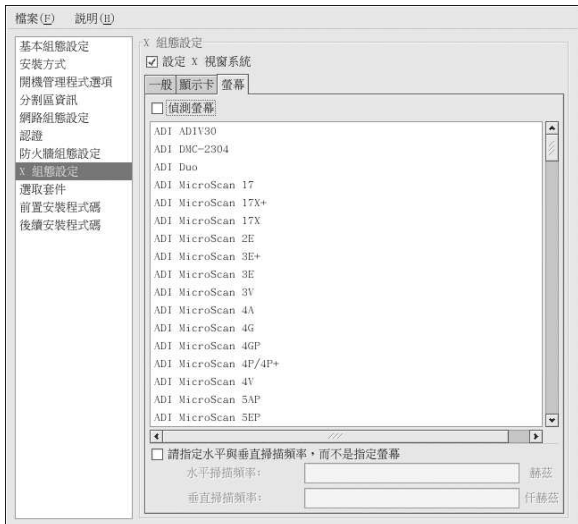
或者您可以從如圖形8-12 所示的『顯示卡』標籤頁中的清單選取您的顯示卡。再從『顯示卡記憶體』的下拉式選單中指定所選取之顯示卡上的記憶體容量，安裝程式將使用這些數值來設定X 視窗系統。



圖形8-12. X 組態設定- 顯示卡

### 8.8.3. 螢幕

在設定好顯示卡後，請點選如圖形8-13 所示的『螢幕』標籤頁。

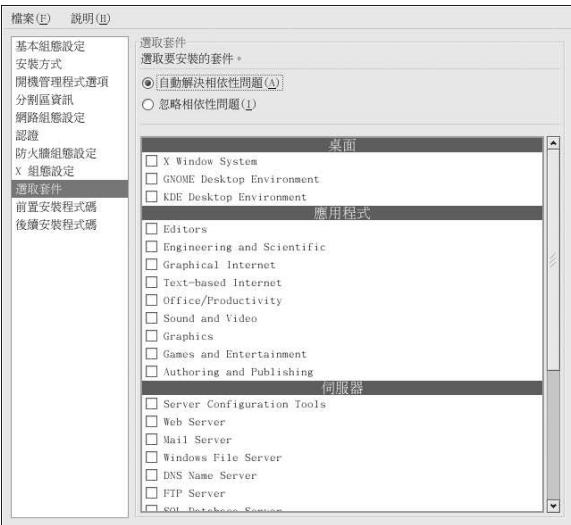


圖形8-13. X 組態設定- 螢幕

『偵測螢幕』的選項是被預設選取的，請接受這個預設值來讓安裝程式於安裝中偵測螢幕，這個偵測工作可使用在大部分現今的螢幕。假如有選取這個選項，不過安裝程式卻無法成功偵測螢幕，安裝程式將會停頓在螢幕的設定畫面。如要使安裝過程繼續，請從清單中選取您的螢幕，然後點選下一步。

或者您可以從清單中選取您的螢幕，您也可以選取『請指定水平與垂直掃描頻率，而不是指定螢幕』選項來指定水平與垂直掃描頻率，而不用選取一個特定的螢幕。當系統的螢幕沒有出現在清單中時，您可以使用這個選項。請注意當啟用這個選項時，螢幕的清單將會失效。

## 8.9. 選取套件



圖形8-14. 選取套件

『選取套件』視窗讓您選擇要安裝的套件群組。

在此也有自動解決或忽略套件相依性問題的選項。

目前，**Kickstart 設定程式**並不允許您選擇個別的套件，如要安裝個別的套件，請在儲存kickstart 檔案後，修改`%packages`的部份，請參考 7.5 節 以取得詳細資訊。

## 8.10. 前置安裝程式碼



圖形8-15. 前置安裝程式碼

在解析kickstart 檔案之後與開始安裝之前，您可以增加要在系統上立即執行的指令。假如您在kickstart 檔案中有設定網路資訊，在處理這個部份之前便已經啟動網路了。如要加入一個前置安裝的程式碼，請在文字區域輸入。

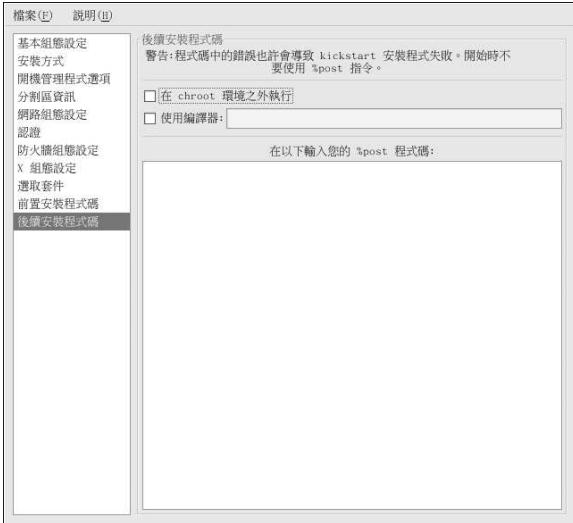
如要指定用來執行程式碼的一個程式語言，請選取『使用編譯器』的選項，然後在旁邊的文字欄中輸入編譯器的名稱。舉例來說，可以指定`/usr/bin/python2.2`來執行Python 程式碼。這個選項與您在kickstart 檔案中使用`%pre --interpreter /usr/bin/python2.2`是相同的。



警告

請勿加入`%pre` 指令，將會自動幫您加入。

## 8.11. 後續安裝程式碼



圖形8-16. 後續安裝程式碼

您也可以增加要在安裝完成後於系統上執行的指令，假如您在kickstart 檔案中有設定網路資訊，此時已經啟動網路了，而程式碼也可以含有存取網路資源的指令。如要加入後續安裝的程式碼，請在文字區域輸入。



### 警示

請勿加入`%post` 指令，將會自動幫您加入。

舉例來說，如要為新安裝的系統變更今日訊息，請將以下指令加入到`%post` 部份：

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



### 建議

可在 [7.7.1 節](#) 找到更多的例子。

### 8.11.1. Chroot 環境

如要在chroot 環境之外執行後續安裝的程式碼，請點選『**後續安裝程式碼**』視窗頂端該選項旁的選取盒。這等於您在`%post` 部份使用`--nochroot` 的選項。



在chroot 環境之外，如要在後續安裝的程式碼部份對新安裝的檔案系統做任何的變更，請記得在目錄名稱前加上/mnt/sysimage/。

舉例來說，假如您選擇『**在chroot 環境之外執行**』的選項，以上的例子必須變更為如下：

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

### 8.11.2. 使用編譯器

如要指定用來執行程式碼的一個程式語言，請選取『**使用編譯器**』的選項，然後在旁邊的文字欄中輸入編譯器的名稱。舉例來說，可以指定**usr/bin/python2.2**來執行Python 程式碼。這個選項與您在kickstart 檔案中使用`%post --interpreter /usr/bin/python2.2`是相同的。

## 8.12. 儲存檔案

在您完成您的kickstart 選項後，如要檢視kickstart 檔案的內容，請選取程式選單上的『**檔案**』=>『**預覽**』。



圖形8-17. 預覽

如要儲存kickstart 檔案，請點選預覽視窗上的**儲存到檔案**的按鈕，或選擇『**檔案**』=>『**儲存檔案**』，或按下[Ctrl]-[S]。會出現一個對話窗，讓您選擇在何處儲存這個檔案。

儲存檔案後，請參考 7.10 節 以取得關於如何啟動kickstart 安裝的資訊。



## 基本的系統回復

當問題發生時，總是會有辦法解決。然而，這些方法需要您對系統有相當的了解。這個章節將描述如何開機進入救援模式、單一使用者模式以及緊急模式，在其中您可以使用您的知識來修復系統。

### 9.1. 一般問題

因為下列的原因，您也許需要開機進入這些救援模式的其中之一：

- 您無法正常開機進入Red Hat Linux（執行等級3或5）。
- 您有硬體或軟體的問題，而您想要從您系統的硬碟取出一些重要的檔案。
- 您忘記您的root密碼。

#### 9.1.1. 無法開機進入Red Hat Linux

這個問題通常是由於在您安裝Red Hat Linux系統後，安裝另一個作業系統所造成的。許多其他的作業系統假定您的電腦上並沒有任何其他的作業系統，它們將覆寫原本含有GRUB或LILO開機管理程式的主開機紀錄區(MBR)，假如開機管理程式被覆寫了，除非您可以進入救援模式並重新設定開機管理程式，否則您將無法開機進入Red Hat Linux。

另一個可能性是安裝完後當您使用磁碟分割工具來重新調整一個分割區或從剩餘空間建立一個新的分割區，而且更改了分割區的順序，假如/分割區的號碼更改了，開機管理程式將無法找到它，以掛載該分割區。如要修復這個問題，請開機進入救援模式，並修改/boot/grub/grub.conf（假如您是使用GRUB）或/etc/lilo.conf（假如您是使用LILO）。您也必須在每次修改LILO設定檔案後，執行/sbin/lilo指令。

#### 9.1.2. 硬體/軟體問題

這個類別包括相當廣泛的不同狀況，其中包括了硬碟發生錯誤以及在開機管理程式設定檔案中指定一個無效的根目錄(root)裝置這兩個例子。假如都不屬於這兩種情況，您也許無法重新開機以進入Red Hat Linux。然而假如您開機進入其中一種系統回復模式，您也許可以解決這個問題或者至少複製出重要的檔案。

#### 9.1.3. Root 密碼

假如您忘記您的root密碼該如何？如要重設它為另一個密碼，請開機進入救援模式或單一使用者模式，然後使用passwd指令來重設root密碼。

### 9.2. 開機進入救援模式

救援模式提供了從磁片、光碟片或某些其他的開機方式（非從系統的硬碟），開機進入一個小型的Red Hat Linux環境。

如名稱所示，救援模式是提供來援助您的困難，在正常的操作下，您的Red Hat Linux系統使用在系統硬碟上的檔案來做所有的事情—執行程式、儲存檔案等等。

然而在有些情況下，您卻無法使Red Hat Linux完好地運作以使你從系統的硬碟中存取檔案。藉由使用救援模式，即使您無法真正從您的硬碟執行Red Hat Linux，您仍然可以存取在您系統硬碟上的檔案。

如要開機進入救援模式，您必須可以使用下列的其中一種方法啟動系統：

- 從一片安裝開機磁片（由bootdisk.img 映像檔所建立）啟動系統。<sup>1</sup>
- 從安裝的開機光碟啟動系統。<sup>2</sup>
- 使用Red Hat Linux 第一片光碟啟動系統。

當您使用以上的其中一種方法開機後，請在安裝的開機提示符號輸入以下指令：

```
linux rescue
```

您將會被提示詢問一些基本的問題，包括要使用那一種語言。也會提示您選擇放置一個有效救援映像檔的位置，請選擇『**本機光碟機**』、『**硬碟**』、『**NFS 映像檔**』、『**FTP**』或『**HTTP**』。所選取的位置必須包含一個有效的安裝目錄，而且該安裝目錄必須與您所開機之Red Hat Linux 第一片光碟含有相同的Red Hat Linux 版本。假如您使用一片開機光碟或磁碟片來啟動救援模式，安裝目錄必須來自與用來建立該媒體相同的目錄。如需更多關於如何設定在硬碟、NFS 伺服器、FTP 伺服器或HTTP 伺服器中安裝目錄的更多資訊，請參考Red Hat Linux 安裝手冊。

假如您選取一個不需要網路連線的救援映像檔，您仍會被訊問是否要建立一個網路連線。假如您需要備份檔案到另一部電腦會從一個共享的網路位置安裝某些RPM 套件時，網路連線將會很有幫助。

您將會看到下列的訊息：

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

假如您選取**繼續**，它將會試著掛載您的檔案系統到/mnt/sysimage 目錄下，假如無法掛載該分割區，系統將會提示您。假如您選取**僅能讀取**，系統將會試著以僅能讀取的模式掛載檔案系統到/mnt/sysimage 目錄下。假如您選取**略過**，您的檔案系統將不會被掛載，假如您認為您的檔案系統已經毀損了，請選擇**略過**。

當您進入救援模式後，在虛擬主控台1 與2 會出現一個提示符號（使用[Ctrl]-[Alt]-[F1] 按鍵組合來進入虛擬主控台1，而使用[Ctrl]-[Alt]-[F2] 來進入虛擬主控台2）：

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

假如您選擇**繼續** 來自動掛載您的分割區，而且成功掛載，您即會進入單一使用者模式。

即使您的檔案系統已經被掛載了，救援模式中的預設根目錄分割區只是暫時的根目錄分割區，而不是正常使用者模式（執行等級3 或5）檔案系統所使用的根目錄分割區。假如您選擇要掛載您的檔案系統，而且掛載順利，您可以更改救援模式環境的根目錄分割區為您檔案系統的根目錄分割區，請使用下列指令：

```
chroot /mnt/sysimage
```

假如您需要執行例如rpm 指令時（需要您的根目錄分割區掛載為/），這個方法將會很有用。如要離開chroot 的環境，請輸入exit，您則會回到提示符號。

1. 如要建立一片安裝開機磁片，請放入一個空白的軟碟片，並使用dd if=bootdisk.img of=/dev/fd0 指令來建立Red Hat Linux 第一片光碟中images/bootdisk.img 映像檔的開機片。
2. 如要建立安裝的開機光碟，請參閱Red Hat Linux 安裝手冊 中的指示。

假如您選擇略過，您仍然可以在救援模式中試著手動掛載分割區，您只要建立一個例如`/foo`的目錄，然後輸入以下指令：

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

在以上的指令中，`/foo`是您剛建立的目錄，而`/dev/hda5`為您想要掛載的分割區。假如該分割區類型為`ext2`，請以`ext2`取代`ext3`。

假如您不知道分割區的名稱，請使用下列指令來將它們列出：

```
fdisk -l
```

在提示符號下，您可以執行許多有用的指令，如

- `list-harddrives`：以列出系統中的所有硬碟
- `ssh,scp` 與 `ping`：測試網路是否已啟動
- `dump` 與 `restore`：適用於擁有磁帶機的使用者
- `parted` 與 `fdisk`：用來管理分割區
- `rpm`：用來安裝或升級軟體
- `joe`：用來編輯設定檔案（假如您試著啟動其他受歡迎的編輯器，例如`emacs`、`pico` 或 `vi`，將會啟動 `joe` 編輯器。）

### 9.3. 開機進入單一使用者模式

單一使用者模式的其中一個好處是您不需要一個開機磁片或光碟片，然而您卻無法掛載檔案系統為僅能讀取或根本不掛載它們。

在單一使用者模式，您的電腦為開機進入執行等級1，您的檔案系統已經被掛載，不過您的網路尚未啟動，您可以使用一個系統維護的`shell`。單一使用者模式不像救援模式，它會試著自動掛載檔案系統，假如您的檔案系統無法被成功掛載，請勿使用單一使用者模式。而且假如系統上的執行等級1的設定已經毀損，您也無法使用單一使用者模式。

假如您的系統可以開機，不過當完成開機時卻不允許您登入，請試著使用單一使用者模式。

假如您是使用GRUB，請使用下列的步驟來開機進入單一使用者模式：

1. 假如您有設定一個GRUB密碼，請輸入`p`，然後再輸入密碼。
2. 選取您想要開機的Red Hat Linux核心版本，再輸入`e`代表編輯。您將會看到您所選取之標題在設定檔案中所含的一系列項目。
3. 請選取以`kernel`開頭的那行，再輸入`e`以編輯該行。
4. 在該行的最後輸入另一個字`single`（按下[空白鍵]然後再輸入`single`），再按下[Enter]以離開編輯模式。
5. 回到GRUB畫面後，輸入`b`以開機進入單一使用者模式。

假如您是使用LILO，請在LILO開機提示符號下（假如您是使用圖形的LILO，您必須先按下[Ctrl]-[x]以離開圖形畫面，然後進入`boot:`提示符號）輸入：

```
linux single
```

#### 9.4. 開機進入緊急模式

在緊急模式中，您是開機進入盡可能最小的環境中。根目錄檔案系統將會被掛載為僅能讀取，而且將不會做任何的設定。比起單一使用者模式，緊急模式最主要的優點是並不載入init 檔案。因此當init 檔案毀損或無法使用時，您仍然可以掛載檔案系統以回復重新安裝階段中遺失的資料。

如要開機進入緊急模式，請使用如 9.3 節 所示開機進入單一使用者模式的相同方法，僅有一個不同處，就是以關鍵字**emergency** 取代關鍵字**single**。

請先閱讀第3章 以了解RAID 的基本觀念、硬體與軟體RAID 的相異處，以及RAID level 0, 1 與5 等模式的相異處。

在Red Hat Linux 的圖形安裝程式或在kickstart 的安裝階段中，可以配置軟體RAID 的設定。這個章節將討論如何在安裝過程中使用**Disk Druid** 介面來配置軟體RAID 設定。

在您建立一個RAID 裝置前，您必須先建立RAID 分割區，請遵照下列的一步步指示：

1. 在『**磁碟分割設定**』的畫面，選擇使用**Disk Druid** 分割磁碟。
2. 在**Disk Druid** 中點選**新增** 來建立一個新的分割區。
3. 在此您將無法輸入一個掛載點（在您建立您的RAID 裝置後，您才可以輸入掛載點）。
4. 請從如圖形10-1 所示的『**檔案系統類型**』下拉式選單中選擇『**軟體RAID**』。



圖形10-1. 建立一個新的RAID 分割區

5. 在『**可使用的磁碟機**』中選擇要用來建立RAID 的磁碟機。假如您有多個磁碟機，在此將會選取所有的磁碟機，而您則必須取消選取不放置 RAID 陣列於其上的磁碟機。
6. 請輸入該分割區的大小。
7. 選擇『**固定大小**』以設定分割區為指定的大小；選擇『**填滿分割區直到(MB)**』，再以MB 輸入大小以給予分割區大小的一個範圍，或選擇『**填滿分割區至可獲得的最大值**』以使它填滿硬碟上所有可用的空間。假如您設定一個以上的分割區為非固定大小的，它們將會分享硬碟上可使用的剩餘空間。
8. 假如您想要該分割區成為一個主分割區，請選擇『**強制成為主要分割區**』。
9. 假如您想要安裝程式在格式化前檢查硬碟上的損壞磁區，請選擇『**格式化時順便檢查是否有損壞的磁區**』。
10. 點選**確定** 以回到主畫面。

重複以上步驟來建立您的RAID 設定所需的所有分割區，請注意所有的分割區並不一定要成為RAID 分割區，例如您可以只設定 /home 分割區為一個軟體RAID 裝置。

在您建立所有的『**軟體RAID**』分割區後，請遵照以下步驟：

1. 在**Disk Druid** 的主要磁碟分割畫面中（請看圖形10-3），選取**RAID** 按鈕。
2. 再來將會出現圖形10-2，在此您可以建立一個RAID 裝置。



圖形10-2. 建立一個RAID 裝置

3. 輸入一個掛載點。
4. 為分割區選擇檔案系統類型。
5. 為RAID 裝置選擇例如**md0**的裝置名稱。
6. 選擇您要設定RAID 模式，您的選擇有**RAID 0**、**RAID 1** 以及**RAID 5**。



#### 請注意

假如您要建立一個/boot 的RAID 分割區，您必定要選擇RAID level 1，而且它必須使用前面的兩個磁碟機的其中一個（第一個IDE 或第二個SCSI）。假如您沒有設定一個/boot 的RAID 分割區，而您要建立一個/ 的RAID 分割區，此時必須設定為RAID level 1 而且它必須使用前面的兩個磁碟機的其中一個（第一個IDE 或第二個SCSI）。

7. 您剛才建立的RAID 分割區會出現在『**RAID 成員**』清單中，從這些分割區中選擇要用來建立RAID 裝置的分割區。
8. 假如設定為RAID 1 或RAID 5，請指定備援(spare)分割區的數量。當一個軟體RAID 分割區失敗時，將會自動使用備援分割區來當作一個替代品。對於您想要指定的每一個備援裝置，您必須要建立一個額外的軟體RAID 分割區（在當作RAID 裝置的分割區之外）。在上一個步驟，請選擇RAID 裝置的分割區以及用作備援裝置的分割區。
9. 在點選**確定**後，RAID 裝置將會出現在如圖形10-3 所示的『**磁碟機摘要**』清單中。在此您便可以繼續您的安裝程序，請參考*Red Hat Linux* 安裝手冊 以得到更進一步的資訊。





圖形10-3. RAID 陣列已建立



可以在Red Hat Linux 的圖形安裝程式與一個kickstart 的安裝中設定LVM，您可以使用來自lvm 套件的工具程式建立您的LVM 設定，不過在這個章節的指示將重點放在Red Hat Linux 安裝程式中使用**Disk Druid** 來完成這項工作。

請先閱讀第4章 以學習關於LVM 的資訊，以下是用來設定LVM 所需的步驟概要：

- 在硬碟中建立『實體磁區』。
- 在實體磁區中建立『磁區群組』。
- 在磁區群組中建立『邏輯磁區』，並指定掛載點給邏輯磁區。



#### 請注意

您只能在GUI 安裝模式編輯LVM 磁區群組，在文字安裝模式，您可以指定掛載點給既有的邏輯磁區。

在Red Hat Linux 安裝過程中，如要建立含有邏輯磁區的一個邏輯磁區群組：

1. 在『磁碟分割設定』畫面，請選擇**使用Disk Druid 分割磁碟**。
2. 選取**新增**。
3. 您將無法指定一個掛載點（在建立好磁區群組後才能指定）。
4. 從『檔案系統類型』的下拉式選單選取『**實體磁區(LVM)**』（如圖形11-1 所示）。



圖形11-1. 建立一個實體磁區

5. 一個實體磁區必須侷限在一個磁碟機上，在『**可使用的磁碟機**』欄位中選取要用來建立實體磁區的磁碟機。假如您有多個磁碟機，所有的磁碟機都會被選取，而您則只能選取一個。
6. 再輸入該實體磁區的大小。
7. 選擇『**固定大小**』以使得實體磁區為指定的大小，選擇『**填滿至最大空間(MB)**』並且輸入以MB 表示的大小以給予實體磁區一個空間範圍，或者是選擇『**填滿至最大的可獲得空間**』，使得該磁區填滿硬碟上所有可用的空間。假如您設定一個以上可增大的磁區，它們將會分享硬碟上可使用的剩餘空間。
8. 假如您要該分割區成為主分割區，請選擇『**強制成為主要分割區**』。

9. 假如您希望安裝程式在格式化前幫您檢查硬碟上是否有損壞的磁區，請選擇『**格式化時順便檢查是否有損壞的磁區**』。

10. 點選**確定**以回到主畫面。

重複這些步驟來為您的LVM設定建立您所需的實體磁區。舉例來說，假如您想要邏輯磁區群組跨越一個以上的磁碟，您必須在每一個磁碟上建立一個以上的實體磁區。



#### 警告

/boot 分割區不可以在磁區群組中，因為開機管理程式將無法讀取到它。假如您想要使您的根目錄在一個邏輯磁區上，您將必須建立一個分開的/boot 分割區（也不可以是磁區群組的一員）。

在建立好所有的實體磁區後，請遵照以下這些指示：

1. 點選**LVM** 按鈕以收集實體磁區到磁區群組中，一個磁區群組基本上是實體磁區的集合，您可以擁有多個邏輯磁區群組，不過一個實體磁區僅能隸屬於一個磁區群組。



#### 請注意

在邏輯磁區群組中有保留給用來儲存系統額外資訊的磁碟空間，實體磁區大小的總和也許不等於磁區群組的大小，然而在此所顯示的邏輯磁區大小是正確的。



圖形11-2. 建立一個LVM裝置

2. 您可以更改『**磁區群組名稱**』。
3. 必須分配『**實體範圍(physical extent)**』的單位在磁區群組中的所有邏輯磁區，預設情況下，實體範圍的單位設定為4MB；因此邏輯磁區的大小必須是可由4MB 整除劃分的。假如您所輸入的大小不是4MB 的倍數，安裝程式將會自動選取最接近其倍數的大小。不建議您改變這個設定。
4. 選取要使用那一個實體磁區當作磁區群組。
5. 建立邏輯磁區並為其指定掛載點（如/home，請記得/boot 掛載點不可以當作一個邏輯磁區，如要增加一個邏輯磁區，請點選『**邏輯磁區**』部份的**新增** 按鈕，將會出現一個類似圖形11-3的對話窗。



圖形11-3. 建立一個邏輯磁區

重複這些步驟來建立您想要的磁區群組。



**建議**

您也許會想要預留一些空間在邏輯磁區群組中，因此您可以在之後擴大邏輯磁區的範圍。



圖形11-4. 已建立邏輯磁區



### III. 網路相關的設定

在解釋完如何設定網路後，這個章節將探討關於網路連線的主題，包括如何允許遠端登入、透過網路共享檔案與目錄以及設定一部網頁伺服器。

#### 內容目錄

12章網路設定 .....	81
13章基本的防火牆設定.....	97
14章控制服務的存取 .....	105
15章OpenSSH.....	111
16章網路檔案系統(NFS).....	117
17章Samba.....	123
18章動態主機設定協定(DHCP).....	131
19章Apache HTTP 伺服器設定 .....	137
20章Apache HTTP 安全伺服器設定.....	151
21章BIND 組態設定 .....	161
22章認證設定 .....	167
23章郵件傳送代理(MTA)的設定 .....	171





為了要與其他電腦連線，電腦需要一個網路的連線。因此作業系統必須能夠辨識一個介面卡（如乙太網路卡、ISDN 數據機或記號環狀網路裝置），並且設定該介面以連線到網路。

可以使用**網路管理工具**來設定下列的網路介面類型：

- 乙太網路
- ISDN
- 數據機
- xDSL
- 記號環狀網路
- CIPE
- 無線網路裝置

如要使用**網路管理工具**，您必須擁有root 權限。如果要啟動這個應用程式，請選擇面板上的『主選單按鈕』=> 『系統設定』=> 『網路』，或是在shell 提示符號（如**XTerm** 或**GNOME 終端機**）下輸入**redhat-config-network** 指令。假如您輸入這個指令，在執行X 的情況下將會啟動圖形化的版本，否則將會顯示文字介面的版本。如要強制執行文字介面的版本，請使用**redhat-config-network-tui** 指令。



圖形12-1. 網路管理工具

假如您較喜歡直接修改設定檔案，請參考**Red Hat Linux** 參考手冊 以取得關於它們的位置與內容。



### 建議

請拜訪**Red Hat** 的硬體相容清單(<http://hardware.redhat.com/hcl/>) 以決定**Red Hat Linux** 是否支援您的硬體裝置。

## 12.1. 概要

如要使用**網路管理工具**來設定網路連線，請執行下列步驟：

1. 新增實體硬體裝置到硬體清單。
2. 新增一個與該實體硬體裝置關聯的網路裝置。
3. 配置主機名稱與DNS設定。
4. 配置無法透過DNS搜尋的任何主機。

這個章節將為每一種網路連線類型討論每一個步驟。

## 12.2. 建立一個乙太網路連線

如要建立一個乙太網路連線，您需要一片網路介面卡(NIC)、一條網路纜線（通常為CAT5的纜線）以及一個網路以用來進行連線。不同的網路環境使用不同的網路速度，因此請確定您的網路卡與您想要連線的網路相容。

如要新增一個乙太網路連線，請遵照以下步驟：

1. 點選『**裝置**』的標籤頁。
2. 再點選工具列上的**新增**按鈕。
3. 從『**裝置類型**』的清單中選取『**乙太網路連線**』，再點選下一步。
4. 假如您已經將該網路介面卡加入到硬體清單中，請從『**乙太網路介面卡**』的清單中選取它，否則請選擇『**其他乙太網路介面卡**』來新增硬體裝置。



### 請注意

安裝程式會偵測有支援的乙太網路裝置，並提示您來設定它們。假如您在安裝過程中有設定任何的乙太網路裝置，它們將會出現在『**硬體**』標籤頁中的硬體清單。

5. 假如您選擇『**其他乙太網路介面卡**』，將會出現『**選取乙太網路介面卡**』的視窗。請選取該乙太網路卡的製造商與型號，並選取裝置名稱。假如這是系統的第一片乙太網路卡，請選擇**eth0**當作裝置名稱，假如是第二片，則選擇**eth1**，依此類推。**網路管理工具**也讓您設定該網路卡的資源，請點選下一步繼續。
6. 在如圖形12-2所示的『**網路設定**』視窗中，請選擇DHCP或一個靜態的IP位址。假如在每次啟動網路時，這個裝置都接收到一個不同的IP位址，請不要指定一個主機名稱。點選下一步繼續。
7. 請在『**建立乙太網路裝置**』的頁面點選**套用**。



圖形12-2. 乙太網路設定

在設定好乙太網路裝置後，它將會出現在如圖形12-3 所示的裝置清單中。



圖形12-3. 乙太網路裝置

請確定要選擇『檔案』=>『儲存』來儲存變更。

在新增完乙太網路裝置後，您可以從裝置清單中選取它，再點選**編輯**的按鈕來修改它的設定。例如，當新增裝置後，它是預設設定在開機時啟動，如果要更改這個設定，請選取要編輯這個裝置，修改『**電腦啟動時啟用裝置**』的數值，再儲存變更。

當新增一個裝置後，該裝置並沒有立即啟用，可由它的『**暫停不用的**』狀態得知。如要啟動這個裝置，請從裝置清單中選取它，再點選**啟用**按鈕，假如系統設定為在電腦開機時即（預設）啟動這個裝置，您便不用再一次地執行這個步驟。

假如您在一一個乙太網路卡設定多個網路裝置，其後的裝置為裝置別名。藉由使用裝置別名，使您可以在一個實體裝置上設定多個虛擬裝置，也就使得一個實體裝置擁有多個IP位址。例如您可以設定一個eth1裝置以及一個eth1:1裝置。需要詳細資訊，請參考 12.13 節。

## 12.3. 建立一個ISDN 連線

ISDN 連線是由一個ISDN 數據機透過由電話公司安裝的特殊電話線所建立的一種網際網路連線。ISDN 連線在歐洲很受歡迎。

如要新增一個ISDN 連線，請遵照以下步驟：

1. 點選『裝置』的標籤頁。
2. 再點選工具列上的**新增** 按鈕。
3. 從『裝置類型』的清單中選取『ISDN 連線』，再點選下一步。
4. 從下拉式選單中選取ISDN 介面卡，然後為該介面卡設定資源以及D 頻道通訊協定。再點選下一步繼續。



圖形12-4. ISDN 設定

5. 假如您的網路服務提供者(ISP)有出現在預先設定的清單，請選取它。否則請輸入關於您ISP 帳號的必要資訊，假如您不知道這些資訊，請聯絡您的ISP，再點選下一步。
6. 在『IP 設定』的視窗中，選擇『封裝模式』以及是否要透過DHCP 取得IP 位址，或者設定為靜態模式。完成後點選下一步。
7. 在『建立撥接連線』的頁面點選套用。

在設定好ISDN 裝置後，它將會以**ISDN** 的裝置類型出現在如圖形12-5 所示的裝置清單中。

請確定要選擇『檔案』=>『儲存』來儲存變更。

在新增完ISDN 裝置後，您可以從裝置清單中選取它，再點選**編輯** 的按鈕來修改它的設定。例如，當新增裝置後，它是預設設定在開機時不啟動。請編輯它的組態設定以修改這個設定。您也可以更改壓縮、PPP 選項、登入名稱、密碼等等。

當新增一個裝置後，該裝置並沒有立即啟用，可由它的『**暫停不用的**』狀態得知。如要啟動這個裝置，請從裝置清單中選取它，再點選**啟用** 按鈕，假如系統設定為在電腦開機時即（預設）啟動這個裝置，您便不用再一次地執行這個步驟。



圖形12-5. ISDN 裝置

## 12.4. 建立一個數據機連線

數據機可以使用來透過現行的電話線設定一個網際網路連線，您也需要一個網路服務提供者(ISP)的帳號（也稱為一個撥接帳號）

如要新增一個數據機連線，請遵照以下步驟：

1. 點選『裝置』的標籤頁。
2. 再點選工具列上的**新增** 按鈕。
3. 從『裝置類型』的清單中選取『數據機連線』，再點選下一步。
4. 假如在硬體清單中已經設定好一部數據機（位於『硬體』標籤頁），**網路管理工具** 會假設您將使用它來建立一個數據機連線。假如目前並沒有設定任何的數據機，它將會試著在系統中偵測數據機的存在。這個偵測也許會花上一些時間，假如找不到數據機，會顯示一個訊息告訴您所顯示的數值並不是偵測過程中所找到的。
5. 偵測完成後，將會出現圖形12-6 視窗。

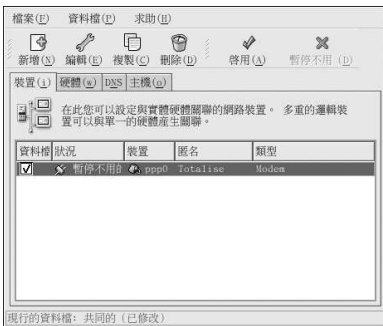


圖形12-6. 數據機設定

6. 設定數據機裝置、速率、流量控制以及數據機的聲音。假如您不知道這些數值，請接受預設值（如果有成功偵測數據機的話），假如您沒有按鍵式的電話，請取消選取相對應的選取盒，再點選下一步。

7. 假如您的網路服務提供者(ISP)有出現在預先設定的清單，請選取它。否則請輸入關於您ISP 帳號的必要資訊，假如您不知道這些資訊，請聯絡您的ISP，再點選下一步。
8. 在『IP 設定』的視窗中，選擇是否要透過DHCP 取得IP 位址，或者設定為靜態模式。完成後點選下一步。
9. 在『建立連接連線』的頁面點選套用。

在設定好數據機裝置後，它將會以Modem 裝置類型出現在如圖形12-7 所示的裝置清單中。



圖形12-7. 數據機裝置

請確定要選擇『檔案』=>『儲存』來儲存變更。

在新增完數據機裝置後，您可以從裝置清單中選取它，再點選編輯的按鈕來修改它的設定。例如，當新增裝置後，它是預設設定在開機時不啟動。請編輯它的組態設定以修改這個設定。您也可以更改壓縮、PPP 選項、登入名稱、密碼等等。

當新增一個裝置後，該裝置並沒有立即啟用，可由它的『暫停不用的』狀態得知。如要啟動這個裝置，請從裝置清單中選取它，再點選啟用 按鈕，假如系統設定為在電腦開機時即（預設）啟動這個裝置，您便不用再一次地執行這個步驟。

## 12.5. 建立一個xDSL 連線

DSL 代表『數位用戶迴路』(Digital Subscriber Lines)，有許多種不同類型的DSL，如ADSL，IDSL 以及SDSL。**網路管理工具** 使用專有名詞xDSL 來代表所有種類的DSL 連線。

有些DSL 提供者需要系統使用乙太網路卡並設定為透過DHCP 取得一個IP 位址，有些則需要您使用乙太網路卡設定一個PPPoE (Point-to-Point Protocol over Ethernet) 連線，請向您的DSL 提供者詢問該使用那一種方式。

假如您需要使用DHCP，請參考 12.2 節 來設定您的乙太網路卡。

假如您需要使用PPPoE，請遵照下列步驟：

1. 點選『裝置』的標籤頁。
2. 再點選工具列上的**新增** 按鈕。
3. 從『裝置類型』的清單中選取『xDSL 連線』，再點選下一步。
4. 假如您的乙太網路卡已經在硬體清單中，請從如圖形12-8 所示頁面的下拉式選單中選取『乙太網路裝置』。否則將會出現『選取乙太網路介面卡』的視窗。



### 請注意

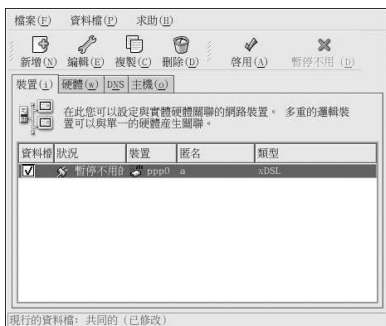
安裝程式會偵測有支援的乙太網路裝置，並提示您來設定它們。假如您在安裝過程中有設定任何的乙太網路裝置，它們將會出現在『硬體』標籤頁中的硬體清單。



圖形12-8. xDSL 設定

- 假如出現『選取乙太網路介面卡』的視窗，請選擇該乙太網路卡的製造商與型號，並選取裝置名稱。假如這是系統的第一片乙太網路卡，請選擇**eth0**當作裝置名稱，假如是第二片，則選擇**eth1**，依此類推。**網路管理工具**也讓您設定該網路卡的資源，請點選**下一步**繼續。
- 請輸入『提供者名稱』、『登入名稱』以及『密碼』。假如您擁有一個T-Online的帳號，請勿在預設視窗中輸入『登入名稱』與『密碼』，請點選**T-Online 帳號設定**的按鈕，在輸入需要的資訊。點選**下一步**繼續。
- 在『建立DSL連線』的頁面點選**套用**。

在設定好DSL連線後，它將會出現在如圖形12-7所示的裝置清單中。



圖形12-9. xDSL 裝置

請確定要選擇『檔案』=>『儲存』來儲存變更。

在新增完xDSL 連線後，您可以從裝置清單中選取它，再點選**編輯**的按鈕來修改它的設定。例如，當新增裝置後，它是預設設定在開機時不啟動。請編輯它的組態設定以修改這個設定。

當新增一個裝置後，該裝置並沒有立即啟用，可由它的『**暫停不用的**』狀態得知。如要啟動這個裝置，請從裝置清單中選取它，再點選**啟用**按鈕，假如系統設定為在電腦開機時即（預設）啟動這個裝置，您便不用再一次地執行這個步驟。

## 12.6. 建立一個記號環狀網路連線

一個記號環狀網路就是所有網路中的電腦以環形的模式連接在一起。一個記號或一個特殊的網路封包會在環狀網路中傳遞，以使得電腦可以傳送資訊給其他電腦。

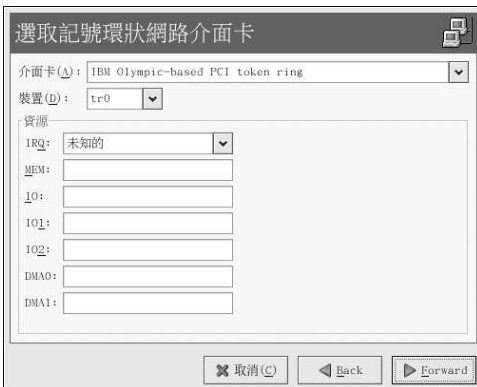


### 建議

如需關於在Linux 中使用記號環狀網路的資訊，請參考位於<http://www.linuxtr.net/> 的Linux Token Ring Project 網站。

如要新增一個記號環狀網路連線，請遵照以下步驟：

1. 點選『**裝置**』的標籤頁。
2. 再點選工具列上的**新增**按鈕。
3. 從『**裝置類型**』的清單中選取『**記號環狀網路連線**』，再點選下一步。
4. 假如您已經將該記號環狀網路卡加入到硬體清單中，請從『**記號環狀網路卡**』的清單中選取它，否則請選擇『**其他記號環狀網路卡**』來新增硬體裝置。
5. 假如您選擇『**其他記號環狀網路卡**』，將會出現如圖形12-10 所示的『**選取記號環狀網路介面卡**』的視窗。請選取該介面卡的製造商與型號，並選取裝置名稱。假如這是系統的第一片記號環狀網路卡，請選擇**tr0** 當作裝置名稱，假如是第二片，則選擇**tr1**，依此類推。**網路管理工具** 也讓您設定該介面卡的資源，請點選下一步 繼續。



圖形12-10. 記號環狀網路設定



6. 在『網路設定』視窗中，請選擇DHCP 或一個靜態的IP 位址。您可以為該裝置指定一個主機名稱，假如在每次啟動網路時，這個裝置都接收到一個動態的IP 位址，請不要指定一個主機名稱。點選下一步 繼續。

7. 在『建立記號環狀網路裝置』的頁面點選套用。

在設定好記號環狀網路裝置後，它將會出現在如圖形12-11 所示的裝置清單中。



圖形12-11. 記號環狀網路裝置

請確定要選擇『檔案』=>『儲存』來儲存變更。

在新增完裝置後，您可以從裝置清單中選取它，再點選**編輯**的按鈕來修改它的設定。例如您可以設定是否要在開機時啟動這個裝置。

當新增一個裝置後，該裝置並沒有立即啟用，可由它的『暫停不用的』狀態得知。如要啟動這個裝置，請從裝置清單中選取它，再點選**啟用** 按鈕，假如系統設定為在電腦開機時即（預設）啟動這個裝置，您便不用再一次地執行這個步驟。

## 12.7. 建立一個CIPE 連線

CIPE 代表Crypto IP Encapsulation。它是使用來設定一個IP 穿隧裝置的。例如，可以使用CIPE 來允許來自外來網路對一個虛擬私人網路(VPN)的存取權。假如您需要設定一個CIPE 裝置，請聯絡您的系統管理員，以取得正確的數值。

圖形12-12. CIPE 設定

**建議**

如需關於CIPE 與如何設定CIPE 的更多資訊，請參考 *Red Hat Linux* 安全性設定手冊。

## 12.8. 建立一個無線網路連線

無線乙太網路裝置近來漸漸地受歡迎，它的組態設定相當類似乙太網路的設定，除了您還需要為無線網路裝置配置例如SSID 與金鑰的設定。

如要新增一個無線網路連線，請遵照以下步驟：

1. 點選『裝置』的標籤頁。
2. 再點選工具列上的**新增** 按鈕。
3. 從『裝置類型』的清單中選取『無線網路連線』，再點選下一步。
4. 假如您已經將該無線網路介面卡加入到硬體清單中，請從『無線網路卡』的清單中選取它，否則請選擇『其他的無線網路卡』來新增硬體裝置。

**請注意**

安裝程式會偵測有支援的無線乙太網路裝置，並提示您來設定它們。假如您在安裝過程中有設定任何的乙太網路裝置，它們將會出現在『硬體』標籤頁中的硬體清單。

5. 假如您選擇『其他的無線網路卡』，將會出現『選取乙太網路介面卡』的視窗。請選取該乙太網路卡的製造商與型號，並選取裝置名稱。假如這是系統的第一片乙太網路卡，請選擇**eth0** 當作裝置名稱，假如是第二片，則選擇**eth1**，依此類推。**網路管理工具** 也讓您設定該無線網路介面卡的資源，請點選**下一步** 繼續。
6. 在如圖形12-13 所示的『設定無線網路連線』頁面配置該無線網路裝置的設定。



圖形12-13. 無線網路設定

7. 在『網路設定』視窗中，請選擇DHCP 或一個靜態的IP 位址。您可以為該裝置指定一個主機名稱，假如在每次啟動網路時，這個裝置都接收到一個動態的IP 位址，請不要指定一個主機名稱。點選下一步 繼續。
8. 在『建立無線網路裝置』的頁面點選套用。

在設定好無線網路裝置後，它將會出現在如圖形12-14 所示的裝置清單中。



圖形12-14. 無線網路裝置

請確定要選擇『檔案』=>『儲存』來儲存變更。

在新增完無線網路裝置後，您可以從裝置清單中選取它，再點選編輯 的按鈕來修改它的設定。例如您可以設定是否要在開機時啟動這個裝置。

當新增一個裝置後，該裝置並沒有立即啟用，可由它的『暫停不用的』狀態得知。如要啟動這個裝置，請從裝置清單中選取它，再點選啟用 按鈕，假如系統設定為在電腦開機時即（預設）啟動這個裝置，您便不用再一次地執行這個步驟。

## 12.9. 管理DNS 設定

在DNS 的標籤頁中，您可以設定系統的主機名稱、網域、名稱伺服器以及搜尋路徑。名稱伺服器是用來尋找網路上的其他主機。

假如DNS 伺服器名稱是來自DHCP 或PPPoE（或來自ISP），請勿增加任何的名稱伺服器。

假如主機名稱是動態地來自DHCP 或PPPoE（或來自ISP），請勿更改它。



圖形12-15. DNS 設定



#### 請注意

名稱伺服器部份並不設定系統成為一部名稱伺服器，然而在此可以設定要使用的名稱伺服器來解析IP 位址為主機名稱，且反之亦然。

## 12.10. 管理主機

在『主機』的標籤頁中，您可以新增編輯或移除/etc/hosts 檔案中的主機。這個檔案包含IP 位址以及相對應的主機名稱。

當您的系統試著要解析一個主機名稱到一個IP 位址或要找出一個IP 位址的主機名稱時，在向名稱伺服器查詢前，會先參考/etc/hosts 檔案中的紀錄（假如您是使用預設的Red Hat Linux 組態設定）。假如您的網路中含有IP 位址未列出在DNS 設定中的電腦，建議您將它們加入到/etc/hosts 檔案中。

如要增加一項紀錄到/etc/hosts 檔案中，請至『主機』的標籤頁，點選工具列上的**新增** 按鈕，輸入需要的資訊，再點選**確定** 的按鈕。選擇『檔案』=>『儲存』，或按下[Ctrl]-[S] 來儲存變更到/etc/hosts 檔案。因為目前版本的此檔案是在每次解析一個位址時被參考的，因此並不需要重新啟動網路或網路服務。



#### 警告

請勿移除localhost 的紀錄，即使系統並不連接至任何的網路或並不持續在一個網路連線的環境中，某些程式需要透過localhost 的loopback 介面來連線至系統。



圖形12-16. 主機設定

**建議**

如要變更搜尋的順序，請編輯 `/etc/host.conf` 檔案，這一行 `order hosts, bind` 指出 `/etc/hosts` 檔案的優先次序較高於名稱伺服器。如將此行更改為 `order bind, hosts`，將會設定系統先使用名稱伺服器來解析主機名稱與 IP 位址。假如無法透過名稱伺服器解析 IP 位址，系統將會轉而到 `/etc/hosts` 檔案中尋找 IP 位址。

**12.11. 啟用裝置**

可以設定在開機時是否要啟動網路裝置，舉例來說，數據機連線的網路裝置通常設定為不在開機時啟動，然而乙太網路連線通常設定為在開機時啟動。假如您的網路裝置是設定為不在開機時啟動，在開機後，您可以使用『Red Hat 網路裝置控制』程式來啟動它。如果要啟動它，請選擇面板上的『主選單按鈕』=>『系統工具』=>『網路裝置控制』，或輸入 `redhat-control-network` 指令。



圖形12-17. 啟用裝置

如要啟用一個裝置，請從清單中選取它，再點選**啟用**的按鈕；如要停用一個裝置，請從清單中選取它，再點選**暫停不用**。

假如有設定一個以上的網路資料檔，它們將會列出在這個介面中，而且可以被啟用。請參考 12.12 節以取得詳細資訊。

## 12.12. 使用資料檔

可以為每一個實體硬體裝置建立多個邏輯網路裝置，舉例來說，假如您的系統中有一個乙太網路卡(eth0)，您可以建立含有不同匿名與不同設定選項的邏輯網路裝置，所有都是與eth0 特定相關的。

邏輯網路裝置與裝置別名是不同的，與同一實體裝置關聯的邏輯網路裝置必須存在不同的資料檔中，而且無法同時啟用。裝置別名也是與同一實體硬體裝置關聯的，它們可以同時被啟用。請參考 12.13 節以取得關於建立裝置別名的詳細資訊。

可以使用資料檔來為不同網路建立多個設定組。一個設定組包括邏輯裝置以及主機與DNS 設定。在設定好資料檔後，您可以使用**網路管理工具**來在它們之間做轉換。

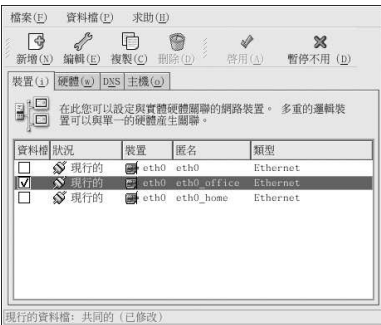
預設情況下，有一個稱為『共同的』資料檔，如要建立一個新的資料檔，請從程式選單選擇『資料檔』=>『新增』，然後為該資料檔輸入一個獨特的名稱。

主要視窗底端的狀態列將指出您已經修改新的資料檔。

點選清單中既有的裝置，再點選**複製**的按鈕來複製既有的裝置到一個邏輯網路裝置。假如您使用**新增**的按鈕，將會建立一個裝置別名，這是不正確的。如要更改邏輯裝置的內容，請從清單中選取它，再點選**編輯**的按鈕。舉例來說，可以更改匿名為一個較具描述性的名稱，如**eth0\_office**，以使之更容易辨識。

在裝置清單中，有一個標示為『資料檔』的欄位，對於每一個資料檔，您可以選取或取消選取裝置。只有選取的裝置會被含括在目前選取之資料檔中，舉例來說，假如您在一個稱為**Office**的資料檔中建立一個稱為**eth0\_office**的邏輯裝置，而您想要在該資料檔被選取時啟動該邏輯裝置，請取消選取eth0 裝置，並選取eth0\_office 裝置。

例如，圖形12-18 顯示含有**eth0\_office** 邏輯裝置的一個稱為**Office**的資料檔，它是被設定為使用DHCP 來啟動第一個乙太網路裝置。



圖形12-18. Office 資料檔

請注意如圖形12-19 所示的**Home** 資料檔將啟動與eth0 關聯的**eth0\_home** 邏輯裝置。



圖形12-19. Home 資料檔

您也可以設定只在**Office** 資料檔啟動eth0，而只在**Home** 資料檔啟動一個ppp（數據機）裝置。另一個例子是，使**Common** 資料檔啟動eth0，而當您在外旅行時讓**Away** 資料檔啟動一個ppp 裝置。

無法設定資料檔在開機時啟用，只有在『共同的』資料檔（預設資料檔）中設定要在開機時啟動的裝置，才會在開機時啟動。在系統開機後，請選擇面板上的『主選單』=>『系統工具』=>『網路裝置控制』（或輸入redhat-control-network 指令），並選取一個資料檔以啟用它。假如系統上有設定除了預設『共同的』資料檔之外的資料檔，這個啟用資料檔的部份只會出現在『網路裝置控制』的介面。

另外，您還可以使用下列的指令來啟用一個資料檔（請以資料檔名稱取代<profilename>）：

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

## 12.13. 裝置別名

裝置別名是與同一實體硬體關聯的虛擬裝置，不過可以同時以不同的IP 位址來啟用它們。通常它們是以裝置名稱加上一個冒號以及一個數字來表示（如eth0:1）。假如您想要讓系統擁有多個IP 位址，不過系統只有一張網路卡，您便可以使用這個選項。

在設定好乙太網路裝置（如eth0）來使用一個靜態的IP 位址後（不可使用DHCP 在別名設定上），請前往『裝置』標籤頁，然後點選**新增**的按鈕。選取要設定別名的乙太網路卡，為該別名設定一個靜態的IP 位址，再點選**套用**來建立它。因為該乙太網路卡已經設定了一個裝置名稱，現在要建立的則會是一個別名，如eth0:1。



### 警告

假如您要設定一個乙太網路裝置使之擁有一個別名，該裝置與其別名都不能使用DHCP，您必須手動設定IP 位址。

圖形12-20 顯示含有一個別名的eth0 裝置的例子，請注意eth0:1 裝置——為eth0 裝置的第一個別名；而第二個別名則是eth0:2，依此類推。如要修改裝置別名的設定，例如是否要在開機時啟動它以及別名號碼等，請從清單中選取它，再點選**編輯** 按鈕。



圖形12-20. 網路裝置別名範例

選取一個別名再點選**啟用**的按鈕來啟用該別名。假如您有設定多個資料檔，請選擇要將它放在那一個資料檔中。

如要確認該別名是否已經啟用，請使用 `/sbin/ifconfig` 指令，輸出應該要顯示含有不同IP 位址的裝置以及裝置別名：

```
eth0  Link encap:Ethernet HWaddr 00:A0:CC:60:B7:G4
       inet addr:192.168.100.5 Bcast:192.168.100.255 Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:161930 errors:1 dropped:0 overruns:0 frame:0
       TX packets:244570 errors:0 dropped:0 overruns:0 carrier:0
       collisions:475 txqueuelen:100
       RX bytes:55075551 (52.5 Mb) TX bytes:178108895 (169.8 Mb)
       Interrupt:10 Base address:0x9000

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

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



## 基本的防火牆設定

如同建築物中的防火牆試著要防止火勢蔓延，電腦的防火牆也要試著防止電腦受到電腦病毒的入侵以及阻止未經授權的使用者存取您的電腦。防火牆介於您的電腦與網路之間，它決定網路上的遠端使用者可以存取您電腦中的那些服務。一個妥善設定的防火牆可以大大地增加系統的安全性。在此建議您為任何擁有網際網路連線的Red Hat Linux 系統設定一個防火牆。

### 13.1. 安全等級設定工具

在Red Hat Linux 安裝的『防火牆設定』畫面，您可以選擇一個高度、中度或無防火牆的安全性設定，以及允許特定的裝置、流入的服務以及連接埠等。

在安裝完成後，您可以使用**安全等級設定工具**來變更系統的安全等級。假如您較喜歡使用一個精靈為主的應用程式，請參考 13.2 節。

如要啟動該應用程式，請選擇面板上的『主選單按鈕』=>『系統設定』=>『安全等級』，或在shell 提示符號下（如XTerm 或GNOME 終端機）輸入`redhat-config-securitylevel`指令。



圖形13-1. 安全等級設定工具

從下拉式選單中選擇想要的**安全等級**。

#### 高安全性

假如您選擇『**高安全性**』，您的系統將不接受任何您沒有特定定義的連線（除了預設的設定外），預設設定下，只允許下列的連線：

- DNS 回應
- DHCP — 所以任何使用DHCP 的網路介面仍可以正確地設定

假如您選擇『**高安全性**』，您的防火牆將不允許下列的連線：

- 主動模式的FTP（大部分用戶端預設使用的被動模式FTP 應該可以使用）

- IRC DCC 檔案傳輸
- RealAudio™
- 遠端的X 視窗系統用戶端

假如您連線您的系統到網際網路，但不打算執行一個伺服器，這是一個最安全的選擇。如果您需要額外的服務，您可以選擇**自訂**以允許特定服務通過防火牆。



#### 請注意

假如您選擇一個中度或高安全性的防火牆設定，您將無法使用網路認證方式(NIS 與LDAP)。

### 中安全性

如果您選擇『**中安全性**』，您的防火牆將不允許遠端的機器存取您系統上的某些資源。預設情況下，是不允許存取下列資源的：

- 低於1023 的連接埠號——大部分系統服務所使用的標準保留連接埠號，例如**FTP**、**SSH**、**telnet**、**HTTP** 以及**NIS**。
- NFS 伺服器連接埠(2049) — NFS 會停止遠端伺服器與本機用戶端使用。
- 本機的X 視窗系統顯示給遠端的X 用戶端。
- X 字型伺服器式連接埠（預設情況下，**xfs** 並不聽取網路上的訊息；它在字型伺服器式中被停用）。

如果您想要允許使用例如**RealAudio™**的資源，而仍然要拒絕存取一般系統的服務，請選擇『**中安全性**』。並選取『**自訂**』來允許可通過防火牆的特定服務。



#### 請注意

假如您選擇一個中度或高安全性的防火牆設定，您將無法使用網路認證方式(NIS 與LDAP)。

### 無防火牆

無防火牆的設定提供了完全存取您的系統，而且不做任何的安全性檢驗。安全性檢驗就是用來停止存取某些服務。如果您的系統在一個信任的網路環境內（非網際網路），或打算往後再設定防火牆，您才應該選擇這個選項。

選取『**自訂**』來新增信任裝置或允許使用額外的服務。

### 信任裝置

選取任何的『**信任裝置**』將允許從該裝置存取系統的所有流量；它將會排除防火牆的規則。例如，如果您正在執行一個區域網路，不過是經由一個PPP 撥號連接至網際網路，您可以選取**eth0**，如此將會允許所有來自於區域網路的流量。選取**eth0** 當作信任裝置表示允許所有來自這個乙太網路的流量，而且將**ppp0** 仍然放置在防火牆中。如果您想限制某一介面的流量，請讓它保持沒有選取的狀態。

在此不建議您設定任何連線至公開網路（例如網際網路）的裝置為一個『**信任裝置**』。

### 允許進入

啟用這些選項將允許通過防火牆的特定服務。請注意，在工作站的安裝中，大部分的這些服務都沒有安裝在系統上。

## DHCP

如果您允許DHCP查詢與回應進入，您將允許了任何使用DHCP決定IP位址的網路介面。DHCP通常是啟用的，如果DHCP沒有啟用，您的電腦將不再取得一個IP位址。

## SSH

Secure *SHell* (SSH) 是一套工具用來在遠端機器登入與執行指令。如果您打算使用SSH工具通過防火牆來存取您的機器，請啟用這個選項。為了要使用SSH工具遠端存取您的電腦，您將需要安裝openssh-server套件。

## Telnet

Telnet 是一種用來登入遠端電腦的通訊協定。Telnet 的連線是未加密的，並且不提供對於網路竊聽的安全性保護。在此並不建議允許Telnet存取的流入。如果您真的要允許流入Telnet的存取，您將需要安裝telnet-server套件。

## WWW (HTTP)

HTTP 通訊協定是由Apache（以及其他的網頁伺服器）使用來伺服網頁。如果您打算使您的網頁伺服器可公開存取，請啟用這個選項。這個選項對於本機上瀏覽網頁或開發網頁並不需要。如果您想要伺服網頁，您將需要安裝httpd套件。

啟用**WWW (HTTP)**不會開啟一個連接埠給HTTPS。要啟用HTTPS，請在『**其他埠**』的欄位指定它。

## Mail (SMTP)

如果您想允許流入的郵件傳送通過您的防火牆，使遠端的主機就可以直接連線至您的機器來傳送郵件，請啟用這個選項。如果您是使用POP3或IMAP從您的ISP伺服器下載郵件或者是您使用一種工具，例如fetchmail，您則不需要啟用這個選項。請注意，一個錯誤設定的SMTP伺服器會允許遠端機器使用您的伺服器來傳送垃圾郵件。

## FTP

FTP 通訊協定是用來在網路上的機器間傳輸檔案。假如您打算讓您的FTP伺服器可公開存取，請啟用這個選項。為了要使用這個選項，您必須安裝vsftpd套件。

點選**確定**來啟動防火牆，在點選**確定**後，所選取的選項會轉譯為iptables指令，並且寫入到/etc/sysconfig/iptables檔案中。iptables服務也同時啟動，使得防火牆在儲存選取之選項後立即啟動。



### 警告

假如您有設定一個防火牆，或在/etc/sysconfig/iptables檔案中有任何的防火牆規則，而您選取『**無防火牆**』，然後點選**確定**以儲存變更，該檔案將會被刪除。

所選取的選項也會寫入到/etc/sysconfig/redhat-config-securitylevel檔案，使得下次啟動應用程式時可以回復設定。請勿手動編輯這個檔案。

如要在開機時自動啟動iptables服務，請參考 13.3節以取得詳細資訊。

## 13.2. GNOME Lokkit

藉由構想基本的iptables網路連線規則，**GNOME Lokkit** 讓您為一般的使用者配置防火牆的設定。該程式將會向您詢問關於如何使用系統的一連串問題，並且為您寫入到規則/etc/sysconfig/iptables檔案中，您便不用自己手動撰寫這些規則。

您不應該試著使用**GNOME Lokkit**來產生複雜的防火牆規則，它是為一般的使用者想要在使用數據機、纜線或DSL 網際網路連線時保護他們自己所設計的。如要設定特定的防火牆規則，請參考**Red Hat Linux**參考手冊中的『使用**iptables**設定防火牆」一章。

如要停用特定的服務，並且拒絕特定的主機與使用者，請參考第14章。

如要啟動圖形化版本的**GNOME Lokkit**，請選擇『主選單按鈕』=>『系統工具』=>『更多系統工具』=> **Lokkit**，或以root 身份在shell 提示符號下輸入**gnome-lokkit** 指令。假如您沒有安裝**X** 視窗系統，或者您較喜歡使用文字介面的程式，請在shell 提示符號下輸入**lokkit** 指令來啟動文字模式的版本。

### 13.2.1. 基本的



圖形13-2. 基本的

在啟動程式後，請為您的系統選擇適當的安全等級：

- **高安全性** — 這個選項關閉絕大部分的網路連線，除了DNS 回應以及DHCP，這使得仍然可以啟動網路介面。IRC, ICQ 以及其他的即時傳訊服務以及RealAudio™ 將無法在缺少代理伺服器的情況下使用。
- **低安全性** — 這個選項將不允許遠端連線到系統，包括NFS 連線以及遠端的X 視窗系統作業階段。在1023 連接埠號以下執行的服務將會被拒絕連線，包括FTP, SSH, Telnet 與HTTP。
- **關閉防火牆** — 這個選項並不建立任何的安全性規則，建議您只使用這個選項在位於信任網路（非網際網路）的系統上、假如系統位於大型防火牆以內，或者您自己撰寫自訂的防火牆規則等情況下。假如您選擇這個選項，並按下一步，請翻閱至 13.3 節。您系統的安全性設定將不會變更。

### 13.2.2. 本地端主機

假如系統上有乙太網路裝置，『本地端主機』的頁面讓您設定是否套用防火牆規則到傳送至每一裝置的連線要求。假如該裝置將系統連線到防火牆內部的一個區域網路，而不直接連線至網際網路，請選擇是。假如乙太網路卡將系統連線到一個纜線或DSL 數據機，建議您選擇否。



圖形13-3. 本地端主機

### 13.2.3. DHCP

假如您使用DHCP來啟動系統上任何的乙太網路介面，您必須在DHCP的頁面回答是。假如您選擇否的話，您將無法使用乙太網路介面建立一個連線。許多纜線與DSL網際網路提供者需要您設定使用DHCP來建立一個網際網路連線。



圖形13-4. DHCP

### 13.2.4. 設定服務

GNOME Lokkit也讓您可以用啟動與停止一般的服務，假如您在服務設定的頁面回答是的話，您將會被提示設定下列的服務：

- **Web 伺服器** — 假如您想要其他人連線到您系統中的一部網頁伺服器（如Apache），請選擇這個選項。假如您只是想要瀏覽您自己系統中與網路上其他伺服器的網頁，您並不需要選擇這個選項。

- **外來的電子郵件** — 假如您的系統需要接收外來的電子郵件，請選擇這個選項，假如您是使用IMAP、POP3 或fetchmail 來接收郵件，您並不需選擇這個選項。
- **安全殼** — Secure Shell 或SSH 是透過加密連線用來在遠端機器登入與執行指令的一套工具。如果您打算使用SSH 工具來存取您的機器，請啟用這個選項。
- **Telnet** — Telnet 可使您用來以遠端登入您的電腦，然而它是不安全的，因為它透過網路傳送未加密的純文字（包括密碼）。建議您使用SSH 遠端登入您的機器，假如您需要使用telnet 來存取您的系統，請選取這個選項。

如要停止其他您不需要的服務，請使用**系統服務設定工具**（請看 14.3 節）或**ntsysv**（請看 14.4 節），或者**chkconfig**（請看 14.5 節）。

### 13.2.5. 啟動防火牆

點選**完成** 將會寫入防火牆規則到/etc/sysconfig/iptables，並且藉由啟動iptables 服務來啟動防火牆設定。



#### 警告

假如您有設定一個防火牆，或在/etc/sysconfig/iptables 檔案中有任何的防火牆規則，而您選取『**停用防火牆**』，再點選**完成** 來儲存變更，該檔案將會被刪除。

強烈建議您在本機執行**GNOME Lokkit**，而不是從一個遠端的X 作業階段？假如您停止遠端存取您的系統，您將不再能夠存取它，或停用防火牆的規則。

假如您不想要寫入防火牆的規則，請點選**取消**。

#### 13.2.5.1. 郵件轉送

郵件轉送是一部允許其他系統透過它傳送電子郵件的系統，假如您的系統是一部郵件轉送，某些人也許會透過您的機器傳送垃圾郵件給其他人。

假如您選擇要啟動郵件服務，在您點選『**啟動防火牆**』頁面上的**完成** 後，您將會被提示要檢查郵件轉送。假如您選擇是以檢查郵件轉送，**GNOME Lokkit** 將會試著連線到位於<http://www.mail-abuse.org/> 的*Mail Abuse Prevention System* 網站，並且執行一個郵件轉送測試程式。當完成後，測試的結果將會顯示出來，假如您的系統是開放給郵件轉送，強烈建議您設定Sendmail 來避免它。

## 13.3. 啟動iptables 服務

防火牆的規則只在iptables 服務執行中時才會啟用，如要手動啟動該服務，請使用下列指令：

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

如要確保在系統開機時有啟動該服務，請執行下列指令：

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

ipchains 服務不能與iptables 服務一併執行，要確定ipchains 服務已經停止，請執行下列指令：

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

可以使用**系統服務設定工具**來設定iptables與ipchains的服務，請參考 14.3 節以取得更詳細資訊。





## 控制服務的存取

維護您Red Hat Linux 系統的安全性是相當重要的，一種用來管理系統安全性的方式是细心的管理系統服務的存取。您的系統也許需要提供一種特定服務的存取（舉例來說，如果您執行一個網頁伺服器，便需要提供httpd 服務）。然而，假如您並不需要提供該項服務，您應該將它關閉，以降低可能遭受入侵的機會。

有許多種不同的方法用來管理系統服務的存取，基於所要提供的服務、您系統的組態設定以及您對Linux 的熟悉程度，您必須決定您想要使用何種方法。

拒絕服務存取的最簡單方法是將它關閉。由xinetd（稍候將會介紹）所管理的服務以及/etc/rc.d 架構下的服務都可使用三種不同的應用程式來設定使其啟動或關閉：

- **系統服務設定工具** — 它是一個圖形化的應用程式，它會顯示每一個服務的描述，並顯示每一個服務是否在開機時啟動（在執行等級3、4 與5），以及用來啟動、停止或重新啟動各項服務。
- **ntsysv** — 一個文字介面的應用程式，可使用它來設定每一個執行等級在開機時要啟動的服務。對非xinetd 服務所做的變更無法立即生效，況且不能使用這個程式來啟動、停止或重新啟動非xinetd 的服務。
- **chkconfig** — 一個命令列的工具程式，可使用它來啟動或停止不同執行等級中所執行的服務。對非xinetd 服務所做的變更無法立即生效，況且不能使用這個程式來啟動、停止或重新啟動非xinetd 的服務。

您將會發現以上這些工具程式會比以下這種方法好用多了— 手動編輯位於/etc/rc.d 目錄下的許多符號連結，或者是編輯位於/etc/xinetd.d 目錄下的xinetd 設定檔案。

另一個管理系統服務存取的方法是使用iptables 來設定一個IP 的防火牆，如果您是使用Linux 的新手，iptables 也許並不適用於您。設定好iptables 可以是一件很複雜的事，通常是由較有經驗的Linux 系統管理員來做。

不過就另一方面來說，使用iptables 的好處是它很有彈性。舉例來說，假如您需要一個能夠提供某些主機來存取某些服務的自訂解決方案，iptables 能夠幫您做到。如需關於iptables 的更多資訊，請參考Red Hat Linux 參考手冊 與Red Hat Linux 安全性設定手冊。

或者是，假如您需要一個工具來為您的個人桌上電腦設定一般的存取法則，或者您是Linux 的新手，您可以試試**安全等級設定工具**（redhat-config-securitylevel），來為您的系統選擇適當的安全等級，它很類似在Red Hat Linux 安裝程式中的『**防火牆設定**』畫面。您也可以使用**GNOME Lokkit**，它是一種GUI 的應用程式，它會問您一些關於您要如何使用您機器的問題，依據您的答案，它將會為您設定一個簡單的防火牆。請參考第13章 以取得關於這些工具的更多資訊。假如您需要更多特定的防火牆規則，請參考Red Hat Linux 參考手冊 中的iptables 一章。

### 14.1. 執行等級

在您設定服務的存取控制前，您必須了解Linux 的執行等級。一個執行等級是一種狀態或模式，它是由/etc/rc.d/rc<x>.d 目錄中列出的服務所定義（<x> 就是執行等級的號碼）。

Red Hat Linux 使用下列的執行等級：

- 0 — 系統關機
- 1 — 單一使用者模式
- 2 — 尚未使用（可由使用者定義）
- 3 — 多使用者模式
- 4 — 尚未使用（可由使用者定義）

- 5 — 多使用者模式 (含有一個X 介面的登入畫面)
- 6 — 重新開機

假如您是使用文字介面的登入畫面，表示您是在執行等級3 中操作；假如您是使用一個圖形的登入畫面，您是在執行等級5 中操作。

可以藉由修改/etc/inittab 檔案來變更預設的執行等級，只需修改如下所示這一行：

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

將這一行中號碼改為您想要的執行等級，在您重新開機後，您所做的變更才會生效。

如要立即變更執行等級，請使用telinit 指令後面加上執行等級編號。您必須是root 才能使用這個指令。

## 14.2. TCP 包裹程式(Wrappers)

許多UNIX 的系統管理員都較習慣使用TCP 包裹程式來管理某些網路服務的存取。任何由xinetd 管理的網路服務 (以及含有libwrap 嵌入式支援的任何程式) 都可以使用TCP 包裹程式來管理存取。xinetd 可以使用/etc/hosts.allow 與/etc/hosts.deny 檔案來設定存取系統的服務。如名稱所示，hosts.allow 包含了一系列的規則以允許存取由xinetd 所控制的網路服務，而hosts.deny 檔案則包含了拒絕存取的規則。系統將會優先搜尋hosts.allow 檔案的內容，然後再搜尋hosts.deny 檔案的內容。可以基於個別的IP 位址 (或主機名稱) 或是一個用戶端的模式來允許或拒絕存取的權限。請參閱Red Hat Linux 參考手冊 以及hosts\_access 第5 部份的man page(man 5 hosts\_access) 以取得更詳細的資訊。

### 14.2.1. xinetd

如要控制網際網路的存取，請使用xinetd，它是inetd 一個較安全的替代品。xinetd 系統程式包除了系統的資源，並且提供存取控制與紀錄檔案，可以使用它來啟動特殊目的的伺服器。xinetd 可以用來提供存取或拒絕存取特定的主機、在某些時間提供服務的存取、限制進來連線的速度或者由這些連線所造成的系統負載等等。

xinetd 會持續性的執行，並聽取它管理的所有連接埠。當出現一個連線要求其中一個它所管理之服務時，xinetd 便會為該項服務啟動適當的伺服器。

xinetd 的設定檔案是/etc/xinetd.conf，不過這個檔案只包含了一些預設值，以及一個要含括/etc/xinetd.d 目錄的指示。如要啟動或停止一個xinetd 的服務，請編輯位於/etc/xinetd.d 目錄下的設定檔案。假如disable 屬性設定為yes，表示該項服務已經停止。假如disable 屬性設定為no，表示該項服務已經啟動。您可以編輯xinetd 任何的設定檔案，或使用系統服務設定工具、ntsysv 或chkconfig 來變更它的啟動狀態。如要取得xinetd 所控制的網路服務，請使用ls /etc/xinetd.d 指令來檢視/etc/xinetd.d 目錄的內容。

## 14.3. 系統服務設定工具

系統服務設定工具 是一個由Red Hat 所開發的圖形化應用程式，可用它來設定在/etc/rc.d/init.d 中那一個SysV 的服務要在開機時啟動 (在執行等級3、4 與5) 以及啟動那一個xinetd 的服務。您也可以使用它來啟動、停止與重新啟動SysV 的服務以及重新啟動xinetd。

如要在桌面啟動系統服務設定工具，請點選『主選單按鈕』 (在面板上) => 『系統設定』 => 『伺服器設定』 => 『服務』，或在shell 提示符號下 (如XTerm 或GNOME 終端機) 輸入redhat-config-services 指令。



圖形14-1. 系統服務設定工具

**系統服務設定工具** 會顯示目前的執行等級以及您正要編輯的執行等級。如要編輯另一個執行等級，請從程式選單中選取『**編輯執行等級**』然後選擇執行等級3、4或5。請參考 14.1 節 以取得關於執行等級的描述。

**系統服務設定工具** 會列出/etc/rc.d/init.d 中的服務以及由xinetd 所控制的服務。點選在應用程式式左邊欄位中的服務名稱，將會顯示該服務的簡短描述以及目前的執行狀態。假如這個服務不屬於xinetd 服務的一部分，狀態視窗將會顯示該服務是否正在執行中。假如該服務為xinetd 所控制，狀態視窗將會顯示 **xinetd service**。

如要立即啟動、停止或重新啟動一項服務，請從清單中選取該服務，並點選工具列上的適當按鈕（或由『**動作**』選單中選取要做的動作）。假如該服務屬於xinetd 服務之一，動作的按鈕將會被停用，因為它們不能個別的啟動或停止。

假如您藉由選取或取消選取一個xinetd 服務名稱旁的選取盒來啟動或停止該服務，您必須從工具列上選擇『**檔案**』=>『**儲存變更**』來重新啟動xinetd，然後立即啟動或停止您所變更的xinetd 服務。xinetd 也已經設定為可以記憶設定，您可以同時啟動或停止一個以上的xinetd 服務，然後在您完成後再儲存變更。

例如，假設您選取rsync 讓它在執行等級3 時啟動，並儲存變更，rsync 服務已經立即啟動了。下次當xinetd 啟動時，rsync 仍然還是啟用的。

**警告**

當您儲存變更到xinetd 的服務，xinetd 就會重新啟動，而且變更將會立即生效。當您儲存變更到其他的服務時，就會重新設定執行等級，不過所做的變更不會立即生效。

如要在目前選取的執行等級下開機時啟動一個非xinetd的服務，請點選在清單中該服務名稱旁的選取盒。在設定好執行等級後，請從工具列的選單中選擇『檔案』=>『儲存變更』來套用變更。現在已經改變執行等級的設定，不過尚未重新啟動執行等級，因此所做的變更沒有立即生效。

舉例來說，假設您要設定執行等級3，假如您改變anacron服務的值由選取改為未選取，然後選擇『儲存變更』，執行等級3的設定已經改變，所以anacron不會在開機時啟動。然而，您尚未重新初始化執行等級3，所以anacron仍然在執行中。在此您可以選擇下列的其中一種選項：

1. 停止anacron服務—從清單中選取它再點選**停止**的按鈕來停止該服務。會出現一個訊息告訴您已經成功停止該服務了。
2. 重新初始化執行等級—在shell提示符號下輸入telinit 3指令來重新初始化執行等級（3為執行等級的編號）。假如您更改一個以上之服務『開機時啟動』的值，而且想要立即使變更生效，建議您使用這個選項。
3. 不做任何事—您並不需要停止anacron的服務，您可以等系統重新開機時，便會停止該服務。下次系統開機後，執行等級將會被初始化而且不會執行anacron服務。

## 14.4. ntsysv

ntsysv 工具提供了一個簡單的介面，可用來啟動與停止各項服務。您可以使用ntsysv來啟動或停止一個xinetd管理的服務。您也可以使用ntsysv來設定執行等級，預設情況下只會設定目前的執行等級。如要設定另一個執行等級，請使用--level 選項來指定一個或多個執行等級。舉例來說，ntsysv --level 345 指令是要來設定執行等級3、4與5。

ntsysv 的程式介面就像是文字模式的安裝程式，您可以使用上下方向鍵來上下瀏覽服務清單。空白鍵是用來選取或取消選取服務，而且也可使用來"按下"『確定』與『取消』按鈕。如要在服務清單與『確定』、『取消』按鈕間移動，請使用[Tab] 按鈕。一個\*符號代表一項服務已經設定為啟動。按下[F1] 按鈕將會跳出該項服務的簡短說明。



警告

在ntsysv 裡做設定會立即影響到由xinetd 所管理的服務，至於其他的服務，變更不會立即生效。您必須使用service daemon stop 指令來停止或啟動個別的服務。在以上這個例子中，請以您想要停止的服務名稱取代daemon，如httpd。請以start 或restart 來取代stop 以啟動或重新啟動該服務。

## 14.5. chkconfig

chkconfig 指令也可以使用來啟動或停止服務，假如您使用chkconfig --list 指令，您將會看到系統服務的清單以及在執行等級0-6 中它們是啟動(on) 或停止(off)。在這個清單的最後，您將會看到一個部份列出由xinetd 管理的所有服務。

假如您使用chkconfig --list 來查詢一個由xinetd 管理的服務，您將會看到該xinetd 的服務是否已經啟動(on) 或停止(off)。例如，chkconfig --list finger 指令會傳回以下的輸出：

```
finger    on
```

如以上所示，finger 已經啟動為一個xinetd 的服務。假如xinetd 在執行中，表示finger 也已經啟動了。

假如您使用chkconfig --list 來查詢在/etc/rc.d 中的服務，您將會看到在每一個執行等級中該項服務的設定。例如chkconfig --list anacron 指令將傳回以下的輸出：

```
anacron   0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

`chkconfig` 也可以使用來設定在一個特定的執行等級中要啟動（或停止）的服務。例如要在執行等級3、4 與5 中將`nscd` 服務停止，請使用下列指令：

```
chkconfig --level 345 nscd off
```



**警告**

`chkconfig` 指令會立即影響到由`xinetd` 管理的服務，假如`xinetd` 正在執行中，而`finger` 服務已經停止，執行`chkconfig finger on` 的指令後將會立即啟動`finger` 服務，而不需手動重新啟動`xinetd`。而在`chkconfig` 指令後，對其他服務所做的變更不會立即生效。您必須使用`service daemon stop` 指令來停止或啟動個別的服務。在以上這個例子中，請以您想要停止的服務名稱取代`daemon`，如`httpd`。請以`start` 或`restart` 來取代`stop` 以啟動或重新啟動該服務。

## 14.6. 其他的資源

如需要更多的資訊，請參考下列的資源。

### 14.6.1. 已安裝的說明文件

- `ntsysv`、`chkconfig`、`xinetd` 與`xinetd.conf` 的`man pages`。
- `man 5 hosts_access` — 主機存取控制檔案格式的`man page`（位於`man pages` 的第五部份）。

### 14.6.2. 很有用的網站

- <http://www.xinetd.org> — `xinetd` 的官方網站，這裡有更詳細的特色清單以及設定檔案的範例。

### 14.6.3. 相關書籍

- *Red Hat Linux* 參考手冊, Red Hat, Inc. — 這本手冊包含了關於TCP 包裹程式以及`xinetd` 允許或拒絕存取的詳細資訊、關於如何使用它們設定網路存取的更詳細資訊，以及建立`iptables` 防火牆規則的指示。



OpenSSH 是一種免費且開放原始碼的SSH 通訊協定的實作(*Secure SHell*)。它使用安全且加密的網路連線工具來取代telnet、ftp、rlogin、rsh 與rcp。OpenSSH 支援1.3、1.5 與2 版的SSH 通訊協定，從OpenSSH 2.9 版本開始，預設的通訊協定是預設使用RSA 金鑰的版本2。

### 15.1. 為什麼要使用OpenSSH ?

假如您使用OpenSSH 工具，您便加強了您系統的安全性，所有使用OpenSSH 工具的通訊包括密碼都是經過加密的。Telnet 與ftp 是使用明文(clear text)的密碼，而且所有傳送的訊息都是未加密的。這有可能會導致傳送的資訊以及密碼被截取，然後您的系統便會被未經認證的人使用所截取的密碼來登入您的系統，造成危害系統的機會。所以請盡可能使用OpenSSH 所提供的工具組以避免這些安全性的問題。

另一個使用OpenSSH 的理由是它將自動傳送DISPLAY 的環境變數到用戶端的機器，也就是說，假如您在本機上執行X 視窗系統，然後您使用ssh 指令登入到一部遠端的機器，當您在遠端的機器上執行需要X 的程式，該程式將會顯示在您的本機機器上。假如您較習慣使用圖形化的系統管理工具，不過卻無法實際操作您的伺服器，這樣的特色將帶給您很大的方便。

### 15.2. 設定一個OpenSSH 伺服器

如要執行OpenSSH 伺服器，您必須先確定您已安裝適當的RPM 套件，您需要openssh-server 套件，而且它相依於openssh 套件。

OpenSSH 系統程式使用/etc/ssh/sshd\_config 設定檔，Red Hat Linux 預設安裝的設定檔案應該就可符合大多數人的需求。假如您想要的系統程式設定與預設的sshd\_config 所提供的不同，請參考sshd 的man page 以取得您可以在設定檔案中定義的關鍵字。

如要啟動OpenSSH 服務，請使用/sbin/service sshd start 指令，如要停止OpenSSH 伺服器，請使用/sbin/service sshd stop 指令。假如您想要在開機時自動啟動這個系統程式，請參考第14章 以取得如何管理服務的資訊。

假如您重新安裝一部Red Hat Linux 系統，而您的用戶端在重新安裝前曾經使用OpenSSH 工具連線到您的系統，在重新安裝完後，用戶端的使用者如果要試著連線您的機器，將會看到以下的訊息：

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@  WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!  @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
```

重新安裝的系統建立了一組新的認證金鑰，因此才有關於RSA 主機金鑰改變的警告。假如您想要保留系統所產生的主機金鑰，請備份/etc/ssh/ssh\_host\*key\* 等檔案，然後在重新安裝完後，將它們複製回去。這樣的程式將會保留系統的識別身份，使得當用戶端使用者在重新安裝完後試著連線到系統時，不會收到警告訊息。

### 15.3. 設定一部OpenSSH 用戶端

如要從一部用戶端機器連線到一部OpenSSH 伺服器，用戶端機器必須已安裝openssh-clients 與openssh 套件。

### 15.3.1. 使用ssh 指令

ssh 指令是rlogin、rsh 以及telnet 等指令之強調安全性的替代品。它使您可以登入到遠端的機器以及在遠端機器上執行指令。

使用ssh 登入到遠端機器相當類似使用telnet。如要登入稱為penguin.example.net 的遠端機器，請在shell 提示符號下輸入以下指令：

```
ssh penguin.example.net
```

當您第一次ssh 登入到一部遠端機器，您將會看到如下的訊息：

```
The authenticity of host 'penguin.example.net' can't be established.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

請輸入**yes** 以繼續。這個動作（如以下所示）將會加入該伺服器到您的系統已知的主機清單中：

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list of known hosts.
```

再來您將會看到一個提示符號問您在遠端機器的密碼，在輸入密碼後，您就會得到遠端機器的一個shell 提示符號。假如您沒有指定使用者名稱，您在用戶端機器登入的使用者名稱將會傳送至遠端機器。假如您想要指定一個不同的使用者名稱，請使用下列的指令：

```
ssh username@penguin.example.net
```

您也可以使用如ssh -l username penguin.example.net 的語法。

可以使用ssh 指令在遠端機器上來執行指令（不需要登入shell 提示符號），語法是ssh hostname command。舉例來說，假如您在遠端機器(penguin.example.net)上執行ls /usr/share/doc 指令，請在shell 提示符號下輸入以下指令：

```
ssh penguin.example.net ls /usr/share/doc
```

在您輸入正確的密碼後，將會列列出遠端目錄/usr/share/doc 的內容，而且您會回到您的本機shell 提示符號。

### 15.3.2. 使用scp 指令

可以使用scp 指令來透過一個安全且加密的連線在機器間傳輸檔案，就如同rcp 指令。

傳輸一個本機檔案到遠端機器的一般語法如下：

```
scp localfile username@tohostname:/newfilename
```

localfile 代表來源檔案，而username@tohostname:/newfilename 代表目的地。

如要傳輸本機檔案shadowman 到您在penguin.example.net 主機中的帳號，請在shell 提示符號下輸入以下指令（使用您的使用者名稱取代username）：

```
scp shadowman username@penguin.example.net:/home/username
```

這將會傳輸本機檔案shadowman 到penguin.example.net 主機上的/home/username/shadowman。

如果要傳輸一個遠端的檔案到本機系統，一般的語法如下：

```
scp username@tohostname:/remotefile /newlocalfile
```

remotefile 代表來源檔案，而newlocalfile 代表目的地。



還可以指定多重的檔案當作來源檔案，例如要傳輸/downloads 目錄的內容到遠端機器 penguin.example.net 上一個既存的目錄稱為 uploads，請在 shell 提示符號下輸入以下指令：

```
scp /downloads/* username@penguin.example.net:/uploads/
```

### 15.3.3. 使用 sftp 指令

sftp 工具可以使用來開啟一個安全的且互動式的 FTP 連線，它相當類似 ftp，不過它是使用一種安全且加密的連線。一般的語法是 `sftp username@hostname.com`。一旦認證通過後，您便可以使用類似 FTP 中的一系列指令。請參閱 sftp 的 man page 以取得這些指令的清單。如要讀取 man page，請在 shell 提示符號下執行 `man sftp` 指令。sftp 工具只包含在 OpenSSH 2.5.0p1 以上的版本。

### 15.3.4. 產生金鑰對

假如您不想要每次使用 ssh、scp 或 sftp 來連線到遠端機器時都必須輸入密碼，您可以產生一個認證的金鑰。

必須產生金鑰給每一個使用者，如要如此做，請以想要連線到遠端機器的使用者身份執行下列的步驟。假如您以 root 使用者完成以下步驟，只有 root 才能使用這些金鑰。

從 OpenSSH 3.0 版本開始，`~/.ssh/authorized_keys2`、`~/.ssh/known_hosts2` 與 `/etc/ssh_known_hosts2` 都已經被取代不用了。SSH 通訊協定 1 與 2 共用 `~/.ssh/authorized_keys`、`~/.ssh/known_hosts` 與 `/etc/ssh/ssh_known_hosts` 檔案。

Red Hat Linux 9 預設使用 SSH 通訊協定 2 以及 RSA 金鑰。



#### 建議

假如您重新安裝 Red Hat Linux，而想要儲存您之前所產生的金鑰對，請備份您家目錄下的 `.ssh` 目錄。在重新安裝完後，將該目錄複製回去您的家目錄中，系統上的所有使用者（包括 root）都可以完成這個過程。

#### 15.3.4.1. 產生一副版本 2 的 RSA 金鑰對

請使用以下的步驟來產生 SSH 通訊協定版本 2 的一副 RSA 金鑰對，這是從 OpenSSH 2.9 版本開始的預設值。

1. 如要產生一副 RSA 金鑰對以使用於版本 2 的通訊協定，請在 shell 提示符號下輸入以下指令：

```
ssh-keygen -t rsa
```

請接受 `~/.ssh/id_rsa` 的預設檔案位置，並輸入一個與您本機帳號的密碼不同的通行密碼 (passphrase)，然後再輸入一次以做確認。

公鑰將會寫入到 `~/.ssh/id_rsa.pub`，而私鑰則是寫入到 `~/.ssh/id_rsa`。請勿散佈您的私鑰給任何人。

2. 使用 `chmod 755 ~/.ssh` 指令來變更 `.ssh` 目錄的權限設定。
3. 複製 `~/.ssh/id_rsa.pub` 的內容到您想要連線之機器的 `~/.ssh/authorized_keys` 檔案中，假如 `~/.ssh/authorized_keys` 不存在，您可以複製 `~/.ssh/id_rsa.pub` 檔案到另一部機器的 `~/.ssh/authorized_keys` 檔案。
4. 假如您是使用 GNOME 的桌面環境，請跳過本章節至 15.3.4.4 節，假如您並沒有使用 X 視窗系統，請跳過本章節至 15.3.4.5 節。

### 15.3.4.2. 產生一副版本2的DSA金鑰對

請使用下列的步驟來產生SSH通訊協定版本2的一副DSA金鑰對。

1. 如要產生一副DSA金鑰對以使用於版本2的通訊協定，請在shell提示符號下輸入以下指令：

```
ssh-keygen -t dsa
```

請接受`~/.ssh/id_dsa`的預設檔案位置，並輸入一個與您本機帳號的密碼不同的通行密碼，然後再輸入一次以做確認。



#### 建議

通行密碼是用來認證一個使用者的一串文字與字元，它與密碼不同的地方在於您可以使用空白字元或tab按鍵在通行密碼上。通行密碼通常都比密碼長，因為它們通常是片語而不是單字。

公鑰將會寫入到`~/.ssh/id_dsa.pub`，而私鑰則是寫入到`~/.ssh/id_dsa`。請切記決不散佈您的私鑰給任何人。

2. 使用`chmod 755 ~/.ssh`指令來變更`.ssh`目錄的權限設定。
3. 複製`~/.ssh/id_dsa.pub`的內容到您想要連線之機器的`~/.ssh/authorized_keys`檔案中，假如`~/.ssh/authorized_keys`不存在，您可以複製`~/.ssh/id_dsa.pub`檔案到另一部機器的`~/.ssh/authorized_keys`檔案。
4. 假如您是使用GNOME的桌面環境，請跳過本章節至 15.3.4.4節，假如您並沒有使用X視窗系統，請跳過本章節至 15.3.4.5節。

### 15.3.4.3. 產生一副版本1.3與1.5的RSA金鑰對

請使用以下的步驟來產生SSH通訊協定版本1的一副RSA金鑰對，假如您只連線到使用DSA的系統，您並不需要RSA版本1.3或RSA版本1.5的金鑰對。

1. 如要產生一副RSA金鑰對以使用於版本1.3與1.5的通訊協定，請在shell提示符號下輸入以下指令：

```
ssh-keygen -t rsa1
```

請接受預設的檔案位置(`~/.ssh/identity`)，並輸入一個與您本機帳號的密碼不同的通行密碼，然後再輸入一次以做確認。

公鑰將會寫入到`~/.ssh/identity.pub`，而私鑰則是寫入到`~/.ssh/identity`。請勿散佈您的私鑰給任何人。

2. 使用`chmod 755 ~/.ssh`與`chmod 644 ~/.ssh/identity.pub`來變更`.ssh`目錄與金鑰的權限設定。
3. 複製`~/.ssh/identity.pub`的內容到您想要連線之機器的`~/.ssh/authorized_keys`檔案中，假如`~/.ssh/authorized_keys`不存在，您可以複製`~/.ssh/identity.pub`檔案到另一部機器的`~/.ssh/authorized_keys`檔案。
4. 假如您是使用GNOME的桌面環境，請跳過本章節至 15.3.4.4節，假如您並不是使用GNOME，請跳過本章節至 15.3.4.5節。

### 15.3.4.4. 在GNOME中設定ssh-agent

`ssh-agent`工具可以使用來儲存您的通行密碼，所以您便不需在每次啟動`ssh`或`scp`連線時輸入通行密碼。假如您是使用GNOME，`openssh-askpass-gnome`工具可以用來當您登入GNOME時提示您輸入您的通行密碼，並儲存它直到您登出GNOME。在該GNOME作業階段中所作的任何`ssh`或`scp`連線，都將不需要您輸入您的密碼或通行密碼。假如您不是使用GNOME，請參考 15.3.4.5節。

如要在GNOME 作業階段儲存您的通行密碼，請遵照以下的步驟：

1. 系統需要安裝了 `openssh-askpass-gnome` 套件，您可以使用 `rpm -q openssh-askpass-gnome` 以檢查它是否已經安裝了。假如沒有的話，請從您的 Red Hat Linux 光碟套裝或是從 Red Hat 的 FTP 映射站台，或是使用 Red Hat Network 來安裝它。
2. 請選擇『主選單按鈕』（面板上）=>『偏好設定』=>『更多偏好設定』=>『作業階段』，然後點選『初始啟動程式』的真籤。點選**新增**然後在『初始啟動指令』的文字欄輸入 `/usr/bin/ssh-add`。請設定它的次序號碼高於任何已有的指令，以確保它是最後才執行的。在此建議您將 `ssh-add` 次序號碼設為70 或以上，次序號碼越高，它的執行順序越後面。假如在此您尚有其他程式，這個程式應該是最後才執行。請點選**關閉**以離開這個程式。
3. 先登出然後再登入GNOME；也就是說，重新啟動X。在GNOME 啟動後，會出現一個對話窗提示您輸入您的通行密碼，請輸入正確的通行密碼。假如您有設定DSA 與RSA 金鑰環，您將會被提示兩次。從此開始，您將不再被 `ssh`, `scp` 或 `sftp` 提示輸入密碼了。

#### 15.3.4.5. 設定ssh-agent

`ssh-agent` 可以使用來儲存您的通行密碼，所以您便不需要在每次建立 `ssh` 或 `scp` 連線時輸入密碼。假如您不是使用X 視窗系統，請在shell 提示符號下執行這些步驟；假如您是使用GNOME，而您不想設定為在登入時提示您輸入通行密碼（請看 15.3.4.4 節），這個程序可以使用在終端機視窗中（如XTerm）。假如您正在執行X 而不是GNOME，這個程序也可使用在終端機視窗。然而您的通行密碼只適用於該終端機視窗，而不適用於全域的設定。

1. 在shell 提示符號下輸入以下指令：  

```
exec /usr/bin/ssh-agent $SHELL
```
2. 然後再輸入這個指令：  

```
ssh-add
```

然後輸入您的通行密碼。假如您有設定一個以上的金鑰對，您將會收到每一個的提示要求輸入密碼。
3. 當您登出後，您的通行密碼將會被釋放，當您每次登入到一個虛擬主控台或開啟一個終端機視窗，您必須執行這兩個指令。

## 15.4. 其他的資源

OpenSSH 與OpenSSL 專案是處於經常性的開發狀態，在它們的網站便可取得關於它們最新的資訊。OpenSSH 與OpenSSL 工具的man page 也是詳細資訊的很好來源。

### 15.4.1. 已安裝的說明文件

- `ssh`, `scp`, `sftp`, `sshd` 與 `ssh-keygen` 的man pages — 這些man pages 包含如何使用這些指令的資訊以及所有它們可以使用的參數。

### 15.4.2. 很有用的網站

- <http://www.openssh.com> — OpenSSH FAQ 的網頁、程式錯誤報告、郵遞論壇、專案目標以及關於安全性特色的一個較技術性的解釋。
- <http://www.openssl.org> — OpenSSL FAQ 的網頁、郵遞論壇以及專案目標的描述。

- <http://www.freessh.org> — 用於其他平台的SSH 用戶端軟體。

## 網路檔案系統(NFS)

網路檔案系統(NFS) 是一種在網路中的機器間分享檔案的方式，所分享的檔案就好像放置在用戶端本機的硬碟上一樣。Red Hat Linux 可以當作一部NFS 伺服器以及一部NFS 用戶端機器，也就是說它可以匯出檔案系統給其他的系統，以及掛載由其他機器所匯出的檔案系統。

### 16.1. 為何要使用NFS？

NFS 在同一網路中的許多使用者間共享檔案的目錄是很有用的，舉例來說，一組從事同一專案的使用者可以使用NFS 檔案系統中的一個共享目錄（一般稱為NFS 共享），並將之掛載在本機的/myproject 目錄下來存取該專案的檔案。如要存取共享的檔案，使用者必須進入本機機器上的/myproject 目錄，並不需要輸入密碼或指令，使用者將會覺得這個目錄就好像存在本機的機器上一樣。

### 16.2. 掛載NFS 檔案系統

使用mount 指令來掛載另一部機器上一個共享的NFS 目錄：

```
mount shadowman.example.com:/misc/export /misc/local
```



警告

本機上的掛載點目錄（以上例子中的/misc/local）必須存在。

在這個指令中，shadowman.example.com 就是NFS 檔案伺服器的主機名稱，/misc/export 就是shadowman 主機所匯出的目錄，而/misc/local 就是用來掛載到本機的位置。在執行mount 指令之後（而且該用戶端也必須擁有適當的權限存取shadowman.example.com NFS 伺服器），用戶端的使用者便可執行ls /misc/local 指令來列出位於shadowman.example.com 主機上的/misc/export 目錄中的檔案。

#### 16.2.1. 使用/etc/fstab 來掛載NFS 檔案系統

另一個從其他機器掛載一個NFS 共享資源的方法是增加一行到/etc/fstab 檔案中，該行必須含有NFS 伺服器的主機名稱、該伺服器所匯出的目錄以及要掛載NFS 共享的本機目錄。您必須以root 身份才能修改/etc/fstab 檔案。

The general syntax for the line in /etc/fstab 檔案中該行的一般語法如下：

```
server:/usr/local/pub /pub nfs rsize=8192,wsiz=8192,timeo=14,intr
```

掛載點/pub 必須存在於用戶端機器中。在將此行加入到用戶端系統的/etc/fstab 檔案後，請在shell 提示符號下輸入mount /pub，將會從伺服器掛載共享目錄到/pub 掛載點下。

#### 16.2.2. 使用autofs 掛載NFS 檔案系統

用來掛載NFS 共享的第三個選擇是使用autofs，Autofs 使用automount 系統程式來管理您的掛載點，只在當它們被存取時才動態地掛載它們。

Autofs 藉由查閱主要對應設定檔案/etc/auto.master 以決定定義了那些掛載點，然後便啟動一個automount 的程序，並含有對於每一個掛載點的適當參數。主要對應檔案中的每一行都定義一個掛載點，而另一個對應檔案則定義要掛載到此掛載點的檔案系統。舉例來說，/etc/auto.misc 檔案也許定義在/misc 目錄的掛載點；這個對應關係將會定義在/etc/auto.master 檔案中。

auto.master 檔案中的每一項紀錄都有三個欄位，第一個欄位是掛載點，第二個欄位是對應檔案的位置，而三個欄位則是可不輸入的。第三個欄位可以包含例如逾時數值的資訊。

舉例來說，如果要掛載遠端機器penguin.example.net 上的/proj52 目錄到您機器的/misc/myproject 掛載點，請將下列這一行加入到auto.master 檔案中：

```
/misc /etc/auto.misc --timeout 60
```

增加下列這一行至/etc/auto.misc 檔案中：

```
myproject -rw,soft,intr,rsize=8192,wsize=8192 penguin.example.net:/proj52
```

/etc/auto.misc 檔案的第一個欄位是/misc 子目錄的名稱，這個目錄是由automount 動態建立的，它不應該實質上存在於用戶端機器上，第二個欄位包含掛載選項，如rw 代表允許讀取與寫入的存取，第三個欄位就是NFS 所匯出的位置，包括主機名稱與目錄。



#### 請注意

/misc 目錄必須存在於本機的檔案系統中，而且/misc 目錄下不應該含有任何的子目錄。

Autofs 是一項服務，如要啟動這個服務，請在shell 提示符號下輸入下列指令：

```
/sbin/service autofs restart
```

如要檢視現行的掛載點，請在shell 提示符號下輸入下列指令：

```
/sbin/service autofs status
```

假如您在autofs 執行中的情況下修改/etc/auto.master 設定檔案，您必須shell 提示符號下輸入下列指令來告知automount 系統程式重新載入：

```
/sbin/service autofs reload
```

如要學習關於如何設定在開機時啟動autofs，請參考第14章 以取得管理服務的資訊。

### 16.3. 匯出NFS 檔案系統

從一部NFS 伺服器分享檔案稱為匯出目錄，可以使用NFS 伺服器設定工具 來設定系統當作一部NFS 伺服器。

如要使用NFS 伺服器設定工具，您必須執行X 視窗系統，並擁有root 的權限，且已安裝redhat-config-nfs RPM 套件。如要啟動該應用程式，請選擇面板上的『主選單按鈕』=> 『系統設定』=> 『伺服器設定』=> 『NFS 伺服器』，或輸入redhat-config-nfs 指令。



圖形16-1. NFS 伺服器設定工具

如要新增一個NFS 共享，請點選**新增** 按鈕，將會出現如圖形16-2 所示的對話窗。

『基本的』標籤頁需要下列的資訊：

- **目錄** — 指定要分享的目錄，如/tmp。
- **主機** — 指定可以共享這個目錄的主機，請參考 16.3.2 節 以取得可用格式的解釋。
- **基本權限設定** — 指定該目錄是否為僅能讀取或可讀寫的權限設定。



圖形16-2. 新增共享

您可以在『一般選項』的標籤頁中設定下列的選項：

- **允許大於埠號1024 的連線** — 在1024 以下的埠號啟動的服務，必須由root 才能啟動，選取這個選項以使得非root 的使用者也可以啟動NFS 服務，這個選項等同於insecure。
- **允許非安全的檔案鎖定** — 不需要一個鎖定要求，這個選項等同於insecure\_locks。
- **停用subtree 的檢查** — 假如匯出檔案系統的一個子目錄，不過並不匯出整個檔案系統，伺服器將會檢查所要求的檔案是否在所匯出的子目錄中，這種檢查稱為『subtree 的檢查』，選取這個選項以停

用subtree的檢查。假如匯出整個檔案系統，選取停用subtree的檢查將可增加傳輸速率。這個選項等同於no\_subtree\_check。

- **要求同步寫入操作** — 預設已啟用，在要求所做的變更寫入到磁碟上前，這個選項不允許伺服器對要求做出回應。這個選項等同於sync，假如沒有選擇這個選項，則使用async選項。
- **強制立即同步寫入操作** — 不延遲寫入磁碟，這個選項等同於no\_wdelay。

您可以在『使用者存取』的標籤頁中設定下列選項：

- **視遠端的root使用者為本機的root** — 預設情況下，root的使用者與群組IDs都是0，Root squashing對應使用者ID 0與群組ID 0為匿名的使用者與群組IDs，使得用戶端上的root沒有NFS伺服器上的root權限。假如已選擇這個選項，root並不對應到匿名使用者，而且用戶端機器上的root也會擁有匯出目錄的root權限。藉由選取這個選項將會大大地降低系統的安全性，除非有絕對的需要，請勿選取它，這個選項等同於no\_root\_squash。
- **視所有的用戶端使用者為匿名的使用者** — 假如有選取這個選項，所有的使用者與群組ID都對應到匿名的使用者。這個選項等同於all\_squash。
  - **為匿名的使用者指定本機的使用者ID** — 假如有選取『視所有的用戶端使用者為匿名的使用者』選項，這個選項使您可以為匿名的使用者指定一個使用者ID。這個選項等同於anonuid。
  - **為匿名的使用者指定本機的群組ID** — 假如有選取『視所有的用戶端使用者為匿名的使用者』選項，這個選項使您可以為匿名的使用者指定一個群組ID。這個選項等同於anongid。

如要修改一個既有的NFS共享，請從清單中選取它，再點選**屬性**的按鈕。如要刪除一個既有的NFS共享，請從清單中選取它，再點選**刪除**的按鈕。

在點選**確定**來新增、編輯或刪除清單中的一個NFS共享後，變更將立即生效— 伺服器系統程式將重新啟動，而且舊的設定檔案也儲存為/etc/exports.bak，新的設定將會寫入到/etc/exports檔案中。

**NFS 伺服器設定工具**直接讀取並寫入到/etc/exports設定檔案，因此在使用這個工具之後，您可以手動編輯這個檔案，而且在手動編輯完該檔案後（必須以正確的語法格式修改檔案），也可以使用這個工具來做設定。

### 16.3.1. 命令列設定

假如您較喜歡使用一個文字編輯器來編輯設定檔案，或者您沒有安裝X視窗系統，您可以直接修改設定檔案。

/etc/exports 檔案控制NFS伺服器要匯出的目錄，它的格式如下：

```
directory hostname(options)
```

必須指定的唯一選項是sync或async的其中之一（建議使用sync）。假如您指定sync，在要求所做的變更寫入到磁碟之前，伺服器並不對要求做出回應。

例如：

```
/misc/export speedy.example.com(sync)
```

將允許來自speedy.example.com主機的使用者以預設的僅能讀取權限掛載/misc/export目錄，不過：

```
/misc/export speedy.example.com(rw,sync)
```

將允許來自speedy.example.com主機的使用者以讀寫的權限掛載/misc/export目錄。

請參考 16.3.2節以取得關於可用主機名稱格式的說明。



請參考 *Red Hat Linux 參考手冊* 以取得可以指定的選項清單。



#### 警告

請特別小心 `/etc/exports` 檔案中的空白字元，假如主機名稱與括號中的選項間沒有空白字元，這些選項只適用於該主機名稱，假如有空白存在的話，這些選項則適用於其餘的所有人。舉例來說，請仔細檢查下列這兩個例子：

```
/misc/export speedy.example.com(rw, sync)
/misc/export speedy.example.com (rw, sync)
```

第一行允許來自 `speedy.example.com` 的使用者擁有讀寫的存取權限，而拒絕所有其他的使用者。第二行允許來自 `speedy.example.com` 的使用者擁有僅能讀取的權限（預設值），而允許所有其他人讀寫的存取權限。

每次您更改完 `/etc/exports` 檔案，您必須通知 NFS 系統程式，或使用下列指令來重新載入設定檔案：

```
/sbin/service nfs reload
```

### 16.3.2. 主機名稱的格式

主機可以以下列的形式出現：

- 單一機器— 一個有效的網域名稱（可以被伺服器解析的）、主機名稱（可以被伺服器解析的）或是一個 IP 位址
- 以萬用字元指定一連串的機器— 使用 `*` 或 `?` 字元來指定一個字串符合條件，萬用字元不可與 IP 位址一併使用，然而假如 DNS 的反查詢失敗時，它們也許可以使用。當您使用萬用字元在有效的網域名稱時，點(.)並不包括在萬用字元中。舉例來說，`*.example.com` 包括 `one.example.com`，不過並不包括 `one.two.example.com`。
- IP 網路— 使用 `a.b.c.d/z`，這裡的 `a.b.c.d` 為所屬網路，而 `z` 代表網路遮罩的位元數（如 `192.168.0.0/24`）。另一個可用的格式是 `a.b.c.d/網路遮罩`，這裡的 `a.b.c.d` 代表所屬網路，而網路遮罩代表網路遮罩的數值（如 `192.168.100.8/255.255.255.0`）。
- 網路群組— 以 `@group-name` 格式表示，這裡的 `group-name` 就是NIS網路群組的名稱。

### 16.3.3. 啟動與停止伺服器

在匯出 NFS 檔案系統的伺服器上，必須執行 `nfs` 服務。

使用下列指令來檢視 NFS 系統程式的狀態：

```
/sbin/service nfs status
```

使用下列指令來啟動 NFS 系統程式：

```
/sbin/service nfs start
```

使用下列指令來停止 NFS 系統程式：

```
/sbin/service nfs stop
```

如要在開機時啟動 `nfs` 服務，請使用下列指令：

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

您也可以使用`chkconfig`、`ntsysv` 或**系統服務設定工具**來設定那些服務要在開機時啟動，請參考第14章以取得詳細資訊。

## 16.4. 其他的資源

這個章節探討使用NFS的基本觀念，如需更詳細的資訊，請參考下列的資源。

### 16.4.1. 已安裝的說明文件

- `nfsd`, `mountd`, `exports`, `auto.master` 與 `autofs` 的man page (位於第5 與第8 部份) — 這些man pages 將會列出用於NFS 與autofs 設定檔案的正確語法。

### 16.4.2. 好用的網站

- <http://www.tldp.org/HOWTO/NFS-HOWTO/index.html> — 源自Linux Documentation Project 的*Linux NFS-HOWTO*。

### 16.4.3. 相關的書籍

- 由Hal Stern 撰寫，O'Reilly & Associates, Inc. 出版的*Managing NFS and NIS Services*。

Samba 使用SMB 通訊協定透過一個網路連線來共享檔案與印表機。支援這個通訊協定的作業系統包括Microsoft Windows（透過其中的『[網路上的芳鄰](#)』）、OS/2 與Linux。

## 17.1. 為何使用Samba ?

假如您的網路中有Windows 與Linux 的機器，Samba 將可發揮它的功效。使用samba 可以使網路中的所有系統共享檔案與印表機，假如您只是想在Red Hat Linux 機器間共享檔案，請使用如第16章 所討論的NFS。假如您只是想要在Red Hat Linux 機器間共享印表機，您並不需要使用Samba，請您參考第27章。

## 17.2. 設定一部Samba 伺服器

預設的設定檔案(/etc/samba/smb.conf) 使得使用者可以以一個Samba 共享資源的方式檢視他們的Red Hat Linux 家目錄，也分享在Red Hat Linux 系統上設定好的任何印表機為Samba 共享印表機。也就是說，您可以連接一部印表機到您的Red Hat Linux 系統，然後從網路上的Windows 機器進行列印。

### 17.2.1. 圖形化的設定

如要使用一個圖形介面來設定Samba，請您使用**Samba 伺服器設定工具**。至於命令列的設定方式，請翻閱至 17.2.2 節。

**Samba 伺服器設定工具** 是用來管理Samba 共享資源、使用者與基本伺服器設定的一個圖形化介面。它將同時修改位於/etc/samba/ 目錄中的設定檔案，而且將會保留任何非使用這個應用程式所做的變更。

如要使用這個應用程式，您必須執行X 視窗系統，並擁有root 權限，而且已經安裝了redhat-config-samba RPM 套件。如要從桌面啟動**Samba 伺服器設定工具**，請選擇面板上的『[主選單按鈕](#)』=>『[系統設定](#)』=>『[伺服器設定](#)』=>『[Samba 伺服器](#)』，或在shell 提示符號（如XTerm 或GNOME 終端機）下輸入redhat-config-samba 指令。



圖形17-1. Samba 伺服器設定工具



**請注意**

**Samba 伺服器設定工具** 並不顯示共享的印表機，以及允許使用者檢視Samba 伺服器上的使用者家目錄的預設設定。

### 17.2.1.1. 配置伺服器設定

設定Samba 伺服器的第一步是為伺服器配置基本的設定以及一些安全性的選項。在啟動這個應用程式後，請從程式選單選擇『**偏好設定**』=>『**伺服器設定**』，將會顯示如圖形17-2 所示的『**基本設定**』標籤頁。



圖形17-2. 配置基本的伺服器設定

在『**基本設定**』的標籤頁中，請指定這個電腦所屬的工作群組，以及關於這部電腦的一個簡短的描述。這兩個欄位等同於smb.conf 設定檔中的workgroup 與server string 選項。



圖形17-3. 配置伺服器的安全性設定

『安全性設定』標籤頁含有下列的選項：

- **認證模式** — 等同於security 選項，請選取下列認證模式的其中之一。
  - **網域** — Samba 伺服器將倚賴一部Windows NT 的網域主控站或網域備份控制站來驗證使用者。伺服器傳送使用者名稱與密碼到控制站，然後等候回應。請在『**認證伺服器**』的欄位指定網域主控站或網域備份控制站的NetBIOS 名稱。  
假如有選擇這個選項的話，必須設定『**密碼加密**』的選項為『是』。
  - **伺服器** — Samba 伺服器藉由傳送使用者名稱與密碼的結合到另一部Samba 伺服器以試著來驗證它們。假如不可行的話，伺服器將會使用使用者認證模式來做驗證。請在『**認證伺服器**』的欄位指定另一部Samba 伺服器的NetBIOS 名稱。
  - **共享** — 對每一部Samba 伺服器，Samba 使用者並不需要輸入使用者名稱與密碼的組合。除了他們試著要連線到一個特定的共享目錄，他們將不會被提示要求輸入使用者名稱與密碼。
  - **使用者** — (預設值) 對每一部Samba 伺服器，Samba 使用者必須提供一組有效的使用者名稱與密碼。假如您想要使用『**Windows 使用者名稱**』的選項，請選取這個選項，請參考 17.2.1.2 節以取得更詳細資訊。
- **密碼加密** — (預設值為『是』) 假如用戶端從一部Windows 98, Windows NT 4.0(Service Pack 3) 或其他更新版本的Microsoft Windows 進行連線的話，必須啟用這個選項。在伺服器與用戶端間是以加密格式來傳輸密碼，而不是以可被他人截取的純文字字元。這個選項等同於encrypted passwords 選項。請參考 17.2.3 節以取得關於加密Samba 密碼的更多資訊。
- **Guest 帳號** — 當使用者或guest 使用者登入到一部Samba 伺服器，必須對應他們到伺服器上一個有效的使用者。請選取系統上一個既有的使用者名稱來當作guest Samba 帳號。當guest 登入到Samba 伺服器時，他將與該使用者擁有相同的權限。這個設定等同於guest account 選項。

在點選**確定**後，所做的變更將寫入到設定檔案，而且也將會重新啟動系統程式，因此變更將立即生效。

### 17.2.1.2. 管理Samba 使用者

在新增一個Samba 使用者之前，**Samba 伺服器設定工具** 需要作為Samba 伺服器的Red Hat Linux 系統上有一個可使用的既有使用者帳號。Samba 使用者與既有的Red Hat Linux 使用者帳號是相關聯的。



圖形17-4. 管理Samba 使用者

如要新增一個Samba 使用者，請從程式選單選擇『偏好設定』=>『Samba 使用者』，再點選**新增使用者**的按鈕。在『**建立新的Samba 使用者**』視窗中，從本機系統上既有的使用者清單選取一個『**Unix 使用者名稱**』。

假如該使用者在Windows 機器上擁有另一個不同的使用者名稱，而且該使用者將Windows 機器登入到Samba 伺服器，請在『**Windows 使用者名稱**』的欄位指定一個Windows 使用者名稱。在『**伺服器設定**』選項中的『**安全性設定**』標籤頁裡的『**認證模式**』必須設定為『**使用者**』才能使這個選項發生作用。

還要為Samba 使用者設定一個『**Samba 密碼**』，並且再輸入一次以做確認。即使您選擇為Samba 使用加密的密碼，還是建議您讓所有使用者的Samba 密碼與他們的Red Hat Linux 系統之密碼不相同。

如要編輯一個既有的使用者，請從清單中選取該使用者，再點選**編輯使用者**的按鈕。如要刪除一個既有的使用者，請選取該使用者，再點選**刪除使用者**的按鈕。刪除一個Samba 使用者並不會刪除相關的Red Hat Linux 使用者帳號。

再點選**確定** 按鈕後，將立即修改使用者的資訊。

### 17.2.1.3. 新增共享



圖形17-5. 新增共享

如要新增一個共享，請點選**新增** 的按鈕，在『**基本設定**』的標籤頁中可以設定下列選項：

- **目錄** — 透過Samba 共享的目錄，該目錄必須存在。
- **描述** — 關於共享資源的簡單描述。

- **基本權限設定** — 設定使用者對共享目錄的存取權限，包括『只能讀取』與『讀取/寫入』。

在『**存取控制**』的標籤頁中，請選擇是否要允許指定的使用者或所有的Samba 使用者存取共享資源。假如您選擇要允許指定的使用者存取，請從Samba 使用者的清單中選擇使用者。

在點選**確定** 按鈕後，將立即新增該共享資源。

### 17.2.2. 命令列設定方式

Samba 使用/etc/samba/smb.conf 當作它的設定檔案，假如您對這個檔案做任何的變更，在您使用service smb restart 指令重新啟動Samba 系統程式前，變更將不會生效。

如要指定Windows 的工作群組以及關於該Samba 伺服器的簡短描述，請編輯在smb.conf 檔案中的下列幾行：

```
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
```

請以這部機器所屬的Windows 工作群組名稱取代WORKGROUPNAME，BRIEF COMMENT ABOUT SERVER 是可輸入的，是用來當作Windows 中關於Samba 系統的註解。

如要在您的Linux 系統中建立一個Samba 的共享資源，請將下列的部份加入到您的smb.conf 檔案中（請依照您的需求與系統狀況來修改）：

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
writable = yes
printable = no
create mask = 0765
```

以上的例子會允許使用者tfox 與carole 從一部Samba 用戶端進行讀取與寫入Samba 伺服器上的/home/share 目錄。

### 17.2.3. 密碼加密

在Red Hat Linux 9 中，對密碼進行加密是預設啟用的，因為這樣較安全。假如沒有使用加密的密碼，則會使用純文字的密碼，這樣將會有被他人使用網路封包探測器截取的危險。因此建議您使用加密的密碼。

Microsoft SMB 通訊協定原本是使用純文字的密碼，然而Windows NT 4.0（含有Service Pack 3 以上），Windows 98, Windows 2000, Windows ME 以及Windows XP 則需要加密的Samba 密碼。如要在一部Red Hat Linux 系統與一部執行其中一種Windows 作業系統的系統間使用Samba，您可以編輯Windows 的系統登錄來使用純文字密碼或是設定Linux 系統上的Samba 來使用加密的密碼。假如您選擇要修改您的系統登錄，您必須在所有的Windows 機器上進行修改— 這是很危險的，並且也許會導致更多的系統衝突狀況。建議您使用加密的密碼以提供較佳的安全性。

如要在您的Red Hat Linux 系統上設定Samba 使用加密的密碼，請遵照這些步驟：

1. 為Samba 建立另一個密碼檔案，如要以現有的/etc/passwd 檔案為基礎來建立，請在shell 提示符號下輸入以下指令：

```
cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
```

假如系統使用NIS，請輸入下列指令：

```
ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
```

mk smbpasswd.sh 命令稿是由samba 套件安裝在您的 /usr/bin 目錄下。

- 請更改Samba 密碼檔的權限設定，以使得只有root 才擁有讀取與寫入的權限：  
`chmod 600 /etc/samba/smbpasswd`
- 該命令稿並不複製使用者密碼到一個新的檔案，而且在為其設定一個密碼之前，Samba 的使用者帳號是無法使用的。為了更高的安全性起見，建議您採用與使用者Red Hat Linux 密碼不同的Samba 使用者密碼。如要設定每一個Samba 使用者的密碼，請使用下列指令（以每一個使用者名稱取代username）：  
`smbpasswd username`
- 在Samba 的設定檔案中必須啟用加密的密碼設定，請再一次確認這個smb.conf 檔案中的下列這些行沒有加上註解符號：  
`encrypt passwords = yes`  
`smb passwd file = /etc/samba/smbpasswd`
- 請在shell 提示符號下輸入service smb restart 指令以確定smb 服務已經啟動。
- 假如您想要自動啟動smb 服務，您可以使用ntsysv, chkconfig 或系統服務設定工具 在啟動時啟用它。請參考第14章 以取得更詳細資訊。



#### 建議

請閱讀 /usr/share/doc/samba-<版本>/docs/htmldocs/ENCRYPTION.html 來學習更多關於密碼加密的資訊（請以所安裝之Samba 的版本號碼取代<版本>）。

當您使用passwd 指令時，可以使用pam\_smbpass PAM 模組來同步使用者的Samba 密碼與他們的系統密碼。假如一個使用者執行passwd 指令，他使用來登入Red Hat Linux 系統的密碼以及他必須提供來連線到一個Samba 共享資源的密碼都將會更改。

如要啟用這個特色，請將下列這一行加入到/etc/pam.d/system-auth 檔案中的pam\_cracklib.so 部份之下：

```
password required /lib/security/pam_smbpass.so nullok use_authtok try_first_pass
```

### 17.2.4. 啟動與停止伺服器

在透過Samba 分享目錄的伺服器上，必須執行smb 服務。

以下列指令來檢視Samba 系統程式的狀態：

```
/sbin/service smb status
```

使用下列指令啟動系統程式：

```
/sbin/service smb start
```

使用下列指令停止系統程式：

```
/sbin/service smb stop
```

如要在開機時啟動smb 服務，請使用下列指令：

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

您也可以使用chkconfig, ntsysv 或系統服務設定工具 來設定要在開機時啟動的服務，請參考第14章 以取得詳細資訊。



### 17.3. 連線到一個Samba 共享資源

如要從一部Microsoft Windows 機器連線到一部Linux 的Samba 共享，請使用『**網路上的芳鄰**』或圖形化的檔案管理員。

如要從一部Linux 系統上連線到一個Samba 共享，請在shell 提示符號下輸入下列指令：

```
smbclient //hostname/sharename -U username
```

以您想要連線到的Samba 伺服器主機名稱或IP 位址取代`hostname`，以您想要瀏覽的共享目錄名稱取代`sharename`，並以系統上的Samba 使用者名稱取代`username`。再來請輸入正確的密碼或按下[Enter] 按鍵（假如該使用者不需要輸入密碼的話）。

假如您看到`smb:\>` 提示符號，表示您已經成功登入。在您登入後，請輸入`help` 以取得您可以使用的指令清單。假如您想要瀏覽家目錄的內容，請以您的使用者名稱取代`sharename`，假如沒有使用`-U` 的指令參數，目前使用者的使用者名稱將會被傳送至Samba 伺服器。

如要離開`smbclient`，請在`smb:\>` 提示符號下輸入`exit`。

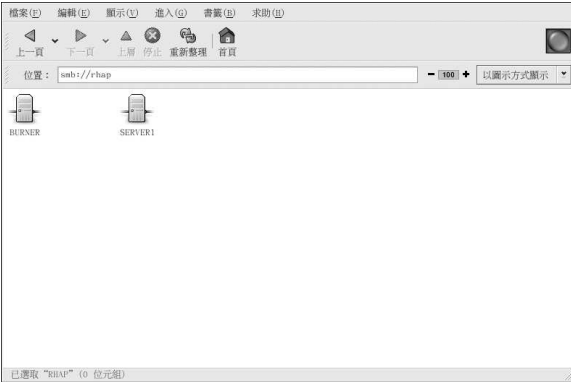
您也可以使用**Nautilus** 來檢視您的網路上可用的Samba 共享資源。請選擇面板上的『**主選單按鈕**』=>『**網路伺服器**』來檢視您網路中的Samba 工作群組。您也可以Nautilus 的『**位置：**』列輸入`smb:` 來檢視工作群組。

如圖形17-6 所示，網路中每一個Samba 工作群組都會以一個圖示出現。



圖形17-6. Nautilus 中的SMB 工作群組

以滑鼠雙點選工作群組的圖示來檢視該工作群組中的電腦清單。



圖形17-7. Nautilus 中的SMB 機器

如您於圖形17-7 所見，工作群組中的每一部機器都以一個圖示來代表，雙點選機器的圖示將可檢視該機器上的Samba 共享資源。假如需要一組使用者名稱與密碼，則會提示您輸入。

或者您可以在『位置：』列上使用以下的語法指定一組使用者名稱與密碼（以適當的數值取代`user`，`password`，`servername` 與`sharename`）：

```
smb://user:password@servername/sharename/
```

## 17.4. 其他的資源

至於在此沒提到的設定選項，請參考下列的資源。

### 17.4.1. 已安裝的說明文件

- `smb.conf` 的man page — 解釋如何配置Samba 的設定檔案
- `smbd` 的man page — 說明Samba 系統程式如何運作
- `/usr/share/doc/samba-<版本號碼>/docs/` — samba 套件所收錄的HTML 與文字檔說明檔案

### 17.4.2. 好用的網站

- <http://www.samba.org> — Samba 的官方網站包含很有用的說明文件、郵遞論壇的資訊以及GUI 介面的列表。

## 動態主機設定協定(DHCP)

動態主機設定協定(Dynamic Host Configuration Protocol - DHCP) 是用來自動指派TCP/IP 資訊給用戶端機器的一種網路協定，每一個DHCP 的用戶端都連線至中心位置的DHCP 伺服器以取得該用戶端的網路設定資訊，包括IP 位址、閘道器以及DNS 伺服器。

### 18.1. 為什麼要使用DHCP ?

DHCP 可用來快速的傳輸用戶端的網路設定，在設定用戶端系統時，系統管理員可以選擇DHCP，並不需要輸入一個IP 位址、網路遮罩、閘道器或DNS 伺服器，用戶端會從DHCP 伺服器取得這些資訊。假如系統管理員想要變更大量系統的IP 位址，DHCP 將會很有用，他可以只編輯伺服器上的一個DHCP 設定檔案使之含有新的IP 位址組，而不用重新設定所有的系統。假如一間公司改變他們的DNS 伺服器，只需在DHCP 伺服器上做這個變更，而不是在DHCP 用戶端上。一旦用戶端重新啟動網路（或者重新開機），變更將會立即生效。

再者，假如一部筆記型電腦或任何的手提電腦設定為DHCP，只要每一個辦公室都有一部DHCP 伺服器，您便可以帶著它到各個辦公室即可連線上網。

### 18.2. 設定一部DHCP 伺服器

您可以使用/etc/dhcpd.conf 設定檔案來設定DHCP 伺服器。

DHCP 也使用/var/lib/dhcp/dhcpd.leases 檔案來儲存用戶端的租賃資料庫。請參考 18.2.2 節以取得更多資訊。

#### 18.2.1. 設定檔案

設定DHCP 伺服器的第一個步驟是建立用來儲存用戶端網路資訊的設定檔案。您也可以宣告適用於所有用戶端的全域性選項，或者是對每一部用戶端系統宣告選項。

設定檔案可以含有任何多餘的跳位字元格或空白行列以美化格式。關鍵字是有分辨大小寫的，而以井字號(#)開頭的行列會被視為註解。

目前已實作兩種DNS 更新的機制— ad-hoc DNS 更新模式與interim DHCP-DNS 相互牽引更新模式。當這兩個被接受為IETF 標準過程的一部分時，將會出現第三個模式— 標準的DNS 更新模式。DHCP 伺服器必須設定來使用目前這兩種機制的其中之一。3.0b2pl11 與之前的版本使用ad-hoc 模式；然而這個模式已經過時了。假如您想要保留相同的行為模式，增加下列這一行到設定檔案的頂端：

```
ddns-update-style ad-hoc;
```

如要使用建議的模式，請加入以下這一行到設定檔案的頂端：

```
ddns-update-style interim;
```

請閱讀dhcpd.conf 的man page，以取得關於不同模式的細節。

設定檔案中有兩種類型的描述：

- 參數(Parameters) — 陳述如何執行一項工作、是否要執行一項工作，或者要傳送何種網路設定選項到用戶端。
- 宣告(Declarations) — 描述網路的拓樸、描述用戶端、提供用戶端的位址或套用一組參數到一組宣告中。

有些參數必須以關鍵字`option` 開頭，並且被當成是`options`，`options` 用來設定DHCP的選項；然而參數是用來設定非可選的數值或控制DHCP 伺服器的操作行為。

在以大括號括住的區間之前宣告的參數（包括`options`）被認為全域性的參數。全域性的參數將會套用於所有其下的部份。



#### 重要

假如您更改設定檔案，所做的變更在使用`service dhcpd restart` 指令重新啟動DHCP 系統程式後才會生效。

在範例18-1 中，`routers`，`subnet-mask`，`domain-name`，`domain-name-servers` 與`time-offset` 選項是使用在任何於其下宣告的`host` 描述。

如範例18-1 所示，您可以宣告一個`subnet`。您必須包含一個`subnet` 的宣告在網路中的每一個子網路，假如沒有的話，DHCP 伺服器將無法啟動。

在這個例子中，有宣告適用於子網路中每一個DHCP 用戶端的全域性選項以及一個`range`。用戶端將會被指派`range` 之間的一個IP 位址。

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    option routers      192.168.1.254;
    option subnet-mask  255.255.255.0;

    option domain-name "example.com";
    option domain-name-servers 192.168.1.1;

    option time-offset  -18000; # Eastern Standard Time

    range 192.168.1.10 192.168.1.100;
}
```

#### 範例18-1. 子網路宣告

共享同一實體網路的所有子網路都應該在如範例18-2 所示的`shared-network` 的聲明中宣告。位於`shared-network` 以內以及在`subnet` 聲明以外的參數被認為全域性的參數。`shared-network` 的名稱必須是網路的一個描述性稱呼，例如`test-lab` 來代表在一個測試實驗室環境中的所有子網路。

```
shared-network name {
    option domain-name      "test.redhat.com";
    option domain-name-servers ns1.redhat.com, ns2.redhat.com;
    option routers          192.168.1.254;
    more parameters for EXAMPLE shared-network
    subnet 192.168.1.0 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.1 192.168.1.31;
    }
    subnet 192.168.1.32 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.33 192.168.1.63;
    }
}
```

#### 範例18-2. Shared-network 聲明

如範例18-3 的例子，group 的聲明可以使用來套用全域性的參數到一組聲明中。您可以群集共享的網路、子網路、主機或其他群組。

```
group {
  option routers          192.168.1.254;
  option subnet-mask      255.255.255.0;

  option domain-name      "example.com";
  option domain-name-servers 192.168.1.1;

  option time-offset      -18000; # Eastern Standard Time

  host apex {
    option host-name "apex.example.com";
    hardware ethernet 00:A0:78:8E:9E:AA;
    fixed-address 192.168.1.4;
  }

  host raleigh {
    option host-name "raleigh.example.com";
    hardware ethernet 00:A1:DD:74:C3:F2;
    fixed-address 192.168.1.6;
  }
}
```

### 範例18-3. Group 聲明

如要設定一部DHCP 伺服器以租賃一個動態的IP 位址給子網路中的一部系統，請以您的數值修改範例18-4。它將宣告一個預設的租賃期間、最大的租賃期間以及用戶端的網路設定數值。這個範例將指派介於192.168.1.10 與192.168.1.100 range 中的IP 位址給用戶端系統。

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";

subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.100;
}
```

### 範例18-4. Range 參數

如要基於網路介面卡的MAC 位址來指派一個IP 位址給一部用戶端，請在host 的聲明中使用hardware ethernet 參數。如範例18-5 範例所示，host apex 聲明指定使用MAC 位址00:A0:78:8E:9E:AA 的網路介面卡總是接收192.168.1.4 這個IP 位址。

請注意您也可以使用可選的參數host-name 來指定一個主機名稱給一部用戶端。

```
host apex {
    option host-name "apex.example.com";
    hardware ethernet 00:A0:78:8E:9E:AA;
    fixed-address 192.168.1.4;
}
```

### 範例18-5. 使用DHCP的靜態IP位址



#### 建議

您可以使用範例設定檔案在Red Hat Linux 9 當作一個起始點，然後再加入您自己的設定選項。請使用以下指令來複製它到適當的位置。

```
cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf
```

(這裡的<version-number> 就是您所使用的DHCP 版本)。

如需要一個完整的選項聲明清單，以及它們的用途，請參考dhcp-options 的man page。

### 18.2.2. 租賃資料庫

在DHCP 伺服器中，`/var/lib/dhcp/dhcpd.leases` 檔案儲存DHCP 用戶端的租賃資料庫。您不能手動地修改這個檔案。DHCP 對每一個近期指派IP 位址的租賃資訊都會自動地儲存在租賃資料庫中。這些資訊包括租賃的長度、IP 位址欲指派的對象、租賃開始與結束的日期以及用來擷取租賃之網路介面卡的MAC 位址。

在租賃資料庫中的所有時間都是格林威治標準時間(GMT)，而不是本地時間。

租賃資料庫是經常建立的，因此它的容量並不大。一開始，所有已知的租賃都儲存在一個暫時的租賃資料庫中。`dhcpd.leases` 檔案會重新命名為`dhcpd.leases~`，而暫時的租賃資料庫則寫入到`dhcpd.leases`。

在租賃資料庫被重新命名為備份檔案後，且在新檔案被寫入之前，DHCP 系統程式也許會被中斷或者系統當機，如果發生這種情況的話，系統將缺少必要的`dhcpd.leases` 檔案來啟動這項服務。在此情況下，請勿建立新的租賃檔案，假如您試著建立的話，所有舊有的租賃資訊都將遺失，並且會導致很多問題。正確的解決方法是重新命名`dhcpd.leases~` 備份檔案為`dhcpd.leases`，然後重新啟動系統程式。

### 18.2.3. 啟動與停止伺服器



#### 重要

在您第一次啟動DHCP 伺服器時，將會失敗，除非有一個既有的`dhcpd.leases` 檔案。假如該檔案不存在的話，請使用`touch /var/lib/dhcp/dhcpd.leases` 指令來建立這個檔案。

如要啟動DHCP 服務，請使用`/sbin/service dhcpd start` 指令。如要停止DHCP 伺服器，請使用`/sbin/service dhcpd stop` 指令。假如您想要系統程式在開機時自動啟動，請參閱第14章 以取得如何管理服務的更多資訊。

假如您的主機含有一片以上的網路介面卡，不過您只想要在其中一個介面卡上啟動DHCP 伺服器，您可以設定DHCP 伺服器只在該裝置上啟動。請在`/etc/sysconfig/dhcpd` 檔案中加上該介面卡的名稱到DHCPDARGS 的清單中：

```
# Command line options here
DHCPDARGS=eth0
```

當您有一部含有兩片網路卡的防火牆機器時，這個選項將對您很有用處。您可以設定一片網路卡當作DHCP的用戶端來擷取網際網路中的一個IP位址，而另一片網路卡則可使用來當作在防火牆裡面之內部網路的DHCP伺服器。只指定連線至內部網路的網路卡將使得系統更加安全，因為使用者將無法透過網際網路連線至該系統程式。

其他可以在`/etc/sysconfig/dhcpd`指定的命令列選項包括：

- `-p <portnum>` — 指定dhcp要聽取的udp連接埠號，預設值是埠號67。DHCP伺服器以比所指定之udp埠號多一號的埠號傳輸回應到DHCP用戶端。舉例來說，假如您接受預設埠號67，伺服器將會聽取埠號67的要求，並以埠號68作出回應。假如您在此指定一個連接埠，並且使用DHCP轉接代理(relay agent)，您必須指定相同的連接埠以使DHCP轉接代理來聽取。請看 18.2.4 節 以取得細節。
- `-f` — 執行該系統程式為一個前景的程序，這最常用在除錯階段。
- `-d` — 紀錄DHCP伺服器系統程式到標準的錯誤描述符，這個選項大都用在除錯階段。假如沒有指定這個，紀錄檔將會寫入到`/var/log/messages`。
- `-cf filename` — 指定設定檔案的位置，預設位置為`/etc/dhcpd.conf`。
- `-lf filename` — 指定租賃資料庫檔案的位置。假如一個租賃資料庫檔案已經存在，每當DHCP伺服器啟動時，必須要使用相同的檔案，這是相當重要的。在此強烈建議您只在非用於生產的系統上除錯時才使用這個選項。預設的位置為`/var/lib/dhcp/dhcpd.leases`。
- `-q` — 啟動系統程式時不要列出整個著作權的訊息。

### 18.2.4. DHCP 轉接代理

DHCP轉接代理(dhcrelay)讓您可以轉接來自一個沒有DHCP伺服器之子網路的DHCP與BOOTP要求到到其他子網路中一個或更多的DHCP伺服器。

當一部DHCP用戶端要求資訊時，DHCP轉接代理將傳送要求到DHCP轉接代理啟動時所指定的DHCP伺服器清單。當DHCP伺服器傳回一個回應時，該回應將在原始要求所送出的網路中廣播或單點傳播。

DHCP轉接代理會聽取所有介面上的DHCP要求，除非在`/etc/sysconfig/dhcrelay`中有指定該介面，且含有INTERFACES指令。

如要啟動DHCP轉接代理，請使用`service dhcrelay start`指令。

## 18.3. 設定一部DHCP用戶端

設定DHCP用戶端的第一個步驟是先確定核心能夠辨識網路介面卡。大部分的卡都可在安裝過程中被辨識，而且系統也會為該介面卡設定使用正確的核心模組。假如您在安裝過程後才安裝新的介面卡，**Kudzu**<sup>1</sup>應該會找到它，並且提示您為其設定相對應的核心模組。請確定您有查看過位於<http://hardware.redhat.com/hcl/>的Red Hat Linux 硬體相容清單。假如網路卡無法透過安裝程式或**Kudzu**來設定，而您知道要載入那一個核心模組，請參考第31章以取得關於載入核心模組的細節。

如要手動設定一部DHCP用戶端，您需要修改`/etc/sysconfig/network`檔案以啟用網路連線，以及位於`/etc/sysconfig/network-scripts`目錄中每一個網路裝置的設定檔案。在這個目錄中，每一個裝置都應該有一個名為`ifcfg-eth0`的設定檔案（這裡的`eth0`為網路裝置的名稱）。

`/etc/sysconfig/network`檔案應該包含下列這一行：

```
NETWORKING=yes
```

1. **Kudzu** 是在系統開機時執行的一種硬體偵測工具，以決定何種硬體已經加入或從系統移除。

在這個檔案中，也許含有更多的資訊，不過NETWORKING 變數必須設為yes，如果您想要在開機時啟動網路連線的話。

/etc/sysconfig/network-scripts/ifcfg-eth0 檔案應該要包含以下這一行：

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

您需要一個設定檔案給每一個您想要設定來使用DHCP的裝置。

假如您較喜歡使用圖形介面來設定DHCP用戶端，請參考第12章以取得藉由**網路管理工具**來設定使用DHCP的一個網路介面。

## 18.4. 其他的資源

關於這裡未討論到的設定選項，請參考以下的資源。

### 18.4.1. 已安裝的說明文件

- dhcpd的man page — 描述DHCP系統程式如何運作
- dhcpd.conf的man page — 解釋如何設定DHCP設定檔案（包括一些範例）
- dhcpd.leases的man page — 解釋如何設定DHCP的租賃檔案（包括一些範例）
- dhcp-options的man page — 解釋在dhcpd.conf檔案中宣告DHCP選項的語法（包括一些範例）
- dhcrelay的man page — 說明DHCP轉接代理以及它的設定選項。



## Apache HTTP 伺服器設定

在Red Hat Linux 8.0 中，Apache HTTP 伺服器已經更新為使用不同設定選項的2.0 版本。並且從Red Hat Linux 8.0 開始，它的RPM 套件也重新命名為httpd。假如您想要手動轉換一個既有的設定檔案，請參考在/usr/share/doc/httpd-<ver>/migration.html 的轉換手冊或*Red Hat Linux* 參考手冊 以取得更詳細資訊。

假如您在之前版本的Red Hat Linux 使用**HTTP 設定工具** 來設定Apache HTTP 伺服器，然後再執行一個升級，您可以使用這個應用程式來轉換設定檔案到2.0 版本的新格式。啟動**HTTP 設定工具**，做任何需要的變更，然後儲存它。所儲存的設定檔案將可與2.0 版本相容。

**HTTP 設定工具** 可幫您為Apache HTTP 伺服器配置/etc/httpd/conf/httpd.conf 設定檔案。它並不使用舊式的srm.conf 或access.conf 設定檔案，並將它們留空。透過圖形化的介面，您可以設定例如虛擬主機、紀錄屬性以及最大連線數等的指令。

只有Red Hat Linux 所包括的模組才能使用**HTTP 設定工具** 做設定，假如有安裝其他的模組，將無法使用這個工具來設定它。

必須已安裝httpd 與redhat-config-httpd RPM 套件才能使用**HTTP 設定工具**。這個程式也需要X 視窗系統與root 存取權限。如要啟動這個應用程式，請選擇『**主選單按鈕**』=> 『**系統設定**』=> 『**伺服器設定**』=> 『**HTTP 伺服器**』，或在shell 提示符號（如XTerm 或GNOME 終端機）下輸入redhat-config-httpd 指令。



### 警告

假如您希望使用這個工具，請勿手動編輯/etc/httpd/conf/httpd.conf 設定檔案，在儲存您的設定並且離開程式後，**HTTP 設定工具** 將會產生這個檔案。假如您想要增加**HTTP 設定工具** 所缺少的額外模組或設定選項，您則不能使用這個工具。

使用**HTTP 設定工具** 來配置Apache HTTP 伺服器的一般步驟如下：

1. 在『**主要**』標籤頁中配置基本的的設定。
2. 點選『**虛擬主機**』的標籤頁來配置預設的設定。
3. 在『**虛擬主機**』的標籤頁設定預設的虛擬主機。
4. 假如您想要伺服一個以上的URL 或虛擬主機，請增加額外的虛擬主機。
5. 在『**伺服器**』的標籤頁配置伺服器的設定。
6. 在『**調整效能**』的標籤頁配置連線設定。
7. 複製所有需要的檔案到DocumentRoot 與cgi-bin 目錄下。
8. 離開這個應用程式，並選擇儲存您的設定。

### 19.1. 基本設定

使用『**主要**』的標籤頁配置基本的伺服器設定。



圖形19-1. 基本的設定

請在『**伺服器名稱**』的欄位輸入您有權使用的一個有效網域名稱。這個選項等同於在`httpd.conf` 檔案中的`ServerName` 指令。`ServerName` 的指令是用來設定網頁伺服器的主機名稱，當您要建立轉址時，便會使用到它。假如您沒有定義一個伺服器名稱，網頁伺服器將會試著從系統的IP 位址來進行解析。這裡的伺服器名稱並不一定要是從伺服器的IP 位址解析得來的網域名稱。例如當您伺服器真實的DNS 名稱為`foo.example.com`，您也許會想要設定伺服器名稱為`www.example.com`。

請在『**Webmaster 的電子郵件地址**』欄位輸入負責維護網頁伺服器之網頁管理員的電子郵件地址。這個選項等同於`httpd.conf` 檔案中的`ServerAdmin` 指令。假如您設定要含括一個電子郵件地址在伺服器的錯誤頁面，則會使用這個電子郵件地址，使得使用者可以傳送電子郵件到伺服器的管理人員以回報所遇到的問題。預設值是`root@localhost`。

使用『**可使用的位址**』區域來定義伺服器用來接受進入要求的連接埠號。這個選項等同於`httpd.conf` 檔案中的`Listen` 指令。預設情況下，Red Hat 會配置Apache HTTP 伺服器監聽埠號80 上的非安全的網頁連線。

點選**新增**的按鈕來定義用來接受要求的額外埠號，將會出現如圖形19-2 所示的一個視窗，您可以選擇『**監聽所有位址**』的選項來監聽所定義之連接埠上的所有IP 位址，或者在『**位址**』欄位指定一個伺服器將接受連線的特定IP 位址。在每一個連接埠號只能指定一個IP 位址，如果您想要在相同的連接埠號上指定一個以上的IP 位址，請為每一個IP 位址個別建立一個紀錄。在此請盡量使用IP 位址，而不要使用網域名稱，以避免DNS 搜尋失敗。請參考<http://httpd.apache.org/docs-2.0/dns-caveats.html> 以取得關於**Issues Regarding DNS and Apache** 的更多資訊。

在『**位址**』的欄位輸入一個星號(\*)相當於選擇『**監聽所有位址**』的選項。在『**可使用的位址**』區域點選**編輯** 按鈕將會出現與點選**新增** 按鈕相同的視窗，除了欄位中已經含有選取的紀錄。如要刪除一項紀錄，請選取它，再點選**刪除** 的按鈕。



#### 建議

假如您設定伺服器要監聽低於1024 連接埠號，您則必須是`root` 才能啟動它，至於1024 (含以上) 的連接埠號，則可以由一般的使用者啟動。



圖形19-2. 可用的位址

## 19.2. 預設設定

在定義完『伺服器名稱』、『Webmaster 的電子郵件地址』與『可用的位址』之後，請點選『虛擬主機』的標籤頁，再點選**編輯預設設定**的按鈕，將會出現如圖形19-3所示的視窗。請在此配置網頁伺服器的預設設定。假如您新增一個虛擬主機，您為該虛擬主機配置的設定將會優先於該虛擬主機。至於虛擬主機中未定義的指令，將會使用預設值。

### 19.2.1. 站台設定

『目錄頁搜尋清單』與『錯誤頁』的預設設定將可使用再大部份的伺服器上，假如您不確定這些設定，請勿修改它們。



圖形19-3. 站台設定

在『目錄頁搜尋清單』所列出的紀錄將用來定義DirectoryIndex指令。當使用者在一個目錄名稱的最後指定一個斜線符號來要求一個目錄的索引時，DirectoryIndex便是伺服器所伺服的預設網頁。

舉例來說，當使用者要求[http://www.example.com/this\\_directory/](http://www.example.com/this_directory/)網頁時，他們將會取得DirectoryIndex的網頁（如果存在的話），或者一個伺服器產生的目錄清單。伺服器將會試著尋找DirectoryIndex指令所列出的檔案，而且將會傳回第一個找到的檔案。假如找不到任何的這些

檔案，而且該目錄有設定 `Options Indexes`，伺服器將會產生並傳回該目錄中的子目錄與檔案的清單（以 HTML 格式表示）。

當發生問題或錯誤時，可以使用『**錯誤碼**』部份來設定 Apache HTTP 伺服器重導用戶到一個本地或外部的 URL。這個選項 `ErrorDocument` 指令。當用戶試著要連線到 Apache HTTP 伺服器時，假如發生一個問題或錯誤，預設的動作便是顯示如『**錯誤碼**』欄位所示的簡短錯誤訊息。如要強制覆寫這個預設設定，請選取一個錯誤碼並點選 **編輯** 按鈕，選擇『**預設值**』以顯示預設的簡短錯誤訊息；選擇『**URL**』來重導用戶到一個外部的 URL，並且在『**位置**』的欄位輸入包括 `http://` 的一個完整 URL；選擇『**檔案**』來重導用戶到一個內部的 URL，並且輸入網頁伺服器中 `document root` 下的檔案位置，這個位置必須以一個斜線開頭，並且必須相對於 `Document Root`。

舉例來說，如要重導一個『**404 - 找不到**』的錯誤碼到一個您所建立稱為 `404.html` 的檔案，請複製 `404.html` 檔案到 `DocumentRoot/errors/404.html`。在這裡，`DocumentRoot` 為您所定義的 `Document Root` 目錄（預設值是 `/var/www/html`）。然後選擇『**檔案**』當作『**404 - 找不到**』錯誤碼的行為，並且在『**Location**』欄為輸入 `/errors/404.html`。

從『**預設錯誤的頁尾**』選單，您可以選擇下列的其中一種選項：

- **顯示含有電子郵件地址的檔尾** — 在所有錯誤頁的底部顯示預設的檔尾加上在 `ServerAdmin` 指令所指定之網站維護者的電子郵件地址。請參考 19.3.1.1 節以取得更多關於設定 `ServerAdmin` 指令的更多資訊。
- **顯示檔尾** — 在錯誤頁的底部只顯示預設的檔尾。
- **缺少檔尾** — 在錯誤頁的底部不顯示檔尾。

### 19.2.2. 紀錄檔

預設情況下，伺服器將寫入傳輸紀錄到 `/var/log/httpd/access_log` 檔案，而寫入錯誤紀錄到 `/var/log/httpd/error_log` 檔案。

傳輸紀錄檔中包含了所有試圖存取網頁伺服器的清單，它紀錄了試圖連線的用戶 IP 位址、存取的日期與時間以及用戶試著要擷取網頁伺服器中的檔案。請輸入要儲存這些資訊的目錄與檔案名稱，假如這個目錄與檔案名稱並不是以斜線開頭，這個路徑必須是相對於所設定的伺服器根目錄。這個選項等同於 `TransferLog` 指令。

The screenshot shows the 'Log' configuration window. On the left, a sidebar lists '網站設定', '紀錄檔' (selected), '環境變數', and '目錄'. The main area is divided into '轉換紀錄' and '錯誤紀錄' sections. In '轉換紀錄', '紀錄至檔案 (L):' is set to 'logs/access\_log'. In '錯誤紀錄', '紀錄至檔案 (L):' is set to 'logs/error\_log'. Below these, '紀錄等級 (V):' is set to 'Error' and '反向 DNS 搜尋 (D):' is set to '反向搜尋'. At the bottom, there are buttons for '求助 (H)', '確定 (O)', and '取消 (C)'.

圖形19-4. 紀錄檔

您可以藉由選取『**使用慣有的紀錄工具**』並且在『**自訂紀錄字串**』的欄位輸入一個自訂的紀錄字串，來設定一個自訂的紀錄格式。這將會設定LogFormat指令，請參考 [http://httpd.apache.org/docs-2.0/mod/mod\\_log\\_config.html#formats](http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formats) 以取得關於這個指令的格式。

錯誤紀錄檔包含了所發生的任何伺服器錯誤清單，請輸入要儲存這些資訊的目錄與檔案名稱，假如這個目錄與檔案名稱並不是以斜線開頭，這個路徑必須是相對於所設定的伺服器根目錄。這個選項等同於ErrorLog指令。

使用『**紀錄等級**』的選單來設定錯誤紀錄檔中錯誤訊息的詳細情況。在此您可以設定它為（從最簡短到最詳細）Emergency, Alert, Critical, Error, Warn, Notice, Info 或Debug。這個選項等同於LogLevel指令。

『**反向DNS搜尋**』的選單所選擇的數值將定義HostnameLookups指令。選擇『**非反向尋找**』將設定這個數值為關閉(off)；選擇『**反向搜尋**』將設定這個數值為開啟(on)；而選擇『**雙重反向尋找**』將設定這個數值為雙重的(double)。

假如您選擇『**反向搜尋**』，您的伺服器將會自動解析每一個要求您伺服器中文件之連線的IP位址。解析IP位址表示您的伺服器將會建立連線到DNS找出對應到一個特定IP位址的主機名稱。

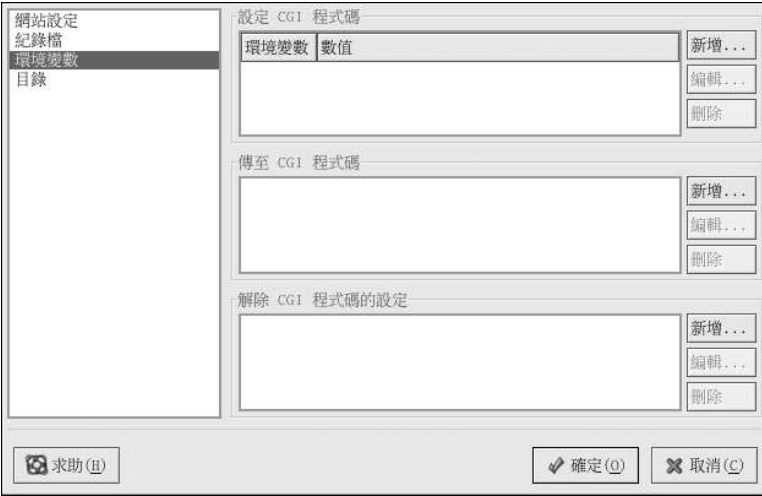
假如您選擇『**雙重反向尋找**』，您的伺服器將會執行一個雙重反向的DNS，也就是說，在執行一次反向搜尋之後，將在結果執行一次正向搜尋。在正向搜尋的結果中，至少要有一個IP位址符合第一次反向搜尋的位址。

一般來說，您應該要將這個選項設定為『**非反向尋找**』，因為DNS的要求將會增加您伺服器的負載，而且也許會使其變慢。假如您的伺服器很繁忙，試著要執行這些反向搜尋或雙重反向搜尋所造成的影響將會很明顯。

對整體來說，反向搜尋與雙重反向搜尋也將為網際網路產生一個令人不得不注意的議題。所有單一連線對其主機名稱的搜尋將產生很大的負載。因此為了您自己的網頁伺服器與網際網路的彼此利益，您應該將這個選項設為『**非反向尋找**』。

### 19.2.3. 環境變數

有時候有必要為CGI程式碼或server-side include (SSI) 網頁修改環境變數，Apache HTTP 伺服器可以使用mod\_env模組來設定傳送至CGI程式碼與SSI網頁的環境變數，請使用『**環境變數**』的頁面來設定這個模組的指令。



圖形19-5. 環境變數

使用『設定 CGI 程式碼』的部份來設定傳送至 CGI 程式碼與 SSI 網頁的一個環境變數。舉例來說，如要設定 MAXNUM 環境變數為 50，請點選如圖形 19-5 所示『設定 CGI 程式碼』部份旁邊的**新增**按鈕，然後在『環境變數』的欄位輸入 MAXNUM，在『設定的數值』欄位輸入 50。點選**確定**來增加它到清單中。『設定 CGI 程式碼』的部份將設定 SetEnv 指令。

當伺服器第一次啟動來伺服 CGI 程式碼時，使用『傳至 CGI 程式碼』的部份來傳送一個環境變數的數值。如想得知這個環境變數，請在 shell 提示符號下輸入 env 指令。在『傳至 CGI 程式碼』的部份點選**新增**按鈕，在跳出的對話窗中輸入環境變數的名稱，再點選**確定**來將它加入清單中。『傳至 CGI 程式碼』的部份將設定 PassEnv 指令。

假如您想要移除一個環境變數使得該數值將不會傳送至 CGI 程式碼與 SSI 頁面，請使用『解除 CGI 程式碼的設定』部份，點選『解除 CGI 程式碼的設定』部份的**新增**按鈕，並輸入要取消設定的環境變數名稱，再點選**確定**來將它加入清單中。這個選項等同於 UnsetEnv 指令。

如要編輯任何的這些環境數值，請從清單中選取它，再點選相對應的**編輯**按鈕，如要從清單中刪除任何的紀錄，請選取它，再點選相對應的**刪除**按鈕。

如要學習更多關於 Apache HTTP 伺服器中環境變數的資訊，請參考下列的網站：

<http://httpd.apache.org/docs-2.0/env.html>

#### 19.2.4. 目錄

使用『目錄』的頁面來設定特殊目錄的選項，這個選項等同於 <Directory> 指令。



圖形19-6. 目錄

點選右上角的**編輯** 按鈕來為其下『目錄』清單中未指定的所有目錄設定『**預設目錄選項**』。您所選擇的選項會被列出當作<Directory> 指令中的 **Options** 指令。您可以設定下列的選項：

- **ExecCGI** — 允許執行CGI 程式碼，假如沒有選擇這個選項，將無法執行CGI 程式碼。
- **FollowSymLinks** — 允許遵循符號連結。
- **Includes** — 允許server-side includes(SSI).
- **IncludesNOEXEC** — 允許server-side includes(SSI)，不過停用CGI 程式碼中的#exec 與#include 命令。
- **Indexes** — 假如在被要求的目錄中沒有DirectoryIndex (例如index.html) 的話，則顯示目錄內容的一個格式化清單。
- **Multiview** — 支援content-negotiated 的多重檢視(multiviews)，這個選項預設是停用的。
- **SymLinksIfOwnerMatch** — 假如目的檔案或目錄與連結屬於相同的擁有者，只遵循符號連結。

如要為特定的目錄指定選項，請點選『目錄』清單部份旁邊的**新增** 按鈕，將會出現如圖形19-7 所示的視窗，請在視窗底端的『目錄』文字欄位輸入要設定的目錄。請選取右邊清單的選項，並以左邊的選項設定Order 指令。Order 指令控制評估允許與拒絕指令的順序。在『**允許的主機名稱**』與『**拒絕主機來自**』的文字欄位，您可以指定下列的其中一個：

- 允許所有主機— 輸入**all** 以允許對所有主機的存取。
- 部份的網域名稱— 允許與所指定之網域名稱字串名稱相符的所有主機。
- 完整的IP 位址— 允許對一個特定IP 位址的存取。
- 一個子網路— 例如**192.168.1.0/255.255.255.0**
- 一個網路的CIDR 指定— 例如**10.3.0.0/16**

順序

讓所有使用者存取此目錄(L)

先過濾拒絕清單，然後過濾允許清單(D)

先過濾允許清單，然後過濾拒絕清單(A)

拒絕名單

拒絕所有主機的存取

拒絕主機來自:

允許名單

允許所有主機的存取

允許的主機名稱:

目錄:

選項

ExecCGI

FollowSymLinks

Includes

IncludesNOEXEC

Indexes

MultiViews

SymLinksIfOwnerMatch

使 .htaccess 檔優先於目錄選項

圖形19-7. 目錄設定

假如您選取『使.htaccess 檔優先於目錄選項』，在.htaccess 檔案中的設定指令將會優先考量。

### 19.3. 虛擬主機設定

您可以使用**HTTP 設定工具**來設定虛擬主機，虛擬主機的設定可以讓您在同一部機器上執行不同位址、不同主機名稱或不同連接埠的多部伺服器。舉例來說，您可以使用虛擬主機在同一部機器上執行http://www.example.com 與http://www.anotherexample.com 等兩個網站。對於預設虛擬主機以及IP 為主的虛擬主機，這個選項等同於<VirtualHost> 指令；而對於一個名稱為主的虛擬主機，這個選項等同於<NameVirtualHost> 指令。

為一部虛擬主機設定的指令只適用於該部特定的虛擬主機，假如一個指令是使用**編輯預設設定**的按鈕來做全域性的設定，而且並沒有在虛擬主機的設定中定義，將會使用預設的設定。舉例來說，您可以在『**主要**』的標籤頁中定義一個『**Webmaster 的電子郵件地址**』，而不用在每一個虛擬主機中定義個別的電子郵件地址。

如圖形19-8 所示，**HTTP 設定工具**含有一個預設的虛擬主機。





圖形19-8. 虛擬主機

<http://httpd.apache.org/docs-2.0/vhosts/> 與您機器上的 Apache HTTP 伺服器說明文件提供了關於虛擬主機更多的資訊。

### 19.3.1. 新增與編輯一個虛擬主機

如要新增一個虛擬主機，請點選『**虛擬主機**』標籤頁中的**新增** 按鈕。您也可以清單中選取一個您要修改的虛擬主機，再點選**編輯** 的按鈕，來修改一個虛擬主機的設定。

#### 19.3.1.1. 一般選項

『**一般選項**』的設定只適用於您要設定的虛擬主機，在『**虛擬主機名稱**』的欄位設定虛擬主機的名稱，這個名稱是由**HTTP 設定工具** 使用來辨別虛擬主機的。

為這個虛擬主機設定『**文件檔所在目錄**』的數值為包含最底層文件檔（如index.html）。這個選項等同於 `<VirtualHost>` 指令下的 `DocumentRoot` 指令。在 Red Hat Linux 7 之前，Red Hat Linux 所提供的 Apache HTTP 伺服器使用 `/home/httpd/html` 當作 `DocumentRoot`。然而在 Red Hat Linux 9 中，預設的 `DocumentRoot` 為 `/var/www/html`。

『**網站管理員的電子郵件地址**』選項等同於 `VirtualHost` 指令中的 `ServerAdmin` 指令。假如您選擇要在錯誤頁顯示含有一個電子郵件地址的頁尾，將會使用這個電子郵件地址在在錯誤頁中的頁尾。

在『**主機資訊**』的部份，請選擇『**預設虛擬主機**』、『**IP 為主的虛擬主機**』或『**名為主的虛擬主機**』。

#### 預設虛擬主機

您只能設定一個預設的虛擬主機（請記得預設已經設定了一個），當所要求的 IP 地址並不在另一個虛擬主機特定地列出，則會使用這個預設的虛擬主機設定。假如沒有定義任何的虛擬主機，則會使用主要的伺服器設定。

#### IP 為主的虛擬主機

假如您選擇『**IP 為主的虛擬主機**』，將會出現一個視窗用來設定以伺服器 IP 地址為主的 `<VirtualHost>` 指令。請在『**IP 地址**』的欄位指定這個 IP 地址，如要指定多個 IP 地址，請以空白將每一個 IP 地址隔開。如要指定連接埠號，請使用『**IP 地址:連接埠**』的格式，使用 `*` 來設定該 IP 地址的所有連接埠，在『**伺服器主機名稱**』的欄位指定該虛擬主機的主機名稱。

### 名稱為主的虛擬主機

假如您選擇『名稱為主的虛擬主機』，將會出現一個視窗用來設定以伺服器主機名稱為主的NameVirtualHost指令。請在『IP位址』的欄位指定這個IP位址，如要指定多個IP位址，請以空白將每一個IP位址隔開。如要指定連接埠號，請使用『IP位址:連接埠』的格式，使用:\*來設定該IP位址的所有連接埠，在『伺服器主機名稱』的欄位指定該虛擬主機的主機名稱。在『別名』的區域，點選新增來增加一個主機名稱的別名，如在此新增一個別名將會增加NameVirtualHost指令中的ServerAlias指令。

### 19.3.1.2. SSL



#### 請注意

您無法在名稱為主的虛擬主機設定使用SSL，因為SSL的handshake（當瀏覽器接受安全網頁伺服器的憑證時）會發生在HTTP要求（用來辨識適當之名稱為主的虛擬主機）之前。假如您想要使用名稱為主的虛擬主機，它們則只能使用在非安全的網頁伺服器。

一般選項	<input checked="" type="checkbox"/> 啟用 SSL 支援 (E)
網站設定	
SSL	
紀錄檔	
環境變數	
目錄	
	SSL 設定
	憑證檔案 (F): /etc/httpd/conf/ssl.crt/server.crt
	憑證金鑰檔案 (K): /etc/httpd/conf/ssl.key/server.key
	憑證連鎖檔案 (C): /etc/httpd/conf/ssl.crt/ca.crt
	憑證授權檔案 (A): /etc/httpd/conf/ssl.crt/ca-bundle.crt
	SSL 紀錄檔案 (L): logs/ssl_engine_log
	SSL 紀錄等級 (v): Info
	SSL 選項
	<input type="checkbox"/> FakeBasicAuth
	<input type="checkbox"/> ExportCertData
	<input type="checkbox"/> CompatEnvVars
	<input type="checkbox"/> StrictRequire
	<input type="checkbox"/> OptRenegotiate
<input type="button" value="求助 (H)"/> <input type="button" value="確定 (O)"/> <input type="button" value="取消 (C)"/>	

圖形19-9. SSL 支援

假如一個Apache HTTP 伺服器並沒有設定含有SSL支援，在一部Apache HTTP 伺服器與它的用戶端之間的連線通訊都是沒有經過加密的。這在不含有個人或機密資訊的網站上是比較沒有太大關係的。舉例來說，一個用來散佈開放原始碼軟體與說明文件的開放原始碼網站是不需要安全連線的。然而一個需要顧客輸入信用卡資訊的電子商務網站，便應該要使用Apache的SSL之原來對其通訊進行加密處理。啟用Apache的SSL支援將啟用mod\_ssl安全模組的使用。如要透過HTTP設定工具來啟用它，您必須在『主要』標籤頁=>『可用的位址』中允許透過埠號443的存取。請參考19.1節以得到更多資訊。然後在『虛擬主機』的標籤頁選取虛擬主機的名稱，再點選編輯的按鈕，從左邊的選單選取『SSL』，然後選取如圖形19-9所示的『啟用SSL支援』選項。『SSL設定』的部份已經預先設定好虛設的數位憑證，這個數位憑證為您的安全網頁伺服器提供認證，並使得用戶端的網頁瀏覽器能夠辨識

這部安全伺服器。您必須購買您自己的數位憑證，請勿在您的網站使用 Red Hat Linux 所提供之虛假的數位憑證。如需關於購買一個 CA 認證的數位憑證的詳細資訊，請參考第 20 章。

### 19.3.1.3. 額外的虛擬主機選項

『網站設定』、『環境變數』與『目錄』等虛擬主機的選項是與您點選**編輯預設定**按鈕要設定的相同指令，除了在這裡設定的選項是適用於您正要設定的個別虛擬主機。請參考 19.2 節以取得關於這些選項的詳細資訊。

## 19.4. 伺服器設定

『伺服器』的標籤頁中可以讓您配置基本的伺服器設定，這些選項的預設設定可適用於大部分的狀況。



圖形 19-10. 伺服器設定

『**鎖定檔**』的數值等同於 `LockFile` 指令。當伺服器被編譯使用 `USE_FCNTL_SERIALIZED_ACCEPT` 或 `USE_FLOCK_SERIALIZED_ACCEPT` 時，這個指令用來設定要使用的鎖定檔路徑，它必須是儲存在本機磁碟中，您應該要保留其預設值，除非 `logs` 目錄是位於一個 NFS 共享資源上。假如是這種情況的話，應該要更改預設值為在本機磁碟上的一個位置，且位於一個僅有 `root` 才能讀取的目錄。

『**PID 檔**』的數值等同於 `PidFile` 指令，這個指令設定伺服器用來紀錄它的程序 ID (pid) 的檔案，這個檔案應該只有 `root` 才能讀取。在大部分的情況下，應該要將它保持為預設值。

『**電腦記憶體容量轉儲目錄**』的數值等同於 `CoreDumpDirectory` 指令。Apache HTTP 伺服器會在進行電腦記憶體容量轉儲前，試著轉換到這個目錄下，預設值是 `ServerRoot`。然而，假如執行這個伺服器的使用者無法寫入這個目錄，將無法寫入電腦記憶體容量轉儲。假如您想要寫入電腦記憶體容量轉儲到磁碟上以用作除錯的用途，必須更改這個數值為執行此伺服器的使用者能寫入的目錄。

『**使用者**』的數值等同於 `User` 指令。它設定伺服器用來回應要求的使用者身份。這個使用者的設定將決定伺服器的存取，這個使用者所無法存取的任何檔案也將使得您網站的訪客無法存取。User 的預設值是 `apache`。

這個使用者應該要擁有足夠的權限，以使得它能夠存取要讓外在世界所能看到的檔案。這個使用者也是由伺服器所衍生出任何 CGI 程序的擁有者。這個使用者不應該允許去執行刻意要用來回應 HTTP 要求的任何程式碼。

**警告**

除非您確實知道您在做什麼事情，請勿設定User 指令為root，使用root 當作User 將會為您的網頁伺服器造成相當大的安全漏洞。

在正常操作下，parent httpd 程序先以root 身份執行，不過再來將立即交付給apache 使用者。伺服器必須以root 啟動，因為它需要繫結至1024 以下的埠號。1024 以下的埠號是保留給系統使用的，所以除了root 之外任何人都無法使用它們。然而當伺服器繫結至它的連接埠後，它將在接收任何連線要求前，把程序交付給apache 使用者。

『群組』的數值等同於Group 指令。Group 指令類似User 指令，Group 設定伺服器將用來回應要求的群組。預設的群組也是apache。

## 19.5. 調整效能

點選『調整效能』的標籤頁來設定您想要的伺服器子程序的最大數量，以及設定用戶連線的Apache HTTP 伺服器選項。這些選項的預設設定可適用於大部分的狀況。更改這些設定也許會影響您網頁伺服器整體的效能表現。



圖形19-11. 調整效能

設定『最大連線數』為伺服器可以處理之同一時間用戶要求的最大數目，對於每一個連線，將會建立一個httpd 子程序。在到達這個最大的程序數量時，並且在一個伺服器的子程序被釋放之前，任何人都無法連線至這部網頁伺服器。在沒有重新編譯的情況下，您不能設定這個數值為超過256。這個選項等同於MaxClients 指令。

『連線論時』以秒數定義通訊過程中的接收與傳輸動作，伺服器將等待的時間。明白來說，『連線論時』定義了您的伺服器接收一個GET 要求、一個POST 或PUT 要求的TCP 封包以及在回應TCP 封包的ACKs 之間所等待的時間。預設情況下，『連線論時』設定為300 秒，這對大部分的狀況是很適當的。這個選項等同於Timeout 指令。

設定『單一連線最大的要求數』為允許每一個持續性連線的最大要求數。預設值是100，這對大部分的狀況已經是相當足夠了。這個選項等同於MaxRequestsPerChild 指令。

假如您選取『允許單一連線有無限次的要求』選項，MaxKeepAliveRequests 指令將會設為0，而將會允許無限次的要求。

假如您取消選取『允許永久的連線』選項，KeepAlive 指令將會設定為false；假如您選取它，KeepAlive 指令將會設定為true，而且KeepAliveTimeout 指令將會設定『下一個連線論時』數值所選取的數字。這個指令設定伺服器將等待後續要求（在伺服一個要求之後與關閉連線之前）的秒數。當接收到一個要求時，則轉而套用『連線論時』的數值。

取決於有多少使用者會進行連線，如果設定『**下一個連線論時**』的數值為一個較高的數值，也許會導致伺服器的速度變慢。這個數值越高，在上一個用戶連線之後，將會有更多的伺服器程序等待下一個連線。

## 19.6. 儲存您的設定

假如您不想儲存您的Apache HTTP 伺服器組態設定，請點選**HTTP 設定工具** 視窗右下角的**取消** 按鈕。將會再次提示您以確認這個選擇，假如您點選是，將不會儲存您的設定。

假如您想要儲存您的Apache HTTP 伺服器組態設定，請點選**HTTP 設定工具** 視窗底端的**確定** 按鈕。將會出現一個對話窗，假如您回答是，將會儲存您的設定到/etc/httpd/conf/httpd.conf 檔案。請記得您原本的設定檔案將會被覆寫。

假如這是您第一次使用**HTTP 設定工具**，您將會看到一個對話窗警告您設定檔案曾經被手動更改，假如**HTTP 設定工具** 偵測到httpd.conf 設定檔案已經被手動更改，它將會自動將該檔案另存為/etc/httpd/conf/httpd.conf.bak 檔案。



### 重要

在儲存您的設定後，您必須使用`service httpd restart` 指令重新啟動httpd 系統程式，您必須是root 才能執行這個指令。

## 19.7. 其他的資源

如要了解更多關於Apache HTTP 伺服器的資訊，請參考下列的資源。

### 19.7.1. 已安裝的說明文件

- Apache HTTP 伺服器說明文件— 假如您已經安裝httpd-manual 套件，而且Apache HTTP 伺服器系統程式(httpd) 也正在執行中，您可以檢視Apache HTTP 伺服器的說明文件，請開啟一個網頁瀏覽器，然後連線到執行Apache HTTP 伺服器伺服器的URL `http://localhost`，然後點選**Documentation** 的連結。
- `/usr/share/docs/httpd-<version>` — *Apache Migration HOWTO* 文件涵蓋了從1.3 版到2.0 版的程式更改清單，以及如何手動轉換設定檔案的相關資訊。

### 19.7.2. 好用的網站

- <http://www.apache.org> — Apache 軟體協會
- <http://httpd.apache.org/docs-2.0/> — Apache 軟體協會Apache HTTP 伺服器2.0 版的說明文件，包括『*Apache HTTP 伺服器2.0 版的使用手冊*』。
- <http://localhost/manual/index.html> — 在您的本機系統上啟動Apache HTTP 伺服器之後，您可以使用這個URL 在您的本機系統檢視Apache HTTP 伺服器2.0 版的說明文件。
- [http://www.redhat.com/support/resources/web\\_ftp/apache.html](http://www.redhat.com/support/resources/web_ftp/apache.html) — Red Hat 的技術支援部門維護有用的Apache HTTP 伺服器連結清單。
- <http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html> — 由Red Hat 所編撰的The Red Hat Linux Apache Centralized Knowledgebase。

### 19.7.3. 相關的書籍

- 由Ben Laurie 與Peter Laurie 撰寫；O'Reilly & Associates, Inc. 所出版的*Apache: The Definitive Guide*。
- 由Red Hat, Inc. 出版的*Red Hat Linux* 參考手冊 — 這本手冊涵蓋手動轉換Apache HTTP 伺服器1.3 版到Apache HTTP 伺服器2.0 版的指示，還有關於Apache HTTP 伺服器指令更詳細的資訊，以及增加模組到Apache HTTP 伺服器的指示。

## Apache HTTP 安全伺服器設定

### 20.1. 簡介

這個章節關於將Apache HTTP 伺服器中`mod_ssl` 安全模組啟用以使用OpenSSL 函式庫與工具包的基本資訊。由Red Hat Linux 所提供的這三種組元件的結合在這個章節中被稱為『安全的網頁伺服器』或只是『安全伺服器』(Secure Server)。

`mod_ssl` 模組是Apache HTTP 伺服器的一個安全模組，`mod_ssl` 模組使用OpenSSL 專案提供的工具來增加一個很重要的特色到Apache HTTP 伺服器中——將通訊加密的能力。相反地，使用一般的HTTP (瀏覽器與網頁伺服器間的通訊都是以純文字的方式傳送)，很有可能在瀏覽器與伺服器間的傳輸路線中被其他人截取並讀取。

這個章節並非要提供關於任何的這些程式完整且獨特的說明文件，不過我們將盡可能在這本手冊中向您指出您可以找到更多關於特定主題較深入的說明文件。

這個章節會向您說明如何安裝這些程式，您也可以學習產生一個私鑰與一個憑證要求的必要步驟、如何產生您自己簽署的憑證，以及如何安裝一個憑證以讓您的安全伺服器使用。

`mod_ssl` 設定檔案位於`/etc/httpd/conf.d/ssl.conf`，為了要載入這個檔案，以使`mod_ssl` 能夠運作，您必須在`/etc/httpd/conf/httpd.conf` 檔案中有`Include conf.d/*.conf` 陳述式。在Red Hat Linux 9 中，預設的Apache HTTP 伺服器設定檔案已經預設包含這個陳述式。

### 20.2. 關於安全性相關之套件的簡要

為了啟用安全伺服器，您至少需要安裝下列這些套件：

#### httpd

httpd 套件包含httpd 系統程式與相關的工具程式、設定檔案、圖示、Apache HTTP 伺服器模組、man pages 以及其他由Apache HTTP 伺服器使用的檔案。

#### mod\_ssl

mod\_ssl 套件包含`mod_ssl` 模組，它透過Secure Sockets Layer (SSL) 與Transport Layer Security (TLS) 通訊協定來為Apache HTTP 伺服器提供功能強大的加密法。

#### openssl

openssl 套件包含OpenSSL 工具包，OpenSSL 工具包實作了SSL 與TLS 通訊協定，而且也收錄了一般用途的密碼函式庫。

除此之外，其他Red Hat Linux 所提供的軟體套件也有提供某些安全的功能性（不過並非運作安全伺服器所需的）：

#### httpd-devel

httpd-devel 套件含有Apache HTTP 伺服器的包含檔案、表頭檔案以及APXS 工具。假如您想要載入任何額外的模組（非這個產品所提供的模組），您將需要所有這些檔案與工具。請閱讀*Red Hat Linux* 參考手冊以取得關於使用Apache 的DSO 功能性來載入模組到安全伺服器的更多資訊。

假如您不想要載入其他的模組到您的Apache HTTP 伺服器，您並不需要安裝這個套件。

#### httpd-manual

httpd-manual 套件含有HTML 格式之Apache 專案的*Apache User's Guide*。這本手冊也可在以下網址中取得：<http://httpd.apache.org/docs-2.0/>。

## OpenSSH 套件

OpenSSH 套件提供OpenSSH 的一組網路連線工具，可用來登入到遠端機器與執行指令。OpenSSH 工具加密所有的網路流量（包括密碼），所以您可以避免網路竊聽、連線劫持以及其他在您的機器與遠端機器間的通訊攻擊。

openssh 套件含有OpenSSH 用戶端程式與OpenSSH 伺服器所需的核心檔案。openssh 套件也含有scp，這是rcp（用來在機器間複製檔案）的一個安全的替代品。

openssh-askpass 套件支援在使用OpenSSH agent 時，顯示一個對話窗以讓使用者輸入密碼。

openssh-askpass-gnome 套件可以與GNOME 桌面環境結合，當OpenSSH 程式提示需要密碼時，顯示一個圖形的對話窗。假如您要執行GNOME，而且要使用OpenSSH 工具，您應該要安裝這個套件。

openssh-server 套件含有sshd 安全殼系統程式以及相關的檔案。安全殼系統程式是OpenSSH 套裝的伺服器端，假如您想要允許SSH 用戶端連線到您的主機，您必須安裝它到您的主機。

openssh-clients 套件含有需要用來建立加密連線到SSH 伺服器的用戶端程式，包括以下的這些工具：ssh（rsh 的一個安全替代品）、sftp（用來在機器間傳輸檔案之ftp 的一個安全替代品）、slogin（用於遠端登入之rlogin 的一個安全替代品）以及透過Telnet 通訊協定與另一部主機通訊的telnet。

如需關於OpenSSH 的更多資訊，請參考第15章、*Red Hat Linux 參考手冊* 以及位於<http://www.openssh.com>的OpenSSH 網站。

## openssl-devel

openssl-devel 套件包含編譯含有許多加密機制與通訊協定支援的應用程式所需的靜態函式庫與其他檔案。只當您要開發含有SSL 支援的應用程式，您才需要安裝這個套件— 您並不需要這個套件以使用SSL。

## stunnel

stunnel 套件提供Stunnel SSL 包裹程式，Stunnel 支援TCP 連線的SSL 加密法，所以在不改變系統程式之程式碼的情況下，它可以提供非SSL 相關的系統程式與通訊協定（如POP、IMAP 與LDAP）的加密。

表格20-1 顯示安全伺服器之套件的摘要以及在安裝一個安全伺服器時，該套件是否為可選的。

套件名稱	可選的？
httpd	否
mod_ssl	否
openssl	否
httpd-devel	是
httpd-manual	是
openssh	是
openssh-askpass	是
openssh-askpass-gnome	是
openssh-clients	是
openssh-server	是
openssl-devel	是
stunnel	是



表格20-1. 安全性的套件

### 20.3. 關於憑證與安全的一個概要

您的安全伺服器使用Secure Sockets Layer (SSL) 通訊協定與（在大多的例子中）一個來自Certificate Authority (CA) 的數位憑證之結合來提供安全性。在您的瀏覽器與您的安全伺服器之間，SSL 處理加密的通訊以及互相的認證。CA 認證通過的數位憑證為您的安全伺服器提供認證（CA 放置他們的聲譽在您公司識別身份的憑證之後）。當您的瀏覽器使用SSL 加密法進行通訊時，您將會在瀏覽列看到以https:// 開頭的URL。

加密法依附於金鑰的使用（將之認定為以資料格式表示之機密加密器與解密器）。在傳統或對稱的加密法中，處理的兩端都擁有相同的金鑰，可以使用來解密彼此的傳輸訊息。在公開的或非同步的加密法上，必須並存兩把金鑰：一把公鑰與一把私鑰。個人或公司將他們的私鑰秘密地保存起來，而公開他們的公鑰。以公鑰加密的資料只能以私鑰解密；以私鑰加密的資料僅能以公鑰將其解密。

如要設定您的安全伺服器，請使用公開的加密法來建立一個含有公鑰與私鑰的金鑰環。在大多的例子中，您傳送您的憑證要求（附上您的公鑰）、您公司識別身份的證明以及費用到CA，CA 會驗證您的憑證要求以及您的身份識別，然後傳回您安全伺服器的一個憑證。

一部安全伺服器藉由一個憑證向網頁瀏覽器證明自己的身份，您可以產生您自己的憑證（稱為一個『自我簽署』的憑證），或者您可以從CA 取得一個憑證。一個來自極具聲望之CA 的憑證，將可保證該網站是與一個特定的公司或組織相關的。

另外您也可以建立您自我簽署的憑證，然而請注意，自我簽署的憑證最好不要使用在用作生產的環境中。自我簽署的憑證將無法被使用者的瀏覽器自動接受— 使用者將會被瀏覽器提示是否要接受憑證來建立一個安全的連線。請參考 20.5 節 以取得關於自我簽署與CA 簽署憑證之相異處的更多資訊。

一旦您擁有一個自我簽署的憑證或一個來自您選擇之CA 簽署的憑證，您需要安裝它到您的安全伺服器。

### 20.4. 使用之前已有的金鑰與憑證

假如您已經有一個既有的金鑰與憑證（例如您要安裝安全伺服器來取代其他公司的安全伺服器），您也許可以在安全伺服器上使用您既有的金鑰與憑證。在以下兩種情況下，您將無法使用您既有的金鑰與憑證：

- 假如您要變更您的IP 位址或網域名稱 — 憑證是根據一對特定的IP 位址與網域名稱所發放的。假如您要變更您的IP 位址或網域名稱，您必須要取得一個新的憑證。
- 假如您有一個來自VeriSign 的憑證，而您想要變更您的伺服器軟體 — VeriSign 是一個被廣泛使用的CA，假如您已經有一個用於其他用途的VeriSign 憑證，您也許有想過要使用您已有的VeriSign 憑證在您新的安全伺服器上，然而，您不允許這麼做，因為VeriSign 是依據一個特定伺服器軟體與IP 位址/網域名稱的組合來發放憑證的。

假如您更改那些參數的其中一種（例如您之前使用一個不同的安全伺服器產品），您取得要使用在之前設定的VeriSign 憑證將無法使用在新的設定上，您必須再申請一個新的憑證。

假如您有一組您可以使用的金鑰與憑證，您並不需要產生一把新的金鑰與取得一個新的憑證，然而您也許需要移動與重新命名含有您金鑰與憑證的檔案。

移動您既有的金鑰到：

```
/etc/httpd/conf/ssl.key/server.key
```

移動您既有的憑證檔案到：

```
/etc/httpd/conf/ssl.crt/server.crt
```

在您已經移動您的金鑰與憑證後，請翻閱至 20.9 節。

假如您是從 Red Hat 的網頁安全伺服器進行升級，您舊的金鑰(`httpsd.key`)與憑證(`httpsd.crt`)是位於 `/etc/httpd/conf/` 目錄下，請移動且重新命名您的金鑰與憑證，以使安全伺服器能夠使用它們。您可以使用下列兩個指令來移動且重新命名您的金鑰與憑證檔案：

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

然後使用下列指令來啟動安全伺服器：

```
/sbin/service httpd start
```

您將被提示輸入您安全伺服器的通行密碼，在您輸入再按下[Enter]鍵後，伺服器將會啟動。

## 20.5. 憑證的種類

假如您從 Red Hat Linux 所提供的 RPM 套件安裝您的安全伺服器，將會產生一把亂數的金鑰以及一個測試(test)的憑證，並且放置到適當的目錄下。然而在您開始使用您的安全伺服器前，您必須產生您自己的金鑰，並取得能夠正確辨識您伺服器的一個憑證。

您需要一把金鑰與一個憑證來運作您的安全伺服器——也就是說，您可以選擇要產生一個自我簽署的憑證或從一個 CA 購買一個 CA 認證的憑證。那麼這兩種有何不同呢？

一個 CA 簽署的憑證為您的伺服器提供兩種重要的功能：

- 瀏覽器（通常）能夠自動辨識憑證，並且在不提示使用者的情況下允許進行安全的連線。
- 當一個 CA 發放一個簽署的憑證時，他們也負責保證提供這個網頁給瀏覽器的組織身份識別。

假如您的安全伺服器大多是被公眾存取，您的安全伺服器需要一個由 CA 簽署的憑證，使得拜訪您網站的人知道該網站是由聲稱擁有它的組織所擁有。在簽署一個憑證之前，CA 會先確認要求憑證之組織確實是該組織。

大部分的支援 SSL 的網頁瀏覽器都有它們自動接受憑證的 CA 清單。假如瀏覽器遇到認證憑證的 CA 不在清單中，瀏覽器將會詢問使用者是否要接受或拒絕連線。

您可以為您的安全伺服器產生一個自我簽署的憑證，不過請特別注意，一個自我簽署的憑證並不提供與一個 CA 簽署之憑證相同的功能性。一個自我簽署的憑證並無法被大部分的網頁瀏覽器自動辨識，而且一個自我簽署的憑證並不對提供該網站之組織身份識別提供任何的保證。一個 CA 簽署的憑證同時為您的安全伺服器提供這兩種重要的功能，假如您的安全伺服器將使用在生產的環境中，您或許需要一個 CA 簽署的憑證。

從一個 CA 取得一個憑證的過程相當簡單，以下有簡單的概要：

1. 建立一組用作加密的私鑰與公鑰金鑰環。
2. 依據公鑰建立一個憑證要求，該憑證要求必須含有關於您伺服器以及管理公司的資訊。
3. 傳送憑證要求並附上證明您身份的文件到一個 CA，我們無法告訴您該選擇那一個憑證機構，您可以根據您之前的經驗或您朋友同事的經驗或者純粹是金錢的因素來做這個決定。  
一旦您決定好一個 CA 後，您將需要遵從他們提供的指示來從他們取得一個憑證。
4. 當 CA 滿意您確實是您本人時，他們將會寄給您一個數位憑證。
5. 安裝這個憑證到您的安全伺服器，然後便可以開始處理安全的通訊。

不管您是從一個 CA 取得一個憑證或產生您自我簽署的憑證，第一個步驟便是產生一把金鑰，請看 20.6 節以取得如何產生一把金鑰的指示。

## 20.6. 產生一把金鑰

您必須是root 才能產生一把金鑰。

首先，cd 到/etc/httpd/conf 目錄，使用下列指令移除安裝過程中產生的虛假金鑰與憑證：

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

下一步，您需要建立您自己的亂數金鑰，請轉換至/usr/share/ssl/certs 目錄再輸入下列指令：

```
make genkey
```

您的系統將會顯示如下的訊息：

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

現在您需要輸入一個通行密碼，為了安全起見，該密碼至少要包含8 個字元，包括數字亦或標點符號，而且不是字典上的字。也請您記得您的通行密碼是有分辨大小寫的。



### 請注意

您需要在每次啟動您的安全伺服器時輸入這個通行密碼，所以請勿忘記它。

請再輸入一次通行密碼以確認它是正確的。當您正確地輸入後，將會建立包含您金鑰的/etc/httpd/conf/ssl.key/server.key 檔案。

請注意，假如您不想要在每次啟動安全伺服器時都要輸入通行密碼，您將需要使用下列這兩個指令（而非make genkey）來建立您的金鑰。

使用下列的指令來建立您的金鑰：

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

然後使用下列的指令以確定該檔案的權限設定是正確的：

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

在您使用以上指令建立您的金鑰後，您將不需要使用一個通行密碼來啟動您的安全伺服器。



### 警告

停用您安全服務器的通行密碼特色會有安全性的考量，因此不建議您停用安全服務器的通行密碼特色。

不使用通行密碼所牽連到的問題會直接關連至主機機器上所維護的安全性。舉例來說，假如一個不擇手段的個人危及主機機器上的一般UNIX 安全設定，那個人也許可以取得您的私鑰（也就是您server.key 檔案的內容），該金鑰可以被使用來伺服似乎來自您安全服務器的網頁。

假如在主機電腦上UNIX的安全性設定是經過嚴格維護的（已安裝所有可用的作業系統修正與更新，且不執行任何非必要或危險的服務等等），安全伺服器的通行密碼也許就不是那麼必要了。然而，因為您的安全伺服器不需要很常重新開機，在大部分的情況下，藉由輸入一個通行密碼以提供額外的安全性是值得的。

`server.key` 檔案應該是由系統上的root使用者所擁有，而且其他任何的使用者絕對不可以存取。請為這個檔案建立一個備份，並將這個備份儲存在一個安全的地方。因為假如您在使用它來建立您的憑證要求後，遺失`server.key`檔案，您將不再能夠使用您的憑證而且CA也無法幫助您，此時您便需要這個備份的副本。您僅有的選擇是要求（並且購買）一個新的憑證。

假如您要從一個CA購買一個憑證，請繼續至 20.7 節；假如您要產生您自我簽署的憑證，請翻閱至 20.8 節。

## 20.7. 產生一個憑證要求以傳送給一個CA

一旦您建立好金鑰後，下一步便是產生一個您需要傳送至您選擇之CA的憑證要求，請確定您位於`/usr/share/ssl/certs`目錄，然後輸入下列指令：

```
make certreq
```

您的系統將會顯示下列的輸出，並且將會向您詢問您的通行密碼（除非您停用通行密碼的選項）：

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

請輸入在產生金鑰時您選擇的通行密碼，您的系統將會顯示一些指示，然後向您詢問一連串的問題。您的輸入將會合併到憑證要求中，系統的顯示（含有範例的答覆）將會如下所示：

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.example.com
Email Address []:admin@example.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

預設的答覆會出現在每一個要求之後的括號[]之間以讓您輸入。例如第一個需要的資訊是將使用該憑證的國家名稱，將會如以下的格式顯示：

```
Country Name (2 letter code) [GB]:
```

括號中預設的輸入為GB，如要接受這個值，請按下[Enter] 鍵，或者填入您國家的兩碼國碼。

您將需要輸入其餘的值，它們應該都是解釋很明白的，不過您需要遵照這些指示：

- 請勿使用地區或州名的縮寫，請將全名寫出（例如St. Louis 應該寫成Saint Louis）。
- 假如您要傳送這個CSR 到一個CA，請特別注意務必在所有欄位提供正確的資訊，特別是Organization Name 與Common Name。CAs 檢查在CSR 中所提供的資訊，來決定您的組織要為您所提供的Common Name 負責。CAs 會拒絕含有他們認為無效資訊的CSRs。
- 至於Common Name，請確定您輸入您安全伺服器的真實名稱（一個有效的DNS 名稱），而且不是您的伺服器所擁有的任何別名。
- Email Address 應該是網站管理員或系統管理員的電子郵件地址。
- 請避免使用任何特殊的字元，如@, #, &, ! 等等。有些CAs 會拒絕含有特殊字元的憑證要求。所以假如您的公司名稱含有一個& 符號，請將它拼成"and"，而不使用"&"。
- 請勿使用任何額外的屬性（A challenge password 與An optional company name）。如要在不輸入任何數值的情況下繼續，您只要按下[Enter] 鍵來接受這兩個欄位空白的預設值。

當您完成輸入您的資訊後，將會建立/etc/httpd/conf/ssl.csr/server.csr 檔案，這個檔案便是您要傳送給CA 的憑證要求。

在您決定好一個CA 之後，請遵照在他們網站上所提供的指示，他們的指示將他們的指示將會告訴您如何傳送您的憑證要求、任何他們需要的其他文件以及您所須付的費用。

在您完成CA 的各種要求後，他們將會傳送一個憑證給您（通常使用電子郵件），將他們傳送給您的憑證儲存（或剪貼）到/etc/httpd/conf/ssl.crt/server.crt 檔案，請記得要備份這個檔案。

## 20.8. 建立一個自我簽署的憑證

您可以建立您自我簽署的憑證，請注意一個自我簽署的憑證並不提供像一個CA 簽署之憑證的安全性保證。請參考 20.5 節以取得關於憑證的更詳細資訊。

假如您想要建立您自我簽署的憑證，首先您必須按照 20.6 節所提供的指示建立一個亂數金鑰。一旦您擁有金鑰後，請確定您是位於/usr/share/ssl/certs 目錄，然後輸入下列的指令：

```
make testcert
```

您將會看到如下的輸出，而且您將會被提示輸入您的通行密碼（除非您產生的金鑰不含通行密碼）：

```
umask 77 ; \  
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key  
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt  
Using configuration from /usr/share/ssl/openssl.cnf  
Enter PEM pass phrase:
```

在輸入您的通行密碼後（或者假如您建立的金鑰不含通行密碼），您將會被問及以提供更多的資訊，電腦的輸出以及一組輸出將會如下所示（您必須提供關於您的組織與主機的正确資訊）：

```
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a  
DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [GB]:US  
State or Province Name (full name) [Berkshire]:North Carolina
```

```

LocalityName (eg, city) [Newbury]:Raleigh
OrganizationName (eg, company) [My Company Ltd]:My Company, Inc.
OrganizationalUnitName (eg, section) []:Documentation
CommonName (your name or server's hostname) []:myhost.example.com
Email Address []:myemail@example.com

```

在您提供完正確的資訊後，一個自我簽署的憑證將會建立在 `/etc/httpd/conf/ssl.crt/server.crt` 檔案。在建立這個憑證之後，您必須使用下列指令來重新啟動您的安全伺服器：

```
/sbin/service httpd restart
```

## 20.9. 測試憑證

如要測試預設安裝的 `test` 憑證、一個 CA 簽署的憑證以及一個自我簽署的憑證，請將您的網頁瀏覽器指向下列的網址（請以您的網域名稱取代 `server.example.com`）：

```
https://server.example.com
```



### 請注意

請特別注意在 `http` 之後的 `s`。 `https`：前置字元是用於安全性的 HTTP 交易處理。

假如您使用來自一個知名的 CA 所簽署的憑證，您的瀏覽器將會自動接受該憑證（不提示使用者），並且建立安全的連線。您的瀏覽器將不會自動辨識一個測試或自我簽署的憑證，因為該憑證不是由一個 CA 所簽署。假如您不是使用來自 CA 的憑證，請遵照瀏覽器所提供的指示來接受這個憑證。

一旦您的瀏覽器接受憑證後，您的安全伺服器將會向您顯示一個預設的首頁。

## 20.10. 存取伺服器

如要存取您安全伺服器，請使用如下的 URL：

```
https://server.example.com
```

您的非安全伺服器可以使用如下的 URL 進行存取：

```
http://server.example.com
```

安全網頁連線的標準連接埠號是 443，而非安全的網頁連線的標準連接埠號則是 80。安全伺服器預設設定會監聽這兩個標準的連接埠號。因此並不需要在 URL 指定埠號（連接埠號已經設定了）。

然而，假如您設定您的伺服器監聽一個非標準的連接埠號（例如除了 80 或 443 之外），因為將要試圖連線到伺服器上的非標準連接埠，所以您必須在每一個 URL 指定連接埠號。

舉例來說，您也許設定您的伺服器讓虛擬主機在非安全的 12331 埠號執行，任何試圖要連線到該虛擬主機的 URL，都必須附加指定連接埠號，下列的 URL 範例試圖要連線到一個監聽 12331 埠號的一部非安全伺服器：

```
http://server.example.com:12331
```

## 20.11. 其他的資源

請參考 19.7 節 以取得關於 Apache HTTP 伺服器的其他資源。

### 20.11.1. 已安裝的說明文件

- `mod_ssl documentation` — 開啟一個網頁伺服器，然後連線至已安裝 `httpd-manual` 套件且執行 Apache HTTP 伺服器之伺服器的 URL `http://localhost/manual/mod/mod_ssl.html`。

### 20.11.2. 好用的網站

- `http://www.redhat.com/mailling-lists/` — 您可以在這個網址訂閱 `redhat-secure-server` 的郵遞論壇。您也可以寄電子郵件到 `<redhat-secure-server-request@redhat.com>`，並且在主旨欄加上 `subscribe` 的字眼來訂閱 `redhat-secure-server` 的郵遞論壇。
- `http://www.modssl.org` — `mod_ssl` 的網站是關於 `mod_ssl` 資訊的絕佳來源，這個網站涵蓋相當多的說明文件，包括位於 `http://www.modssl.org/docs` 的一本 *User Manual*。

### 20.11.3. 相關的書籍

- 由 Ben Laurie 與 Peter Laurie 撰寫；由 O'Reilly & Associates, Inc. 出版的 *Apache: The Definitive Guide* 第二版。





## BIND 組態設定

這個章節假設您對BIND與DNS已經有基本的了解，在此我們將不說明BIND與DNS的基本觀念。這個章節專門解釋如何使用**Bind 設定工具**(redhat-config-bind)來設定基本的BIND伺服器網域。每當您套用變更時，**Bind 設定工具**會建立/etc/named.conf設定檔案以及位於/var/named目錄中的網域設定檔案。

**重要**

請勿編輯/etc/named.conf設定檔案，**Bind 設定工具**會在您套用變更後，自動產生這個檔案。假如您想要配置使用**Bind 設定工具**無法配置的設定，請將它們加入到/etc/named.custom檔案中。

為了要執行**Bind 設定工具**，需要X視窗系統與root存取權限，如要啟動**Bind 設定工具**，請選擇面板上的『主選單按鈕』=>『系統設定』=>『伺服器設定』=>『網域名稱服務』，或在shell提示符號下(XTerm或GNOME終端機)輸入redhat-config-bind指令。



圖形21-1. Bind 設定工具

**Bind 設定工具**配置預設的轄區目錄為/var/named，所有指定的網域檔案都是與這個目錄相關的。在輸入數值後，**Bind 設定工具**也包含了基本的語法檢查，舉例來說，假如一個有效的輸入是一個IP位址，您只允許在這個文字區域輸入數字與句號(.)。

**Bind 設定工具**讓您可以新增一個正解主網域、反解主網域以及一個次網域。在新增完網域後，您可以從如圖形21-1所示的主要視窗中編輯或刪除它們。

在新增、編輯或刪除一個網域後，您必須點選**儲存**的按鈕，或選擇『檔案』=>『儲存』來寫入/etc/named.conf設定檔案以及所有在/var/named目錄中的個別網域檔案。儲存變更也會導致named服務重新載入設定檔案。在離開應用程式前，請選擇『檔案』=>『離開』以儲存變更。

### 21.1. 新增一個正解主網域

如要新增一個正解主網域（也稱為一個primary master），請點選**新增**的按鈕，再選擇『**正解主網域**』，然後在『網域名稱』的文字區域輸入主網域的網域名稱。

將會出現如圖形21-2所示的一個新視窗，並含有下列的選項：

- **名稱** — 在前一視窗所輸入的網域名稱。
- **檔名** — DNS 資料庫檔案的檔名（位於 `/var/named` 目錄中），它是預先設定為網域名稱加上 `.zone`。
- **聯絡資訊** — 主網域主要聯絡人的電子郵件地址。
- **主名稱伺服器(SOA)** — State of authority (SOA) 紀錄。這將指定名稱伺服器為這個網域中最佳的資訊來源。
- **序號** — DNS 資料庫檔案的序號，這個號碼必須在每一次變更檔案後逐次增加，以使得網域的次名稱伺服器可以擷取最新的資料。**Bind 設定工具** 在每次設定變更時會漸次增加這個號碼，您也可以手動來增加這個號碼，只要點選『序號』數值旁的**設定** 按鈕。
- **時間設定** — 『更新週期』、『重試週期』、『有效週期』以及『最小更新週期』TTL(Time to Live) 等數值儲存在DNS 資料庫檔案中，所有的數值都是以秒為單位。
- **紀錄** — 新增、編輯與刪除『主機』、『別名』與『名稱伺服器』等類型的紀錄資源。

圖形21-2. 新增一個正解主網域

必須指定一個『**主名稱伺服器(SOA)**』，而且至少需要指定一個名稱伺服器紀錄（可以點選『**紀錄**』區域中的**新增** 按鈕）。

在設定好正解主網域後，點選**確定** 以回到如圖形21-1 所示的主要視窗，在程式的下拉式選單中點選**儲存** 來寫入到 `/etc/named.conf` 設定檔案以及位於 `/var/named` 目錄中的所有個別的網域檔案，而且使得系統程式重新載入設定檔案。

設定將會在 `/etc/named.conf` 檔案中建立一個類似如下的紀錄：

```
zone "forward.example.com" {
    type master;
    file "forward.example.com.zone";
};
```

也同時建立 `/var/named/forward.example.com.zone` 檔案並且含有以下資訊：

```
$TTL 86400
@ IN SOA ns.example.com. root.localhost (
```

```
2 ; serial
28800 ; refresh
7200 ; retry
604800 ; expire
86400 ; ttl
)

IN NS 192.168.1.1.
```

## 21.2. 新增一個反解主網域

如要新增一個反解主網域，請點選**新增**按鈕並選擇『**反解主網域**』。然後輸入您想要設定之IP位址範圍的前三個數值。舉例來說，假如您要設定IP位址範圍為192.168.10.0/255.255.255.0，請輸入192.168.10在『**IP位址（前三個數值）**』的文字欄位。

會出現如圖形21-3所示的一個新視窗，並含有下列的選項：

1. **IP位址** — 在前一視窗中所輸入的前三個IP位址的數值。
2. **反解IP位址** — 無法編輯的。依據所輸入的IP位址所產生的。
3. **聯絡資訊** — 主網域中主要聯絡人的電子郵件地址。
4. **檔名** — 位於/var/named目錄中的DNS資料庫檔案之檔名。
5. **主名稱伺服器(SOA)** — State of authority (SOA) 紀錄。這將指定名稱伺服器為這個網域中最佳的資訊來源。
6. **序號** — DNS資料庫檔案的序號，這個號碼必須在每一次變更檔案後逐次增加，以使得網域的次名稱伺服器可以擷取最新的資料。**Bind設定工具**在每次設定變更時會漸次增加這個號碼，您也可以手動來增加這個號碼，只要點選『**序號**』數值旁的**設定**按鈕。
7. **時間設定** — 『**更新週期**』、『**重試週期**』、『**有效週期**』以及『**最小更新週期**』TTL(Time to Live)等數值儲存在DNS資料庫檔案中。
8. **名稱伺服器** — 新增、編輯與刪除反解主網域中的名稱伺服器，在此至少需要一個名稱伺服器。
9. **反解位址表** — 位於反解主網域中的IP位址清單以及它們的主機名稱。舉例來說，對於反解主網域192.168.10，您可以新增192.168.10.1與它的主機名稱one.example.com到『**反解位址表**』。主機名稱必須以句號結束，以代表它是一個完整的主機名稱。

反解主域名

IP 位址: 192.168.10

反解 IP 位址: 10.168.192.in-addr.arpa

聯絡資訊(C): root@localhost

檔名(F): 10.168.192.in-addr.arpa.zone

主名稱伺服器 (SOA) (T):

序號: 1 設定(S)...

時間設定(T)...

名稱伺服器

新增(A)

編輯(E)...

刪除(D)

反解位址表

位址	主機或網域

新增(d)...

編輯(l)...

刪除(l)

取消(C) 確定(O)

圖形21-3. 新增一個反解主網域

必須指定一個『主名稱伺服器(SOA)』，而且至少需要指定一個名稱伺服器紀錄（可以點選『名稱伺服器』區域中的**新增**按鈕）。

在設定好反解主網域後，點選**確定**以回到如圖形21-1所示的主要視窗，在程式的下拉式選單中點選**儲存**來寫入到/etc/named.conf 設定檔案以及位於/var/named 目錄中的所有個別的網域檔案，而且使得系統程式重新載入設定檔案。

設定將會在/etc/named.conf 檔案中建立一個類似如下的紀錄：

```
zone "10.168.192.in-addr.arpa" {
    type master;
    file "10.168.192.in-addr.arpa.zone";
};
```

也同時建立/var/named/10.168.192.in-addr.arpa.zone 檔案並且含有以下資訊：

```
$TTL 86400
@ IN SOA ns.example.com. root.localhost (
    2 ; serial
    28800 ; refresh
    7200 ; retry
    604800 ; expire
    86400 ; ttk
)

@ IN NS ns2.example.com.

1 IN PTR one.example.com.
2 IN PTR two.example.com.
```

### 21.3. 新增一個次網域

如要新增一個次網域（也稱為一個secondary master），請點選**新增**的按鈕，再選擇『次網域』，然後在『網域名稱』的文字區域輸入次網域的網域名稱。

將會出現如圖形21-4 所示的一個新視窗，並含有下列的選項：

- **名稱** — 在前一視窗所輸入的網域名稱。
- **主網域清單** — 次網域用來擷取資料的名稱伺服器，在此的每一個數值必須是有效的IP 位址，您只能輸入號碼與句號(.) 到這個文字區域。
- **檔名** — 位於/var/named 目錄中的DNS 資料庫檔案之檔名。



圖形21-4. 新增一個次網域

在設定好次網域後，點選**確定**以回到如圖形21-1 所示的主要視窗，在程式的下拉式選單中點選**儲存**來寫入到/etc/named.conf 設定檔案，而且使得系統程式重新載入設定檔案。

設定將會在/etc/named.conf 檔案中建立一個類似如下的紀錄：

```
zone "slave.example.com" {
    type slave;
    file "slave.example.com.zone";
    masters {
        1.2.3.4;
    };
};
```

當named 從主伺服器下載網域資料後，也同時建立/var/named/slave.example.com.zone 檔案。



當一個使用者登入到 Red Hat Linux 系統，使用者名稱與密碼的組合必須經過確認或認證為一個有效且現行的使用者。有時候用來認證使用者的資訊存放在本機系統，而有時候是使用位於遠端系統的使用者資料庫來做認證。

**網路認證設定工具** 提供一個圖形的介面讓您設定 NIS, LDAP 與 Hesiod 以擷取使用者資訊，以及用來配置 LDAP, Kerberos 與 SMB 當作認證的通訊協定。



#### 請注意

假如您在安裝程式中或使用**安全等級設定工具**來設定一個中級或高級的安全性等級（或在**GNOME Lokkit**程式中選擇高或低的安全性設定），包括 NIS 與 LDAP 等網路認證方式都將無法通過防火牆。

這個章節並不詳細解釋每一個不同的認證類型，在此將會討論如何使用**網路認證設定工具**來設定它們。

如要從桌面啟動圖形化版本的**網路認證設定工具**，請選擇面板上的『**主選單按鈕**』=>『**系統設定**』=>『**認證**』，或是在 shell 提示符號下（如 **XTerm** 或 **GNOME 終端機**）輸入 `authconfig-gtk` 指令。如要啟動文字介面的版本，請在 shell 提示符號下輸入 `authconfig` 指令。



#### 重要

在離開認證設定程式後，所做的變更將會立即生效。

## 22.1. 使用者資訊

『**使用者資訊**』的標籤頁含有許多選項，如要啟用一個選項，請點選旁邊的空白選取盒。如要停用一個選項，請點選在其旁的選取盒以取消選取。點選**確定**以離開這個程式，並且套用變更。



圖形22-1. 使用者資訊

下列的清單將向您說明每一個選項的用意：

- **緩衝貯存使用者資訊** — 請選取這個選項以啟用名稱服務快取系統程式(nscd)，並且設定為開機時即刻啟動。

必須安裝nscd 套件才能使用這個選項。

- **啟用NIS 支援** — 選取這個選項以設定系統為連線到NIS 伺服器以取得使用者與密碼認證的一部NIS 用戶端。點選**設定NIS** 按鈕以指定NIS 網域與NIS 伺服器。假如在此沒有指定NIS 伺服器，系統程式將會試著以廣播的方式進行搜尋。

必須安裝ypbind 套件才能使用這個選項。假如啟用NIS 支援，將會啟動portmap 與ypbind 服務，而且也設定為在開機時即刻啟動。

- **啟用LDAP 支援** — 選取這個選項以設定系統透過LDAP 擷取使用者資訊，點選**設定LDAP** 按鈕來指定『**LDAP 查詢Base DN**』與『**LDAP 伺服器**』。假如『**使用TLS 為連線加密**』已被選取，Transport Layer Security 將被用來加密傳送至LDAP 伺服器的密碼。

必須安裝openldap-clients 套件才能使用這個選項。

如需關於LDAP 的更多資訊，請參考*Red Hat Linux* 參考手冊。

- **啟用Hesiod 支援** — 選取這個選項以設定系統從遠端的Hesiod 資料庫擷取資訊（包括使用者資訊）。

必須已安裝hesiod 套件。

## 22.2. 認證

『**認證**』的標籤頁可讓您設定網路認證方式。如要啟用一個選項，請點選旁邊的空白選取盒。如要停用一個選項，請點選在其旁的選取盒以取消選取。



圖形22-2. 認證

下列的清單將向您說明每一個選項的用意：

- **使用Shadow 密碼** — 選取這個選項以儲存密碼為shadow 的密碼格式在/etc/shadow 檔案中，而不是/etc/passwd。安裝時即預設啟動Shadow 密碼，並且是強烈建議使用的，以大大地增加系統的安全性。

必須安裝shadow-utils 套件才能使用這個選項。如需關於shadow 密碼的更多資訊，請參考*Red Hat Linux* 參考手冊 中的『使用者與群組』一章。

- **使用MD5 編碼** — 選取這個選項以啟用MD5 編碼，這將會允許長達256 字元的密碼長度（而非8 字元以下）。這是在安裝時預設選取的，並且強烈建議您使用的，以增加系統的安全性。



- **啟用LDAP 支援** — 選取這個選項以使得擁有標準PAM-enabled 的應用程式使用LDAP 以做認證。點選**設定LDAP** 按鈕以指定以下資訊：
  - **使用TLS 為連線加密** — 使用Transport Layer Security 為傳送至LDAP 伺服器的密碼加密。
  - **LDAP 查詢Base DN** — 藉由搜尋Distinguished Name (DN) 來擷取使用者資訊。
  - **LDAP 伺服器** — 指定LDAP 伺服器的IP 位址。
 必須安裝openldap-clients 套件才能使用這個選項。請參考*Red Hat Linux* 參考手冊 以取得更多關於LDAP 的資訊。
- **啟用Kerberos 支援** — 選取這個選項以啟用Kerberos 認證，點選**設定Kerberos** 按鈕來進行設定：
  - **領域** — 設定Kerberos 伺服器的領域(realm)。這裡的領域代表使用Kerberos 的網路，其中含有一個或以上的KDCs 以及可能大量的用戶端機器。
  - **KDC** — 定義金鑰發佈中心(Key Distribution Center -KDC)，就是用來發佈Kerberos 票簽的伺服器。
  - **系統管理伺服器** — 指定執行kadmind 的管理伺服器。
 必須安裝krb5-libs 與krb5-workstation 套件才能使用這個選項。請參考*Red Hat Linux* 參考手冊 以取得關於Kerberos 的更多資訊。
- **啟用SMB 支援** — 這個選項設定PAM 來使用一部SMB 伺服器來認證使用者。點選**設定SMB** 按鈕來指定下列資訊：
  - **工作群組** — 指定欲使用的SMB 工作群組。
  - **網域控制站** — 指定欲使用的SMB 網域控制站。

## 22.3. 命令列版本

也可以執行**網路認證設定工具** 為不含任何介面的命令列工具。這個命令列的版本可以被使用在一個設定的程式碼中或一個kickstart 的程式碼中。這些認證選項的摘要在表格22-1。

選項	說明
--enableshadow	啟用shadow 密碼
--disableshadow	停用shadow 密碼
--enablemd5	啟用MD5 編碼
--disablemd5	停用MD5 編碼
--enablenis	啟用NIS
--disablenis	停用NIS
--nisdomain=<domain>	指定NIS 網域
--nissserver=<server>	指定NIS 伺服器
--enableldap	啟用LDAP 擷取使用者資訊
--disableldap	停用LDAP 擷取使用者資訊
--enableldaptls	啟用LDAP 中的TLS 功能
--disableldaptls	停用LDAP 中的TLS 功能
--enableldapauth	啟用LDAP 以做認證

選項	說明
<code>--disableldapauth</code>	停用LDAP 以做認證
<code>--ldapserver=&lt;server&gt;</code>	指定LDAP 伺服器
<code>--ldapbasedn=&lt;dn&gt;</code>	指定LDAP base DN
<code>--enablekrb5</code>	啟用Kerberos
<code>--disablekrb5</code>	停用Kerberos
<code>--krb5kdc=&lt;kdc&gt;</code>	指定Kerberos KDC
<code>--krb5adminserver=&lt;server&gt;</code>	指定Kerberos 管理伺服器
<code>--krb5realm=&lt;realm&gt;</code>	指定Kerberos 領域
<code>--enablesmbauth</code>	啟用SMB
<code>--disablesmbauth</code>	停用SMB
<code>--smbworkgroup=&lt;workgroup&gt;</code>	指定SMB 工作群組
<code>--smbservers=&lt;server&gt;</code>	指定SMB 伺服器
<code>--enablehesiod</code>	啟用Hesiod
<code>--disablehesiod</code>	停用Hesiod
<code>--hesiodlhs=&lt;lhs&gt;</code>	指定Hesiod LHS
<code>--hesiodrhs=&lt;rhs&gt;</code>	指定Hesiod RHS
<code>--enablecache</code>	啟用nscd
<code>--disablecache</code>	停用nscd
<code>--nostart</code>	不啟動或停止portmap、ypbind 或nscd 服務，即使它們已經被設定好
<code>--kickstart</code>	不顯示使用者介面
<code>--probe</code>	偵測與顯示網路預設值

表格22-1. 命令列選項

**建議**

也可在authconfig 的man page 或在Shell 提示符號下輸入authconfig --help 指令來找到這些選項。

## 郵件傳送代理(MTA)的設定

要從一部Red Hat Linux 系統傳送電子郵件必須使用『郵件傳送代理』(MTA) 才行，然而，例如**Evolution**、**Mozilla Mail** 以及**Mutt** 等的『郵件用戶代理』(MUA) 是用來閱讀與編輯郵件的程式。當使用者從一個MUA 寄出一封電子郵件，該郵件將會先交寄給MTA，然後再傳送該訊息到一系列的MTA，直到到達目的地。

即使使用者並沒有打算要從系統寄出郵件，有些自動的工作與系統程式也會使用/bin/mail 指令來傳送包含紀錄檔訊息的電子郵件給本機系統的root 使用者。

Red Hat Linux 9 提供了兩種MTA：Sendmail 與Postfix。假如兩種都安裝了。sendmail 則為預設的MTA，您也可以使用**郵件傳送代理轉換器** 來選擇sendmail 或postfix 來當作系統預設的MTA。

您必須安裝redhat-switch-mail RPM 套件，才可以以文字模式為主的**郵件傳送代理轉換器** 程式版本。假如您比較喜歡圖形化的版本，請安裝redhat-switch-mail-gnome 套件。如需關於安裝RPM 套件的更多資訊，請參考 [V 部](#)。

如要啟動**郵件傳送代理轉換器**，請選擇面板上的『主選單按鈕』=> 『系統工具』=> 『更多系統工具』=> **郵件傳送代理轉換器**，或是在shell 提示符號下（例如XTerm 或GNOME 終端機）輸入redhat-switch-mail 指令。

這個程式將會自動偵測X 視窗系統是否正在執行中，如果是的話，程式將會以如圖形23-1 所示的圖形模式啟動，如果沒有偵測到X，則以文字模式啟動。如要強迫**郵件傳送代理轉換器** 以文字模式執行，請使用redhat-switch-mail-nox 指令。



圖形23-1. 郵件傳送代理轉換器

假如您選擇**確定** 來改變MTA，您所選擇的郵件系統程式將會在開機時自動啟動，而未選取的郵件系統程式則不會在開機時啟動。因為這裡所作的變更將會立即生效，所選取的郵件系統程式會啟動，而另一個郵件系統程式則會停止。

如需關於郵件通訊協定與MTA 的更多資訊，請參考Red Hat Linux 參考手冊。如需關於MUA 的更多資訊，請參考Red Hat Linux 使用手冊。



## IV. 系統組態設定

在討論完主控台存取以及如何從一部Red Hat Linux 系統收集軟硬體資訊，這個部份將解釋一般的系統組態設定工作。

### 內容目錄

24章主控台存取.....	175
25章使用者與群組設定.....	179
26章收集系統資訊.....	187
27章印表機設定.....	195
28章自動工作排程管理.....	213
29章紀錄檔案.....	219
30章升級核心.....	221
31章核心模組.....	227



當一般（非root）的使用者在本機登入到一部電腦時，他們將擁有兩種類型的特殊權限設定：

1. 他們可以執行使用別的方法無法執行的某些程式
2. 他們可以存取使用別的方法無法存取的某些檔案（通常是用來存取軟碟片、光碟片等等特殊的裝置檔案）

因為在一部電腦上有許多主控台，而且在同一時間可以有許多人在本機登入到一部電腦，這些使用者的其中之一必須拔得頭籌以存取檔案。在主控台第一個登入的使用者將擁有那些檔案，當第一個使用者登出後，下一個登入的使用者將會擁有這些檔案。

相反地，每一個登入到主控台的使用者將會被允許執行某些通常限定root使用者才能執行的程式。假如您有執行X，這些動作可以被收錄在圖形使用者介面中的選單項目。在此版本中，主控台可存取的程式包括halt、poweroff 與reboot。

## 24.1. 停用Ctrl-Alt-Del 的關機快捷鍵

預設情況下，當您在主控台按下[Ctrl]-[Alt]-[Del]的按鍵組合，/etc/inittab 指定您的系統設定為關機並重新啟動系統。假如您想要停用這個功能，您將需要在/etc/inittab 檔案中的下列這行加上井字號(#)以註解該行：

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

或者您只是想要允許某些非root的使用者可以在主控台中使用[Ctrl]-[Alt]-[Del]來關閉系統，您可以藉由以下的步驟來限制某些使用者的權限：

1. 增加-a的參數到/etc/inittab 檔案中如以上所述的該行，使其類似如下：  

```
ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
```

  
-a的旗號告訴shutdown 去查看/etc/shutdown.allow 檔案，也就是您下一步要建立的。
2. 在/etc 目錄下建立名為shutdown.allow 的檔案，shutdown.allow 檔案中可以含有允許使用[Ctrl]-[Alt]-[Del] 按鍵組合來關閉系統的任何使用者名稱。/etc/shutdown.allow 檔案的格式為一行一個使用者名稱，如下所示：  
stephen  
jack  
sophie

根據shutdown.allow 這個範例檔案，stephen, jack 與sophie 允許從主控台使用[Ctrl]-[Alt]-[Del]來關閉系統。當這個按鍵組合被使用時，/etc/inittab 檔案中的shutdown -a 將會檢查/etc/shutdown.allow 檔案中的任何使用者（非root）是否已登入到虛擬主控台中。假如其中之一存在的話，系統的關機程序將會繼續；假如沒有的話，將會寫入一個錯誤訊息到系統主控台。

如需關於shutdown.allow 檔案的更多資訊，請參考shutdown的man page。

## 24.2. 停用主控台程式存取

為了要停用使用者存取主控台程式，您必須要以root 身份執行以下指令：

```
rm -f /etc/security/console.apps/*
```

在主控台以別種方式做安全設定的環境下（如設定BIOS 與開機管理程式密碼、停用[Ctrl]-[Alt]-[Delete] 的按鍵組合以及停用電源與重開機的開關等等），您也許不想允許使用者在主控台中執行poweroff, halt 以及reboot 等在主控台中預設可使用的指令。

如要移除這些功能，請以root 身份執行下列指令：

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

### 24.3. 停用所有的主控台存取

pam\_console.so PAM 模組管理主控台的檔案權限設定與認證。（請參考*Red Hat Linux* 參考手冊 以取得關於如何設定PAM 的更多資訊。）假如您想要停用所有的主控台存取（包括程式以及檔案存取），請註解在/etc/pam.d 目錄中指向pam\_console.so 的所有行。請以root 身份執行以下的程式碼即可：

```
cd /etc/pam.d
for i in * ; do
sed '/#[^#].*pam_console.so/s/^/#/' <$i > foo && mv foo $i
done
```

### 24.4. 定義主控台

pam\_console.so 模組使用/etc/security/console.perms 檔案來決定在系統主控台的使用者權限設定。這個檔案的語法相當地有彈性，您可以編輯這個檔案以使得這些指示不再適用。然而，預設的檔案含有如下所示的這一行：

```
<console>=tty[0-9][0-9]*:[0-9]\.[0-9]:[0-9]
```

當使用者登入後，他們便被附加上某種命名的終端機，也許是含有一個名稱的X 伺服器式像:0 或mymachine.example.com:1.0，或者是一個裝置如/dev/ttyS0 或/dev/pts/2。預設值是定義本機的虛擬主控台與本機的X 伺服器式是被認為本地端的，不過假如您想要定義在您主機旁邊的虛擬終端機（位於/dev/ttyS1 連接埠）也是本地端的，您可以更改該行如下所示：

```
<console>=tty[0-9][0-9]*:[0-9]\.[0-9]:[0-9] /dev/ttyS1
```

### 24.5. 使檔案可經由主控台存取

在/etc/security/console.perms 檔案中，有一個部份如下所示：

```
<floppy>=/dev/fd[0-1]* \
/dev/floppy* /mnt/floppy*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
/dev/mixer* /dev/sequencer \
/dev/sound/* /dev/beep
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
```

假如有需要的話，您可以增加一些行到這個部份，請確定您所增加的行有參考到適當的裝置。舉例來說，您可以增加以下這一行：

```
<scanner>=/dev/scanner /dev/usb/scanner*
```



(當然，請確定/dev/scanner 確實是您的掃描器，而不是您的硬碟機。)

這是第一個步驟，第二個步驟是定義那些檔案會做什麼事。請找出/etc/security/console.perms 檔案中類似如下的最後部份：

```
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound> 0640 root
<console> 0600 <cdrom> 0600 root.disk
```

加上如下這一行：

```
<console> 0600 <scanner> 0600 root
```

然後當您登入到主控台後，您將會被給予/dev/scanner 裝置的擁有權，而權限設定為0600（只有您能讀取與寫入）。當您登出後，該裝置將會由root 所擁有，且仍然含有0600（現在則為只能由root 讀取與寫入）的權限設定。

## 24.6. 啟用其他應用程式的主控台存取

假如您想要讓主控台的使用者存取其他應用程式，您必須要做一些較複雜的動作。

首先，主控台存取僅適用於位於/sbin 或/usr/sbin 中的應用程式，所以您想要執行的應用程式必須在那裡。在確認過後，請遵照以下步驟：

1. 建立一個應用程式名稱的連結（例如我們的範例程式foo）到/usr/bin/consolehelper 應用程式：  

```
cd /usr/bin
ln -s consolehelper foo
```
2. 建立/etc/security/console.apps/foo 檔案：  

```
touch /etc/security/console.apps/foo
```
3. 在/etc/pam.d/ 目錄中為foo 服務建立一個PAM 的設定檔案。有一個較簡單的方法是使用halt 服務的PAM 設定檔案，然後依照您的需求來做適當的修改：  

```
cp /etc/pam.d/halt /etc/pam.d/foo
```


現在當您執行/usr/bin/foo 時，將會呼叫consolehelper 並藉由/usr/sbin/userhelper 的輔助來認證使用者。如要認證使用者，consolehelper 假如/etc/pam.d/foo 檔案是/etc/pam.d/halt 的複本，consolehelper 將會詢問使用者的密碼（否則它將會確實執行/etc/pam.d/foo 檔案中所指定的事項），然後再以root 的權限執行/usr/sbin/foo。

在PAM 的設定檔案中，可以設定一個應用程式以使用pam\_timestamp 模組來記憶（快取）一個成功的認證過程。當您啟動一個應用程式並且提供適當的認證資訊（root 密碼），將會建立一個時間戳檔案。預設情況下，一次成功的認證將會快取五分鐘，在這個期間中，任何其他設定來使用pam\_timestamp 的應用程式，如在同一個作業階段執行將會自動地認證為這個使用者——這個使用不需要再次輸入root 密碼。

這個模組收錄在pam 套件中，如要啟用這個特色，在etc/pam.d/ 目錄中的PAM 設定檔案必須包含以下這兩行：

```
auth sufficient /lib/security/pam_timestamp.so
session optional /lib/security/pam_timestamp.so
```

以auth 為開頭的第一行應該在任何其他的auth sufficient 行列之後，而以session 為開頭的行列必須在任何其他的session optional 行列之後。

假如一個設定使用pam\_timestamp 的應用程式從面板上的『主選單按鈕』認證成功，如果您是執行GNOME 桌面環境的話， 圖示將會出現在面板上的提示區域。在認證失效後（預設為5 分鐘），該圖示便會消失。

使用者可以選擇要忘記快取的認證資訊，只要點選該圖示然後選擇要忘記認證資訊的選項。

## 24.7. floppy 群組

假如因為某種因素，主控台存取不適用於您，而您需要給予非root的使用者存取您系統的軟碟機，這可以經由使用floppy 群組來做到。只要使用您所選的工具來增加使用者到floppy 群組。這裡為一個例子顯示如何使用gpasswd 指令來增加使用者fred 到floppy 群組：

```
[root@bigdog root]# gpasswd -a fred floppy
Adding user fred to group floppy
[root@bigdog root]#
```

現在，使用者fred 將可以從主控台存取系統的軟碟機了。

## 使用者與群組設定

**使用者管理員** 讓您您可以檢視、修改、新增與刪除本機使用者與群組。

如想要使用**使用者管理員**，您必須執行X 視窗系統，並擁有root 權限以及已經安裝了redhat-config-users RPM 套件。如要從桌面啟動**使用者管理員**，請選擇面板上的『主選單』=> 『系統設定』=> 『使用者與群組』。或者在shell 提示符號下（如XTerm 或GNOME 終端機）輸入redhat-config-users 指令。



圖形25-1. 使用者管理員

如要檢視系統上所有本機使用者的清單，請點選『**使用者**』的標籤頁；如要檢視系統上所有本機群組的清單，請點選『**群組**』的標籤頁。

假如您需要尋找一個特定的使用者或群組，請在『**搜尋過濾器**』的欄位中輸入名稱的開頭幾個字母，按下[Enter] 或點選**套用過濾器** 的按鈕，過濾的清單將會顯示出來。

如要為使用者或群組做排序，請點選欄位名稱。使用者或群組將會以該欄位的數值來做排序。

Red Hat Linux 保留500 以下的**使用者ID** 給系統使用者使用，預設情況下，**使用者管理員** 並不顯示系統使用者。如要檢視所有的使用者（包括系統使用者），請在『**選項**』的下拉式選單中取消選取『**過濾系統使用者與群組**』。

關於使用者與群組的其他資訊可在**Red Hat Linux 參考手冊** 與**Red Hat Linux 系統管理入門** 中找到。

## 25.1. 新增一個使用者

如要新增一個使用者，請點選**新增使用者** 的按鈕，將會出現一個如圖形25-2 所示的視窗。請在適當的欄位輸入這個新使用者的使用者名稱與全名，並在『**密碼**』與『**密碼確認**』的欄位輸入使用者的密碼。密碼必須至少是六個字元以上。



### 建議

使用者密碼的位數越長，其他人便很難猜到這個密碼以用來登入該使用者的帳號。也建議您不要使用基於一個單字的密碼，最好是使用字母、數字與特殊字元的結合。

您還要選取一個登入的shell，假如您不知道該選取那一個shell，請接受預設設定的/bin/bash。預設的家目錄是/home/username，您可以變更為這個使用者建立的家目錄，或取消選取『**建立家目錄**』以選擇不建立家目錄。

假如您選擇要建立家目錄，預設的設定檔案將會從/etc/skel 目錄複製到新的家目錄下。

Red Hat Linux 使用一種使用者私有群組 (UPG) 的機制，這個UPG 機制並不更改UNIX 標準的處理群組方式，它提供了一個新的作法。當您建立一個新的使用者時，預設情況下將會建立一個與使用者名稱相同的特定群組。假如您不想建立這個群組，請取消選取『**為這個使用者建立私有群組**』。

如要為使用者指定一個使用者ID，請選取**手動指定使用者ID**，假如不選擇這個選項，將會指定下一個使用者ID (由500 開始) 給新的使用者。Red Hat Linux 保留500 以下的使用者ID 給系統使用者。

點選**確定** 來建立這個使用者。

使用者名稱：

全名：

密碼：

密碼確認：

登入的 Shell：  ▼

建立家目錄

家目錄：

為這個使用者建立私有群組

手動指定使用者 ID

使用者 ID (UID)：  ▲▼

圖形25-2. 新的使用者

如要設定像密碼失效期限的進階使用者內容，請在新增使用者後修改該使用者的內容。請參考 25.2 節以取得更多資訊。

如要增加使用者到更多的使用者群組，請點選『**使用者**』的標籤頁，選取一個使用者，再點選**內容**，在『**使用者內容**』的視窗中，選取『**群組**』的標籤頁。選取您想要這個使用者加入的群組名稱，再選取這個使用者的主群組，然後點選**確定**。

## 25.2. 修改使用者內容

如要檢視一個現有使用者的內容，請點選『**使用者**』的標籤頁，從使用者清單中選取一個使用者，再從工具列選單中點選**內容** (或選擇『**檔案**』=>『**內容**』)。將會出現如圖形25-3 的視窗。

圖形25-3. 使用者內容

『使用者內容』的視窗分為下列這幾個標籤頁：

- **使用者資料** — 顯示當您新增使用者時所設定的基本使用者資訊，請使用這個標籤頁來變更使用者的全名、密碼、家目錄或登入shell。
- **帳號資訊** — 假如您設定這個帳號在某個日期失效，請選取**啟用帳號有效期限**，並且在所提供的欄位中輸入日期。選擇『**使用者帳號已被鎖定**』來鎖定使用者的帳號，以使得該使用者無法登入系統。
- **密碼資訊** — 這個標籤頁顯示上一次更改使用者密碼的日期。如要強迫使用者在幾天後更改密碼，請選擇『**啟動密碼有效期限**』，在此您可以更改使用者必須更改密碼前的天數、使用者被警告需更改密碼的天數，以及帳號失效前的天數等。
- **群組** — 選取您想要這個使用者加入的群組名稱以及這個使用者的主群組。

### 25.3. 新增一個群組

如要增加一個新的使用者群組，請點選**新增群組**的按鈕，會出現類似圖形25-4的一個視窗，請輸入要建立的群組名稱，如果要指定一個群組ID給這個新的群組，請選擇**手動指定群組ID**，並選擇一個GID。Red Hat Linux 保留500以下的群組ID給系統的群組。

點選**確定**來建立這個群組，這個新群組會出現在群組清單中。

圖形25-4. 新的群組

如要增加使用者到群組中，請參考 25.4 節。

### 25.4. 修改群組內容

如要檢視一個現有群組的內容，請從群組清單中選擇一個群組，再點選工具列上的**內容**按鈕（或選擇程式選單中的『**檔案**』=>『**內容**』）。將會出現一個類似圖形25-5的視窗。



圖形25-5. 群組內容

『群組使用者』的標籤頁顯示出隸屬這個群組的使用者成員。您可以選取其他的使用者以加入到這個群組，或取消選取使用者以從該群組中移除。點選**確定**來修改這個群組中的使用者。

## 25.5. 命令列設定

假如您較喜歡用命令列工具，或者是沒有安裝X視窗系統，請詳閱這個章節以取得設定使用者與群組的相關資訊。

### 25.5.1. 新增一個使用者

如要新增一個使用者到系統中：

1. 請執行`useradd`指令來建立一個鎖定的使用者帳號：  
`useradd <username>`
2. 請執行`passwd`指令來解除這個帳號的鎖定，並且指定一個密碼與設定密碼的失效指引：  
`passwd <username>`

`useradd` 指令的命令列選項位於表格25-1。

選項	說明
<code>-c comment</code>	對使用者的備註
<code>-d home-dir</code>	欲使用的家目錄，而不是預設的 <code>/home/username</code>
<code>-e date</code>	帳號失效的日期（以YYYY-MM-DD格式表示）
<code>-f days</code>	在密碼過期後與帳號失效前的天數。（假如在此指定0，在密碼過期後帳號將立即失效。假如指定了-1，在密碼過期後，該帳號將不會失效。）
<code>-g group-name</code>	當作使用者預設群組的群組名稱或群組ID（在此指定之前，這個群組必須存在。）
<code>-G group-list</code>	使用者所隸屬之額外群組名稱（非預設的）或群組ID的清單，請以逗號分隔開。（在此指定之前，這個群組必須存在。）
<code>-m</code>	建立家目錄（假如不存在的話）
<code>-M</code>	不建立家目錄

選項	說明
-n	不建立使用者的私有群組
-r	建立一個UID 500 以下的系統帳號，並且不建立一個家目錄
-p <i>password</i>	使用crypt 為密碼加密
-s	使用者的登入shell，預設為/bin/bash
-u <i>uid</i>	使用者的使用者ID，必須是獨特的且大於499

表格25-1. useradd 命令列選項

### 25.5.2. 新增一個群組

如要新增一個群組到系統中，請使用groupadd 指令：

```
groupadd <group-name>
```

groupadd 的命令列選項位於表格25-2。

選項	說明
-g <i>gid</i>	指定給群組的群組ID，必須是獨特的且大於499。
-r	建立一個GID 小於500 的系統群組
-f	假如指定的群組已經存在，隨即離開並出現一個錯誤。（群組資訊並不改變。）假如一併指定-g 與-f，不過該群組已經存在，將會忽略-g 選項。

表格25-2. groupadd 的命令列選項

### 25.5.3. 密碼有效期限設定

為了安全上的考量，最好設定使用者要定期變更他們的密碼，這可以在**使用者管理員** 程式中的『密碼資訊』標籤頁做此設定。

如要在shell 提示符號下設定使用者的密碼失效日期，請使用chage 指令，再加上表格25-3 中的選項，後面再接使用者名稱。



**重要**

必須要啟用Shadow 密碼才能使用chage 指令。

選項	說明
-m <i>days</i>	指定使用者必須要更改密碼的最短天數，假如這個數值是0 的話，密碼絕不會過期。
-M <i>days</i>	指定密碼最長的有效天數，當這個選項所指定的天數加上-d 選項所指定的天數少於目前的天數（從1970年1月1日開始計算），使用者必須馬上更改密碼，才能繼續使用這個帳號。

選項	說明
<code>-d days</code>	指定上次更改密碼的天數（從1970年1月1日開始計算）。
<code>-I days</code>	指定在密碼過期後與帳號被鎖定前的天數，假如指定數值為0的話，在密碼過期後，帳號將不會被鎖定。
<code>-E date</code>	指定要鎖定帳號的日期（以YYYY-MM-DD格式），如不指定日期，也可使用從1970年1月1日起計算的天數。
<code>-w days</code>	指定密碼過期前要警告使用者的天數。

表格25-3. `chage` 的命令行選項



#### 建議

假如`chage` 指令後面直接接一個使用者名稱（不含任何選項），輸出將會顯示目前的密碼使用期限數值，並讓您來更改它們。

假如系統管理員要使用者在第一次登入時設定一個密碼，可以設定使用者的密碼立即過期，強迫使用者在第一次登入時，必須立即更改。

如要在主控台設定以強迫使用者在第一次登入時設定一個自己的密碼，請遵照以下步驟。請注意，這個過程並不適用於使用SSH 通訊協定登入的使用者。

1. 鎖定使用者的密碼 — 假如這個使用者並不存在，請使用`useradd` 指令來建立這個使用者帳號，不過先不要設定他的密碼，以使得這個帳號保持被鎖定的狀態。

假如密碼已經被啟用，請使用下列指令鎖定它：

```
usermod -L username
```

2. 強迫密碼立即失效 — 請輸入以下指令：

```
chage -d 0 username
```

這個指令設定上次更改密碼的日期為新紀元（1970年1月1日），這個數值會強迫密碼立即失效，不管是否有任何的密碼期限設定。

3. 解除帳號的鎖定 — 這裡有兩種通用的方法，管理員可以指定一個初始的密碼或指定一個空的密碼。



#### 警告

請勿使用`passwd` 指令來設定密碼，因為這將會停用剛剛設定的密碼立即失效。

如要指定一個初始的密碼，請使用下列的步驟：

- 使用`python` 指令來啟動命令列的Python 解譯器，會顯示出下列資訊：

```
Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
[GCC 3.2.1 20021207 (Red Hat Linux 8.0 3.2.1-2)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

- 在提示符號下，輸入以下資訊（以要加密的密碼取代`password`；以兩個大寫或小寫的字元、數字、點(.)字元或反斜線(/)的組合取代`salt`（如`ab` 或`12`）：

```
import crypt; print crypt.crypt("password", "salt")
```

這個指令的輸出會是類似`12CsGd8FRcMSM` 的加密密碼。

- 按下`[Ctrl]-[D]` 以離開Python 解譯器。
- 剪貼整個加密的密碼輸出到以下的指令中（不含開頭與結尾的空白）：



```
usermod -p "encrypted-password" username
```

除了指定一個初始的密碼外，也可以使用下列指令來指定一個空的密碼：

```
usermod -p "" username
```



#### 警示

雖然使用一個空的密碼對使用者與管理員都很方便，這樣做有一些風險存在，因為第三者也許會先登入，並存取系統。為了要減低這個威脅，建議您在系統管理員確定使用者已經準備好登入後，才解除鎖定使用者的帳號。

在這兩個例子中，使用者第一次登入後，將會被提示要求輸入一個新的密碼。

## 25.6. 設定過程的解釋

下列的步驟詳述了在啟用shadow 密碼之系統上執行useradd juan 所發生的過程：

1. 在/etc/passwd 檔案中建立一行含有juan 的資訊，該行含有下列的特徵：
  - 以使用者名稱juan 開頭。
  - 在密碼的欄位有一個x 代表系統使用shadow 密碼。
  - 建立一個500 或以上的UID。（在Red Hat Linux 中，500 以下的UIDs 與GIDs 是保留給系統使用。）
  - 建立一個500 或以上的GID。
  - 可選的GECOS 資訊留空。
  - juan 的家目錄設定為/home/juan/。
  - 預設的shell 設定為/bin/bash。
2. 在/etc/shadow 檔案中建立一行含有juan 的資訊，該行含有下列的特徵：
  - 以使用者名稱juan 開頭。
  - 兩個驚嘆號出現在/etc/shadow 檔案中的密碼欄位，用來鎖定帳號。



#### 請注意

假如使用-p 旗號傳送一個加密的密碼，該使用者的資訊將會被放置在/etc/shadow 檔案中新的一行。

- 密碼設定為永不過期。
3. 在/etc/group 檔案中，會建立一行含有juan 的群組名稱。與使用者相同名稱的群組稱為『使用者私有群組』。如需關於使用者私有群組的更多資訊，請參考 25.1 節。  
在/etc/group 檔案中所建立的該行含有下列的特徵：
    - 以群組名稱juan 開頭。
    - 出現在密碼欄位的一個x 代表系統使用shadow 群組密碼。
    - GID 會與/etc/passwd 檔案中所列出的juan 使用者的GID 相同。
  4. 在/etc/gshadow 檔案中，會建立一行含有juan 的群組名稱，該行含有下列的特徵：

- 以群組名稱 `juan` 開頭。
  - 一個驚嘆號(!) 出現在 `/etc/gshadow` 檔案中的密碼欄位，用來鎖定群組。
  - 其餘所有欄位皆留空。
5. 在 `/home/` 目錄下建立一個使用者 `juan` 的目錄，這個目錄是屬於使用者 `juan` 與群組 `juan` 所有，然而它只允許使用者 `juan` 擁有讀取、寫入與執行的權限，並拒絕其他所有的存取權限。
  6. 位於 `/etc/skel/` 目錄中的檔案（其中含有預設的使用者設定）會複製到新的 `/home/juan/` 目錄中。

在此，系統中有一個稱為 `juan` 的鎖定帳號，如要啟用它，系統管理員必須使用 `passwd` 指令來指定一個密碼給這個帳號，並且設定密碼的期限設定（可選的）。

## 收集系統資訊

在您學習如何設定您的系統之前，您應該學習如何收集重要的系統資訊。例如您需要知道如何找出剩餘記憶體的空間、剩餘硬碟空間的容量、您的硬碟是如何分割的以及有那些程序正在執行中。這個章節討論如何使用簡單的指令與一些簡易的程式來從您的Red Hat Linux 系統取得這些類型的資訊。

## 26.1. 系統程序

`ps ax` 指令將會顯示目前系統執行中之程序的清單。如要一併顯示程序的擁有者，請使用 `ps aux` 指令。這個清單是靜態的清單，也就是說，它是當您執行指令時所正在執行之程序的快照。假如您需要要不斷更新的執行程序清單，請使用如下所述的 `top` 指令。

`ps` 指令的輸出可以很長，如要使其不捲動超過畫面，您可以將輸出 `pipe` 到 `less` 指令：

```
ps aux | less
```

您可以使用 `grep` 指令與 `ps` 指令結合來查看一個程序是否正在執行中，例如要查看 `emacs` 是否正在執行中，請使用下列指令：

```
ps ax | grep emacs
```

`top` 指令會顯示正在執行中的程序，以及關於它們的重要資訊，包括它們的記憶體與CPU 用量。這個清單是即時並且為互動模式的，在此提供 `top` 指令的範例輸出如下：

```
00:53:01 up 6 days, 14:05, 3 users, load average: 0.92, 0.87, 0.71
71 processes: 68 sleeping, 2 running, 1 zombie, 0 stopped
CPU states: 18.0% user 0.1% system 16.0% nice 0.0% iowait 80.1% idle
Mem: 1030244k av, 985656k used, 44588k free, 0k shrd, 138692k buff
    424252k actv, 23220k in_d, 252356k in_c
Swap: 2040212k av, 330132k used, 1710080k free      521796k cached
```

```
PID USER   PRI NI  SIZE  RSS SHARE STAT %CPU %MEM  TIME COMMAND
15775 joe     5  0 11028 10M 3192 S   1.5 4.2  0:46 emacs
14429 root    15  0 63620 62M 3284 R   0.5 24.7 63:33 X
17372 joe    11  0 1056 1056 840 R   0.5 0.4  0:00 top
17356 joe     2  0 4104 4104 3244 S   0.3 1.5  0:00 gnome-terminal
  1 root     0  0 544 544 476 S   0.0 0.2  0:06 init
  2 root     0  0  0  0 0 SW  0.0 0.0  0:00 kflushd
  3 root     1  0  0  0 0 SW  0.0 0.0  0:24 kupdate
  4 root     0  0  0  0 0 SW  0.0 0.0  0:00 kpiod
  5 root     0  0  0  0 0 SW  0.0 0.0  0:29 kswapd
347 root     0  0 556 556 460 S   0.0 0.2  0:00 syslogd
357 root     0  0 712 712 360 S   0.0 0.2  0:00 klogd
372 bin      0  0 692 692 584 S   0.0 0.2  0:00 portmap
388 root     0  0  0  0 0 SW  0.0 0.0  0:00 lockd
389 root     0  0  0  0 0 SW  0.0 0.0  0:00 rpciod
414 root     0  0 436 432 372 S   0.0 0.1  0:00 apmd
476 root     0  0 592 592 496 S   0.0 0.2  0:00 automount
```

如要離開 `top`，請按下 `[q]` 按鍵。

您可以在 `top` 使用的互動式指令如下：

指令	說明
[空白鍵]	立即重新整理
[h]	顯示一個說明畫面
[k]	Kill 一個程序，您將會被提示輸入程序ID 以及要傳送給它的訊號。
[n]	變更顯示出來的程序數目，您將會被提示輸入一個數目。
[u]	以使用者排序。
[M]	以記憶體用量排序。
[P]	以CPU 用量排序。

表格26-1. 互動式的top 指令



#### 建議

例如**Mozilla** 與**Nautilus** 等應用程式是 *thread-aware* — 建立多個執行緒以處理多個使用者或多項要求，而且每一個執行緒都給予一個程序ID。預設情況下，ps 與top 只會顯示主要（初始）的執行緒，如要檢視所有的執行緒，請使用ps -m 指令或在top 按下[Shift]-[H]。

假如您較喜歡top 的一個圖形化介面，您可以使用『**GNOME 系統監控**』。如要從桌面啟動它，請選擇面板上的『**主選單按鈕**』=>『**系統工具**』=>『**系統監控**』，或是在X 視窗系統下的shell 提示符號輸入gnome-system-monitor 指令。然後選擇『**程序列表**』的標籤頁。

**GNOME 系統監控** 讓您可以在執行中的程序清單搜尋某個特定程序，以及檢視所有的程序、屬於您的程序或是現行的程序。

如要學習更多關於程序的資訊，請選取它，再點選**顯示詳細資訊** 的按鈕，將會在視窗的底部顯示關於該程序的細節。

如要停止一個程序，請選取它，再點選**終止程序** 的按鈕，這個功能對於停止回應的程序很有用。

如要以一個特定的欄位進行資料的排序，請點選該欄位的名稱，用來做排序的欄位將會以暗灰色的顏色顯示。

預設情況下，**GNOME 系統監控** 並不顯示執行緒，如要更改這個選項設定，請選擇『**編輯**』=>『**偏好設定**』，點選『**程序列表**』的標籤頁，然後選擇『**顯示執行緒**』。偏好設定也讓您設定更新的間隔，預設該顯示關於每一個程序何種類型的資訊，以及系統監視器圖像的顏色。



圖形26-1. GNOME 系統監控

## 26.2. 記憶體用量

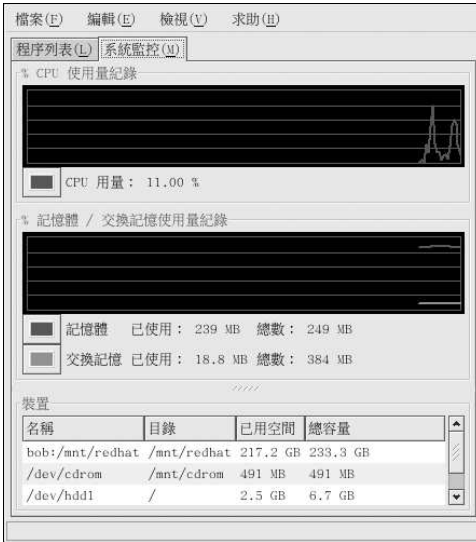
`free` 指令會顯示系統上的所有實體記憶體與swap 空間的容量，以及已使用、剩餘的、共享的、在核心緩衝區以及快取的記憶體容量。

```
total used free shared buffers cached
Mem: 256812 240668 16144 105176 50520 81848
-/+ buffers/cache: 108300 148512
Swap: 265032 780 264252
```

`free -m` 指令以MB 來表示相同的資訊，使得讀取更容易。

```
total used free shared buffers cached
Mem: 250 235 15 102 49 79
-/+ buffers/cache: 105 145
Swap: 258 0 258
```

假如您較喜歡`free` 程式的圖形化介面，您可以使用**GNOME 系統監控**。如要從桌面啟動它，請選擇面板上的『主選單按鈕』=> 『系統工具』=> 『系統監控』，或在X 視窗系統下的shell 提示符號輸入`gnome-system-monitor`，然後選擇『系統監控』的標籤頁。



圖形26-2. GNOME 系統監控

### 26.3. 檔案系統

`df` 指令會報告系統的磁碟空間用量。假如您在 `shell` 提示符號下輸入 `df` 指令，指令的輸出將會如下所示：

```
檔案系統      容量  已用  可用  已用  掛載點
/dev/hda2     10325716  2902060  6899140  30% /
/dev/hda1      15554    8656   6095  59% /boot
/dev/hda3     20722644  2664256  17005732  14% /home
none          256796    0    256796  0% /dev/shm
```

預設情況下，這個工具以 **1KB** 的磁碟區塊表示分割區的大小，以 **KB** 表示已用與可用的磁碟空間。如要以 **MB** 或 **GB** 檢視磁碟用量資訊，請使用 `df -h` 指令，`-h` 引數代表人們可讀的(human-readable)的格式，指令的輸出如下所示：

```
檔案系統      容量  已用  可用  已用  掛載點
/dev/hda2      9.8G  2.8G  6.5G  30% /
/dev/hda1      15M  8.5M  5.9M  59% /boot
/dev/hda3     20G  2.6G  16G  14% /home
none           251M  0    250M  0% /dev/shm
```

在分割區的列表中，有一項 `/dev/shm` 的紀錄，這個紀錄代表系統的虛擬記憶體檔案系統。

`du` 指令將顯示目錄中檔案所使用的估計空間，假如您在 `shell` 提示符號下輸入 `du`，每一個子目錄的磁碟用量都將以清單顯示出來，目前目錄以及子目錄的磁碟用量總計也會在清單的最後一行顯示出來。假如您不想要看到所有子目錄的小計，請使用 `du -hs` 指令以得到只有目錄總計且為人們可讀的格式。使用 `du --help` 指令來得到更多選項。

如要圖形化的格式檢視系統的分割區以及磁碟空間的用量，請使用如圖形26-2 所示在底部的『系統監控』標籤頁。



## 建議

如需關於實作磁碟配額的資訊，請參考第6章。

### 26.3.1. 監視檔案系統

Red Hat Linux 提供了一個稱為 `diskcheck` 的工具，可用來監視系統上的剩餘磁碟空間。根據設定檔案，當一個或以上的磁碟機到達一個指定的容量時，它將會傳送電子郵件給系統管理員。如要使用這個工具，您必須已經安裝了 `diskcheck RPM` 套件。

這個工具是以一個每小時的 `cron`<sup>1</sup> 工作執行。

您可以在 `/etc/diskcheck.conf` 檔案中定義下列的變數：

- `defaultCutoff` — 當磁碟機到達這個百分比容量時，將會回報給系統管理員。舉例來說，如果設定為 `defaultCutoff = 90`，當被監視的磁碟機容量到達90%時，將會傳送一封電子郵件給系統管理員。
- `cutoff[/dev/partition]` — 強制覆寫分割區的 `defaultCutoff` 設定，舉例來說，如果指定 `cutoff['/dev/hda3'] = 50`，當 `/dev/hda3` 分割區到達50%的容量時，`diskcheck` 將會向系統管理員提出警示。
- `cutoff[/mountpoint]` — 強制覆寫掛載點的 `defaultCutoff` 設定，舉例來說，如果指定 `cutoff['/home'] = 50`，當掛載點 `/home` 到達50%的容量時，`diskcheck` 將會向系統管理員提出警示。
- `exclude` — 指定希望 `diskcheck` 忽略的一個或以上的分割區，舉例來說，如果指定 `exclude = "/dev/sda2 /dev/sda4"`，當 `/dev/sda2` 或 `/dev/sda4` 到達所指定的 `cutoff` 百分比時，`diskcheck` 將不會向系統管理員提出警示。
- `ignore` — 以 `-x filesystem-type` 格式指定要忽略的一個和以上的檔案系統，舉例來說，如果指定 `ignore = "-x nfs -x iso9660"`，系統管理員將不會收到關於 `nfs` 或 `iso9660` 檔案系統到達指定容量的警示。
- `mailTo` — 當分割區或掛載點到達指定的容量時，要用來傳送警示之系統管理員的電子郵件地址。舉例來說，假如您指定 `mailTo = "webmaster@example.com"`，`webmaster@example.com` 電子郵件的收件人將會收到警示郵件。
- `mailFrom` — 指定電子郵件送件人的身份，這在當系統管理員想要過濾來自 `diskcheck` 的郵件時會很有用。舉例來說，假如您指定 `mailFrom = "Disk Usage Monitor"`，電子郵件將會以『Disk Usage Monitor』的身份傳送給系統管理員。
- `mailProg` — 指定用來傳送郵件警示的郵件程式，舉例來說，假如您指定 `mailProg = "/usr/sbin/sendmail"`，`Sendmail` 將被使用來當作郵件程式。

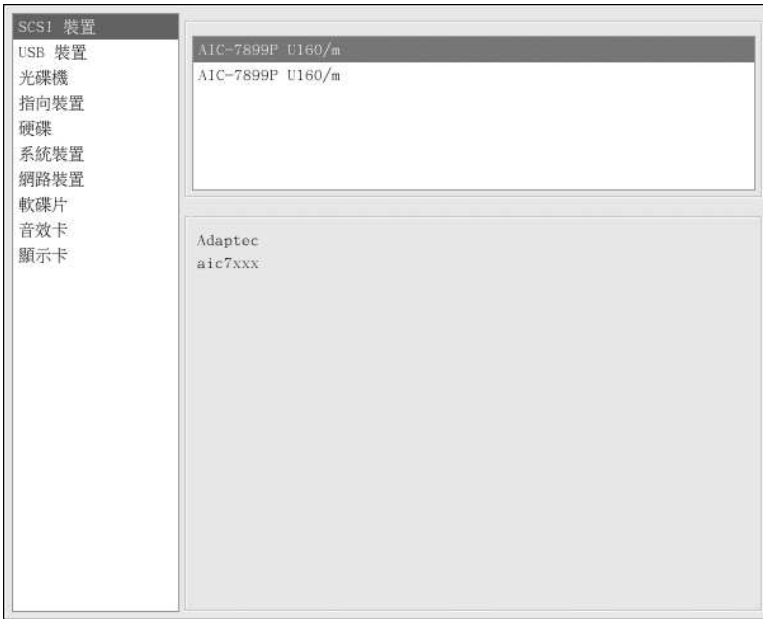
在您更改設定檔之後，您並不需要重新啟動該服務，因為每當執行 `cron` 工作時，它便會被讀取。為了要使 `cron` 工作能夠順利執行，您必須讓 `crond` 服務保持運作。如要知道該系統程式是否執行中，請使用 `/sbin/service crond status` 指令。建議您在系統開機時便啟動這個服務。請參考第14章以取得關於開機時自動啟動 `crond` 服務的詳細資訊。

## 26.4. 硬體

假如您有困難設定您的硬體，或只是想了解您系統上的硬體，您可以使用『**硬體瀏覽器**』應用程式來顯示可被偵測到的硬體。如要從桌面啟動該程式，請選擇『**主選單按鈕**』=>『**系統工具**』=>『**硬體瀏覽器**』，或是在 `shell` 提示符號下輸入 `hwbrowser`。如圖形26-3所示，它會顯示您的光碟機裝置、軟

1. 請參考第28章以取得關於 `cron` 的更多資訊。

碟機、硬碟以及它們的分割區、網路裝置、指向裝置、系統裝置以及顯示卡。點選左邊選單中的類別名稱，則會顯示關於該硬體的資訊。



圖形26-3. 硬體瀏覽器

您也可以使用 `lspci` 指令來列出所有的PCI 裝置，使用 `lspci -v` 指令以取得更詳細的資訊，或 `lspci -vv` 指令以取得相當繁複的輸出。

舉例來說，`lspci` 可以被使用來決定系統顯示卡的製造商、型號以及記憶體容量：

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04) (prog-if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max
Flags: medium devsel, IRQ 16
Memory at f4000000 (32-bit, prefetchable) [size=32M]
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

`lspci` 也可用來決定系統上的網路卡（假如您不知道製造商或型號時）。

## 26.5. 其他的資源

如要學習更多關於收集系統資訊，請參考下列的資源。



### 26.5.1. 已安裝的說明文件

- `ps --help` — 顯示`ps`指令可以使用的選項清單。
- `top`的man page — 輸入`man top`以學習更多關於`top`指令以及它的許多選項。
- `free`的man page — 輸入`man free`以學習更多關於`free`指令以及它的許多選項。
- `df`的man page — 輸入`man df`以學習更多關於`df`指令以及它的許多選項。
- `du`的man page — 輸入`man du`以學習更多關於`du`指令以及它的許多選項。
- `lspci`的man page — 輸入`man lspci`以學習更多關於`lspci`指令以及它的許多選項。
- `/proc` — `/proc`目錄的內容也可被使用來收集詳細的系統資訊，請參考*Red Hat Linux*參考手冊 以取得關於`/proc`目錄的其他資訊。

### 26.5.2. 相關的書籍

- *Red Hat Linux* 系統管理入門; Red Hat, Inc. — 其中含有關於監視資源的一個章節。



使用者可以在Red Hat Linux 中使用**印表機設定工具**來設定一部印表機，這個工具還會維護印表機的設定檔案、列印緩衝器目錄以及列印過濾器。

從9 版本開始，Red Hat Linux 將預設使用CUPS 列印系統，不過仍然有提供之前預設的列印系統-LPRng。假如系統是由之前使用LPRng 的Red Hat Linux 版本所升級，升級的過程將不會以CUPS 取代LPRng，系統將會繼續使用LPRng。

假如系統是由之前使用CUPS 的Red Hat Linux 版本所升級，升級的過程將會保留已設定的佇列，而且系統將會繼續使用CUPS。

**印表機設定工具**可以用來設定CUPS 與LPRng 列印系統，取決於系統的設定。當您套用變更時，它會設定現行的列印系統。

您必須擁有root 權限才能使用**印表機設定工具**，如要啟動這個應用程式，請選擇面板上的『**主選單按鈕**』=>『**系統設定**』=>『**Printing**』，或輸入redhat-config-printer 指令。這個指令將會視該指令是在圖形的X 視窗系統環境或文字介面的主控台執行，以自動決定是否執行圖形化或文字介面的程式。

您可以在shell 提示符號下使用redhat-config-printer-tui 指令來強迫執行**印表機設定工具**為一個文字介面的應用程式。

**重要**

請勿編輯/etc/printcap 檔案或位於/etc/cups/ 目錄中的檔案，每當列印系統程式(lpd 或cups) 啟動或重新啟動時，系統將會動態地建立新的設定檔案。當您套用**印表機設定工具** 應用程式所做的變更時，這些檔案也會動態地建立。

假如您是使用LPRng，而您不想使用**印表機設定工具**來新增一部印表機，請編輯/etc/printcap.local 檔案。/etc/printcap.local 檔案中的紀錄項並不會顯示在**印表機設定工具** 程式中，不過卻會被列印系統程式所讀取。假如您是從之前版本的Red Hat Linux 所升級，您既有的設定檔案會被轉換為由這個應用程式所使用的新格式。每當產生一個新的設定檔案時，便會儲存舊的檔案為/etc/printcap.old。

假如您是使用CUPS，**印表機設定工具**並不會顯示非由**印表機設定工具**所設定的的任何佇列或共享資源，然而它也不會將它們從設定檔案中移除。



圖形27-1. 印表機設定工具

可以設定下列的列印佇列種類：

- **與本機連接的** — 透過並列埠或USB 埠直接與電腦連接的印表機
- **網路連線的CUPS (IPP)** — 可使用Internet Printing Protocol (也稱為IPP) 透過TCP/IP 網路存取印表機 (例如，一部印表機連接到在網路中執行CUPS 的另一部Red Hat Linux 系統)。
- **網路連線的UNIX (LPD)** — 印表機連接至可透過TCP/IP 網路存取的另一個UNIX 系統 (例如，一部印表機連接到在網路中執行LPD 的另一部Red Hat Linux 系統)。
- **網路連線的Windows (SMB)** — 印表機連接至透過SMB 網路分享一部印表機的另一個系統 (例如，一部印表機連接到一部Microsoft™ Windows 的機器)。
- **網路連線的Novell (NCP)** — 印表機連接至使用Novell NetWare 網路技術的另一部系統。
- **網路連線的JetDirect** — 一部印表機透過HP JetDirect (不是經由一部電腦) 直接與網路連接。



**重要**

假如您新增一個列印佇列或修改一個現有的佇列，您必須套用變更以使它們生效。

請點選**套用**的按鈕以儲存您所做的變更並重新啟動列印系統程式，在列印系統程式重新啟動前，所做的變更不會寫入到設定檔案中。或者您可以選擇『**動作**』=>『**套用**』。

## 27.1. 新增一部本機印表機

如要新增一部本機印表機，例如經由並列埠或USB 埠連接至您電腦的印表機，請點選**印表機設定工具**主要視窗中的**新增**按鈕以顯示如圖形27-2 的視窗，再點選**下一步**以繼續。



圖形27-2. 新增一部印表機

在如圖形27-3 所示的視窗中，為印表機輸入一個獨特的名稱到『**名稱**』的文字欄位。印表機名稱不能含有空白且必須以字母開頭，名稱中可以包含字母、數字、引號(-)以及底線(\_)。您還可以為印表機輸入一個簡短的描述，其中可含有空白。



圖形27-3. 選取一個佇列名稱

在點選下一步之後，會出現圖形27-4。請從『選取一個佇列種類』的選單中選擇『與本機連接的』，並選取一個裝置。這裡的裝置通常是以/dev/lp0 代表並列埠的印表機或/dev/usb/lp0 代表USB的印表機。假如清單上沒有出現任何裝置，請點選**重新偵測裝置**來重新偵測您的電腦或點選**自訂裝置**來手動地指定它。最後再點選下一步 以繼續。



圖形27-4. 新增一部本機印表機

下一步是選擇印表機的類型，請跳至 27.7 節 以繼續。

## 27.2. 新增一部IPP 印表機

一部IPP 印表機就是一部連接至在同一網路中執行CUPS 的另一部Linux 系統，或在另一種作業系統上設定使用IPP 的印表機。預設情況下，**印表機設定工具** 會瀏覽網路中任何共享的IPP 印表機。（您可以從下拉式選單中選擇『動作』=>『共享』來更改這個選項。）任何網路連線的IPP 印表機會出現在主要視窗中瀏覽過的佇列。

假如您在列印伺服器有設定一個防火牆，它必須要允許傳送與接收流入的UDP 631 連接埠的連線。假如您在用戶端的機器（傳送列印要求的電腦）有設定一個防火牆，它必須允許於連接埠631 傳送與接收的連線。

假如您停用自動瀏覽的特色，您仍然可以點選**印表機設定工具** 主要視窗中的**新增** 按鈕以顯示如圖形27-2 的視窗來新增一部網路連線的IPP 印表機。再點選**下一步** 以繼續。

在如圖形27-3 所示的視窗中，為印表機輸入一個獨特的名稱到『名稱』的文字欄位。印表機名稱不能含有空白且必須以字母開頭，名稱中可以包含字母、數字、引號(-)以及底線(\_)。您還可以為印表機輸入一個簡短的描述，其中可含有空白。

在點選下一步後，會出現圖形27-5，請從『**選取一個佇列種類**』的選單中選擇『**網路連線的CUPS (IPP)**』。



圖形27-5. 新增一部IPP 印表機

會出現含有下列選項的文字欄位：

- **伺服器** — 印表機所連接之遠端機器的主機名稱或IP 位址。
- **路徑** — 遠端機器上列印佇列的路徑。

點選**下一步**以繼續。

下一步是選擇印表機的類型，請跳至 27.7 節以繼續。



**重要**

網路連線的IPP 列印伺服器必須允許從本機系統的連線，請參考 27.13 節以取得更多資訊。

### 27.3. 新增一個遠端的UNIX (LPD) 印表機

如要新增一部遠端的UNIX 印表機，例如連接到同一網路中的另一部Linux 系統，請點選**印表機設定工具** 主要視窗中的**新增** 按鈕，將會出現如圖形27-2 所示的視窗，再點選**下一步** 以繼續。

在如圖形27-3 所示的視窗中，為印表機輸入一個獨特的名稱到『**名稱**』的文字欄位。印表機名稱不能含有空白且必須以字母開頭，名稱中可以包含字母、數字、引號(-)以及底線(\_)。您還可以為印表機輸入一個簡短的描述，其中可含有空白。

從『**選取一個佇列種類**』的選單中選擇『**網路連線的UNIX (LPD)**』，再點選**下一步**。



圖形27-6. 新增一個遠端的LPD 印表機

會出現含有下列選項的文字欄位：

- **伺服器** — 印表機所連接之遠端機器的主機名稱或IP 位址。
- **佇列** — 遠端的列印佇列，預設的列印佇列通常是lp。

點選**下一步**以繼續。

下一步是選擇印表機的類型，請跳至 27.7 節以繼續。



**重要**

遠端的列印伺服器必須接受來自本機系統列印工作，請參考 27.13.1 節以取得更多資訊。

## 27.4. 新增一部Samba (SMB) 印表機

如要新增一部使用SMB 通訊協定來存取印表機（如連接至一部Microsoft Windows 系統的印表機），請點選**印表機設定工具** 主要視窗中的**新增** 按鈕，便會出現如圖形27-2 的視窗，再點選**下一步** 以繼續。

在如圖形27-3 所示的視窗中，為印表機輸入一個獨特的名稱到『**名稱**』的文字欄位。印表機名稱不能含有空白且必須以字母開頭，名稱中可以包含字母、數字、引號(-)以及底線(\_)。您還可為印表機輸入一個簡短的描述，其中可含有空白。

請從『**選取一個佇列種類**』的選單中選擇『**網路連線的Windows (SMB)**』，再點選**下一步**。假如印表機是連接至一部Microsoft Windows 系統，請選擇這種佇列種類。



圖形27-7. 新增一部SMB 印表機

如圖形27-7 所示，將會自動偵測到SMB 共享資源，並將之列出。點選共享名稱旁的箭號以展開清單。請從展開的清單中選取一部印表機。

假如在清單中找不到您要的印表機，請點選右邊的**指定...** 按鈕，將會出現含有下列選項的文字欄位：

- **工作群組** — 共享印表機所屬的Samba 工作群組名稱。
- **伺服器** — 分享印表機的伺服器名稱。
- **共享** — 您想用來列印的共享印表機名稱，這個名稱必須與遠端Windows 機器上所定義的Samba 印表機名稱相同。
- **使用者名稱** — 您要用來登入以使用印表機的使用者名稱，這個使用者必須存在於Windows 系統中，而且這個使用者必須擁有足夠的權限以使用印表機。Windows 伺服器上典型的預設使用者名稱為**guest**，而Samba 伺服器上則為**nobody**。
- **密碼** — 請輸入『**使用者名稱**』欄位所指定使用者的密碼（假如需要的話）。

點選下一步 以繼續，然後**印表機設定工具** 將會試著連線到共享的印表機。假如共享的印表機需要使用者名稱與密碼的話，則會出現一個對話窗讓您提供一組有效的使用者名稱與密碼。假如發生指定的共享名稱不正確，您也可以在此更改它。假如需要工作群組名稱以用來連線共享資源，您可以在這個對話窗將之輸入。這個對話窗與您點選**指定...** 按鈕時出現的視窗一樣。

下一步是選擇印表機的類型，請跳至 27.7 節 以繼續。



#### 警告

假如您需要一組使用者名稱與密碼，它們以未加密的方式儲存在只能被**root** 與**lpd** 讀取的檔案中。因此假如其他人擁有**root** 權限的話，很有可能被他們讀取使用者名稱與密碼。為了要避免這種情況的發生，用來存取印表機的使用者名稱與密碼不應該與在本機Red Hat Linux 系統中的使用者帳號所使用的使用者名稱與密碼相同。假如它們不相同的話，有可能的安全性問題將會是未經認可的使用印表機。假如該伺服器也有共享檔案，建議您也使用與列印行列不同的密碼。

## 27.5. 新增一部Novell NetWare (NCP) 印表機

如要新增一部Novell NetWare (NCP) 印表機，請點選**印表機設定工具** 主要視窗上的**新增** 按鈕，就會出現如圖形27-1 所示的視窗，再點選**下一步** 以繼續。

在如圖形27-3 所示的視窗中，為印表機輸入一個獨特的名稱到『**名稱**』的文字欄位。印表機名稱不能含有空白且必須以字母開頭，名稱中可以包含字母、數字、引號(-)以及底線(\_)。您還可以用印表機輸入一個簡短的描述，其中可含有空白。

從『**選取一個佇列種類**』選單中選擇『**網路連線的Novell (NCP)**』。



圖形27-8. 新增一部NCP 印表機

會出現含有下列選項的文字欄位：

- **伺服器** — 印表機所連接之NCP系統的主機名稱或IP位址。
- **佇列** — 在NCP系統上印表機的遠端佇列。
- **使用者** — 您要用來登入以使用印表機的使用者名稱。
- **密碼** — 請輸入『使用者』欄位所指定使用者的密碼。

下一步是選擇印表機的類型，請跳至 27.7 節 以繼續。



#### 警告

假如您需要一組使用者名稱與密碼，它們以未加密的方式儲存在只能被root與lpd讀取的檔案中。因此假如其他人擁有root權限的話，很有可能被他們讀取使用者名稱與密碼。為了要避免這種情況的發生，用來存取印表機的使用者名稱與密碼不應該與在本機Red Hat Linux系統中的使用者帳號所使用的使用者名稱與密碼相同。假如它們不相同的話，有可能的安全性問題將會是未經認可的使用印表機。假如該伺服器也有共享檔案，建議您也使用與列印佇列不同的密碼。

## 27.6. 新增一部JetDirect 印表機

如要新增一部JetDirect印表機，請點選**印表機設定工具** 主要視窗中的**新增** 按鈕，將會出現如圖形27-1的視窗，再點選**下一步** 以繼續。

在如圖形27-3所示的視窗中，為印表機輸入一個獨特的名稱到『**名稱**』的文字欄位。印表機名稱不能含有空白且必須以字母開頭，名稱中可以包含字母、數字、引號(-)以及底線(\_)。您還可以為印表機輸入一個簡短的描述，其中可含有空白。

請從『**選取一個佇列種類**』的選單中選擇『**網路連線的JetDirect**』，再點選**下一步**。



圖形27-9. 新增一部JetDirect 印表機

會出現含有下列選項的文字欄位：

- **印表機** — JetDirect 印表機的主機名稱或IP 位址。
- **連接埠** — JetDirect 印表機上聽取列印工作的連接埠，預設連接埠為9100。

下一步是選擇印表機的類型，請跳至 27.7 節以繼續。

## 27.7. 選取印表機型號以完成設定

在選取完印表機的佇列種類後，下一步就是選取印表機的型號。

您將會看到一個類似圖形27-10 的視窗，假如沒有被自動偵測到，請從清單中選取一個型號。印表機是由製造商所分類。請先從下拉式選單中選取印表機的製造商，每當您選擇一個不同的製造商，印表機的型號便會更新，再從清單中選取印表機型號。



圖形27-10. 選取一個印表機型號

基於您所選取的印表機型號，程式將會自動選取印表機驅動程式的建議選項。印表機驅動程式會處理您想要列印的資料為印表機能夠辨識的格式，因為一部印表機直接連接至您的電腦，您需要一個印表機驅動程式以處理要傳送到印表機的資料。

假如您要設定一部遠端的印表機(IPP、LPD、SMB 或NCP)，遠端的列印伺服器通常有它自己的印表機驅動程式，假如您在您的本機電腦上選取一個額外的印表機驅動程式，資料將會被過濾許多次，然後轉換為印表機所無法辨識的格式。

為了確定資料不會被過濾一次以上，請先試著選擇**Generic** 當作製造商，以及『**原始的列印佇列**』或『**Postscript 印表機**』當作印表機型號。在套用變更後，請列印測試頁以測試這個新的設定。假如測試

失敗，遠端的列印伺服器也許沒有設定一個印表機驅動程式。請試著依據遠端印表機的製造商與型號，來試著選取一個印表機驅動程式。在您套用變更後，便可列印一頁測試頁了。



#### 建議

在新增一部印表機後，您可以選擇一個不同的印表機驅動程式，先啟動**印表機設定工具**，再從清單中選取印表機，點選**編輯**後再點選『**印表機驅動程式**』的標籤頁，選擇一個不同的印表機驅動程式，然後再套用變更。

### 27.7.1. 確認印表機的設定

最後一步是確認您的印表機設定，假如所有的設定都正確的話，請點選**套用**來新增列印佇列，或者點選上一步來修改印表機設定。

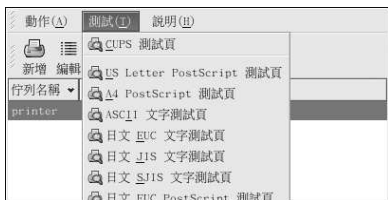
點選主要視窗中的**套用**按鈕以儲存您所做的變更，並重新啟動列印系統程式。在套用變更後，請列印測試頁以確定設定是正確的。請參考 27.8 節以取得更多細節。

假如您需要列印超越基本ASCII字集的字元（包括例如日文等語言所使用的字元），您必須檢視您的驅動程式選項並選取『**預先處理Postscript**』，請參考 27.9 節以取得更多細節。假如您在新增完印表機後想要修改列印佇列，您也可以設定例如紙張大小的選項。

## 27.8. 列印測試頁

在您設定好您的印表機後，您應該要列印測試頁以確定印表機可以正常運作。如要列印測試頁，請從印表機清單中選擇您想要測試的印表機，然後從『**測試**』的下拉式選單中選擇適當的測試頁。


假如您變更印表機驅動程式或修改驅動程式選項，您應該要列印測試頁以測試不同的設定。



圖形27-11. 測試頁選項

## 27.9. 修改既有的印表機

如要刪除一部既有的印表機，請先選取該印表機，再點選工具列上的**刪除**按鈕，該印表機將會從印表機清單中移除。再點選**套用**以儲存變更並且重新啟動列印系統程式。

如要設定預設印表機，請從印表機清單中選取該印表機，再點選工具列上的**預設**按鈕。預設印表機的圖示會出現在清單中預設印表機的『**預設**』欄位。

在新增完印表機後，您可以從印表機清單中選擇該印表機，並點選**編輯**的按鈕來修改該印表機的設定。會出現如圖形27-12所示含有標籤頁的視窗。這個視窗含有所選取印表機的目前設定，請在此做任何需要的變更，再點選**確定**。最後在主要的**印表機設定工具**視窗中點選**套用**的按鈕來儲存變更並重新啟動列印系統程式。



圖形27-12. 編輯一部印表機

### 27.9.1. 佇列名稱

如要重新命名一部印表機或更改它的簡短說明，請更改『佇列名稱』標籤頁中的資料。點選**確定**以回到主要的視窗，您就會發現印表機清單中的印表機名稱已經變更了。點選**套用**的按鈕來儲存變更並重新啟動列印系統程式。

### 27.9.2. 佇列種類

當新增一部印表機以及它的設定時，『佇列種類』的標籤頁會顯示所選取印表機的佇列種類。您可以更改印表機的佇列種類或它的設定，在完成修改後，請點選**確定**以回到主要視窗，再點選**套用**的按鈕來儲存變更並重新啟動列印系統程式。

取決於所選取的佇列種類，將會顯示不同的選項。請參考新增一部印表機的章節，以取得這些選項的描述。

### 27.9.3. 印表機驅動程式

『印表機驅動程式』標籤頁顯示目前所使用的印表機驅動程式。假如您有做任何變更，請點選**確定**以回到主要視窗，再點選**套用**的按鈕來儲存變更並重新啟動列印系統程式。

### 27.9.4. 驅動程式選項

The 『驅動程式選項』標籤頁顯示進階的列印選項，每一個印表機驅動程式的選項皆不同，共同的選項包括了：

- 假如您列印工作的最後一頁並沒有從印表機退出（例如，進紙匣燈閃爍），您應該要選擇『**傳送Form-Feed (FF)**』。假如這樣做仍然無效，試著選擇『**傳送End-of-Transmission (EOT)**』。有些印表機需要設定『**傳送Form-Feed (FF)**』與『**傳送End-of-Transmission (EOT)**』才能退出最後一頁。這個選項只可使用在LPRng 列印系統。
- 假如傳送一個換頁字元(form-feed) 無法使用，您應該要選擇『**傳送End-of-Transmission (EOT)**』。請參考以上的『**傳送Form-Feed (FF)**』。這個選項只可使用在LPRng 列印系統。
- 假如您的列印驅動程式無法辨識某些傳送給它的資料，您應該要選取『**假定未知的資料為文字**』。只當您有列印問題時，才選擇它。如果有選擇這個選項，列印驅動程式會假設任何它無法辨識的資料為

文字，並會試著以文字的格式來列印它。假如您選取這個選項以及『轉換文字成Postscript』，列印驅動程式會假設未知的資料為文字，然後將它轉換為PostScript。這個選項只可使用在LPRng 列印系統。

- 假如您要列印的字元超過基本的ASCII 字元集，而且它們無法被正確的印出（例如日文的字元），您應該要選取『預先處理Postscript』。這個選項將會預先處理(prerender)非標準的PostScript 字型，所以它們就可以被正確的印出。

假如您的印表機不支援您要列印的字型，請試著選取這個選項。例如，當您要列印日文字型到一台非日本製的印表機時，請選取這個選項。

為了要執行這個動作，需要更多的時間。除非您有問題列印正確的字型，否則不要選取它。

假如印表機無法處理PostScript level 3 時，也請您選擇這個選項，這個選項會將之轉換為PostScript level 1。

- 『GhostScript pre-filtering』— 使您可以選擇『No pre-filtering』、『Convert to PS level 1』或『Convert to PS level 2』，萬一印表機無法處理某些PostScript 層級時。這個選項只適用於當PostScript 驅動程式與CUPS 列印系統一起使用時。
- 『轉換文字成Postscript』是預設選取的。假如您的印表機可以印出純文字，當您要列印純文字時，請取消選取它，這樣將會替您節省一些列印時間。假如您是使用CUPS 列印系統，您將無法使用這個選項，因為文字總是被轉換成PostScript。
- 『頁面大小』讓您可以為您的印表機選擇紙張的大小，例如US Letter、US Legal、A3 以及A4。
- 『有效的過濾器區域性』預設為C。假如您要列印日文字元，請選擇ja\_JP。否則，請保留預設值C。
- **Media Source** 預設值為**Printer default**，請更改這個選項以使用不同紙匣的紙張。

修改完驅動程式選項後，點選**確定** 以回到主要視窗。點選**套用** 的按鈕來儲存變更並重新啟動列印系統程式。

## 27.10. 儲存設定檔案

當您使用**印表機設定工具** 儲存印表機設定時，這個應用程式建立自己的設定檔案，可被使用來建立/etc/cups 目錄下的檔案（或者由lpd 所讀取的/etc/printcap 檔案）。您可以使用命令列的選項來儲存或回復**印表機設定工具** 檔案。假如/etc/cups 目錄或/etc/printcap 檔案被儲存並回復到相同的位置，將無法回復印表機設定，因為每次重新啟動列印系統程式，它將會從**印表機設定工具** 特殊的設定檔案來建立一個新的/etc/printcap 檔案。當您要建立系統設定檔案的備份時，請使用下列方法來儲存印表機的設定檔案。假如系統是使用LPRng，而且自訂的設定已經被加入到/etc/printcap.local 檔案中，也應該儲存它為備份系統的一部分。

如要儲存您的印表機設定，請以root 身份輸入以下指令：

```
/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
```

您的組態設定將會儲存為settings.xml 檔案。

假如有儲存這個檔案，可以使用它來回復印表機的設定。這在當印表機設定被刪除或重新安裝Red Hat Linux，或者是多部系統需要相同的印表機設定時，將會很有用。在重新安裝之前，應該儲存這個檔案到另一部系統中。如要回復組態設定，請以root 身份輸入以下指令：

```
/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
```

假如您已經有一個設定檔案（您已經在系統上設定一部以上的印表機），而您試著要匯入另一個設定檔案，原本的設定檔案將會被覆寫。假如您想要保留原本的設定檔案，並且增加設定到已儲存的檔案，您可以使用下列的指令來合併檔案（請以root 身份）：

```
/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
```

您的印表機清單將會含有您之前在系統上設定的印表機以及您從儲存的設定檔匯入的印表機。假如匯入的設定檔案中含有與系統上既有列印行列相同的名稱，匯入檔案中的列印行列將會強制覆寫原有的印表機。

在匯入設定檔案後（不管有無使用merge 指令），您都必須重新啟動列印系統程式。假如您是使用CUPS，請執行下列指令：

```
/sbin/service cups restart
```

假如您是使用LPRng，請執行這個指令：

```
/sbin/service lpd restart
```

## 27.11. 命令列的設定

假如您沒有安裝X，而且您也不想要使用文字介面的設定工具，您可以經由命令列來新增一部印表機。假如您想要從一個程式碼或在kickstart 安裝的%post 階段來新增一部印表機，這個方法將對您很有幫助。

### 27.11.1. 新增一部本機印表機

要新增一部印表機：

```
redhat-config-printer-tui --Xadd-local 選項
```

選項：

**--device=節點**

（必要的）要使用的裝置節點，例如/dev/lp0。

**--make=廠牌**

（必要的）輸入IEEE 1284 MANUFACTURER 字串，如果沒有製造商字串，請輸入在foomatic 資料庫中的印表機製造商名稱。

**--model=型號**

（必要的）輸入IEEE 1284 MODEL 字串，如果沒有型號字串，請輸入在foomatic 資料庫中列出的印表機型號。

**--name=名稱**

（可選的）新列印行列的名稱，假如不指定的話，將會使用基於裝置節點的一個名稱（如“lp0”）。

**--as-default**

（可選的）設定為預設行列。

假如您使用CUPS 當作您的列印系統（預設值），在新增完印表機後，請使用下列指令來啟動/重新啟動列印系統程式：

```
service cups restart
```

假如您使用LPRng 當作您的列印系統，在新增完印表機後，請使用下列指令來啟動/重新啟動列印系統程式：

```
service lpd restart
```

### 27.11.2. 移除一部本機印表機

您也可以經由命令列來移除一個印表機佇列。

以root 身份來移除一個印表機佇列：

```
redhat-config-printer-tui --Xremove-local 選項
```

選項：

`--device=節點`

(必要的) 要使用的裝置節點，例如/dev/lp0。

`--make=make`

(必要的) 輸入IEEE 1284 MANUFACTURER 字串，或者（假如沒有的話）輸入foomatic 資料庫中的印表機製造商名稱。

`--model=型號`

(必要的) 輸入IEEE 1284 MODEL 字串，或者（假如沒有的話）輸入foomatic 資料庫中的所列出的印表機型號。

假如您使用CUPS 當作您的列印系統（預設值），在從**印表機設定工具** 設定中移除印表機後，請重新啟動列印系統程式以使變更生效：

```
service cups restart
```

假如您使用LPRng 當作您的列印系統，在從**印表機設定工具** 設定中移除印表機後，請重新啟動列印系統程式以使變更生效：

```
service lpd restart
```

假如您是使用CUPS，並且已經移除所有的印表機，如果您不再想要執行列印系統程式，請執行下列的指令：

```
service cups stop
```

假如您是使用LPRng，並且已經移除所有的印表機，如果您不再想要執行列印系統程式，請執行下列的指令：

```
service lpd stop
```

## 27.12. 管理列印工作

當您傳送一個列印工作到列印系統程式，例如從**Emacs** 列印文字檔案或從**The GIMP** 列印一個影像檔案，該列印工作將會增加至列印緩衝器佇列。列印緩衝器佇列中含有已經傳送至印表機的列印工作清單以及關於每一個列印要求的資訊（如列印要求的狀態、傳送要求的使用者名稱、傳送要求的系統主機名稱與工作編號等等）。

假如您正在執行一個圖形桌面環境，請點選面板上的『**列印管理員**』圖示來啟動如圖形27-13 所示的『**GNOME 列印管理員**』。



圖形27-13. GNOME 列印管理員

您也可以選擇面板上的『主選單按鈕』=>『系統工具』=>『印表機管理程式』來啟動它。

如要更改印表機的設定，請以滑鼠右鍵點選印表機的圖示，然後選擇『屬性』，便會啟動印表機設定工具。

雙點選一個設定好的印表機來檢視如圖形27-14 所示的列印緩衝器佇列。



圖形27-14. 列印工作清單

如要取消在『GNOME 列印管理員』所列出的一个特定列印工作，請從清單中選取它，再從下拉式選單中選擇『編輯』=>『取消列印文件』。

假如在列印緩衝器中有現行的列印工作，一个印表機提示圖示將會出現在如圖形27-15 所示的桌面面板上的『面板提示區域』。因為它每五秒鐘偵測一次現行的列印工作，對於較短的二印工作也許不會顯示該圖示。

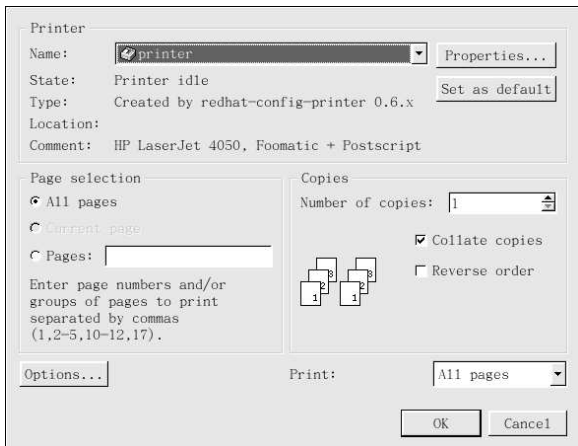


圖形27-15. 印表機提示圖示

點選印表機提示圖示將會啟動『GNOME 列印管理員』，並且顯示目前列印工作的清單。

另外還有一個『列印管理員』的圖示出現在面板上，如要在Nautilus 中列印一個檔案，請先瀏覽該檔案的位置，再以滑鼠將它拖放到面板上的『列印管理員』圖示，便會出現如圖形27-16 所示的視窗，點選**確定** 以開始列印該檔案。





圖形27-16. 列印確認視窗

如要在shell 提示符號下檢視在列印緩衝器中的列印工作清單，請輸入`lpq` 指令。最後的幾行將會如下所示：

```
Rank Owner/ID      Class Job Files  Size Time
active user@localhost+902 A 902 sample.txt 2050 01:20:46
```

#### 範例27-1. `lpq` 指令的輸出範例

假如您想要取消一個列印工作，請使用`lpq` 指令找出列印要求的工作編號，然後使用`lprm` 工作編號 指令來取消該列印工作。舉例來說，`lprm 902` 將會取消範例27-1 中所顯示的列印工作。您必須有適當的權限才能取消一個列印工作，您無法取消由其他使用者啟動的列印工作，除非您在印表機所連接的機器上以`root` 身份登入。

您也可以直接從一個shell 提示符號列印一個檔案，舉例來說，`lpr sample.txt` 指令將會列印出`sample.txt` 文字檔案。列印過濾器會決定該檔案的類型，並將其轉換至印表機所能辨識的格式。

## 27.13. 分享一部印表機

只在您使用CUPS 列印系統時，才能使用印表機設定工具 分享設定選項的功能。如要設定LPRng 的分享功能，請參考 27.13.1 節。

允許網路中不同電腦的使用者列印到您系統上所設定的印表機，這種功能稱為『分享』印表機。預設設定下，使用印表機設定工具 所設定的印表機是沒有分享的。

如要分享一部設定好的印表機，請啟動印表機設定工具，然後從清單中選取一部印表機。然後從選單中選擇『動作』 => 『共享資源』。



#### 請注意

假如您沒有選取任何印表機，選擇『動作』 => 『共享資源』 只會顯示通常出現在『一般』 標籤頁中的全系統性共享資源選項。

在『佇列』的標籤頁中，請選擇分享這個佇列給其他使用者的選項。



圖形27-17. 佇列選項

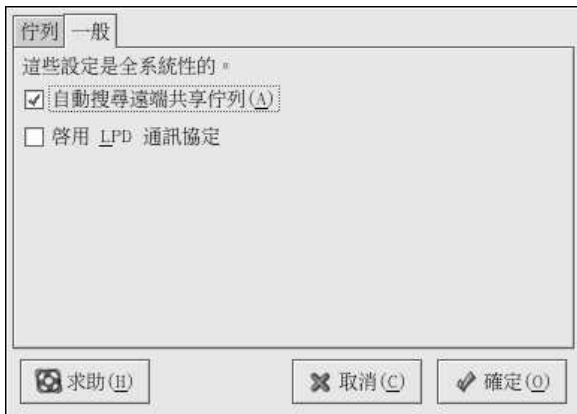
預設情況下，在選取要共享的佇列後，所有的主機都允許列印到共享的印表機。允許網路中的所有系統列印到佇列是一件危險的事，特別是當系統直接連線到網際網路時。建議您更改這個選項，您可以選取**All hosts**的紀錄再點選**編輯** 按鈕來顯示如圖形27-18 所示的視窗。

假如您在列印伺服器上有設定防火牆，它必須允許流入**631 UDP** 埠號的傳送與接收連線。假如您在用戶端（傳送列印要求的電腦）有設定防火牆，它必須允許**631** 埠號傳送與接收的連線。



圖形27-18. 可存取的主機

『一般』的標籤頁可用來做所有印表機的設定，包括**印表機設定工具**中所看不到的印表機。這裡有兩個選項：



圖形27-19. 全系統性的共享選項

- **自動搜尋遠端共享佇列** — 預設選取，這個選項會啟用IPP 瀏覽，也就是說當網路中其他的機器廣播它們所擁有的佇列時，這些佇列將會被自動加入到系統可使用的印表機清單中，由IPP 瀏覽所找到的印表機並不需要其他額外的組態設定。這個選項並不自動分享本機系統上所設定的印表機。
- **啟用LPD 通訊協定** — 這個選項會允許印表機接收來自使用LPD 通訊協定用戶端的列印工作，它是藉由使用cups-lpd 服務，也就是一種xinetd 服務。



警告

假如這個選項已啟用，都會接受來自所有主機的所有列印工作（假如它們是來自一部LPD 用戶端）。

### 27.13.1. 使用LPRng 共享一部印表機

假如您是執行LPRng 列印系統，您必須手動設定共享的機制。如要允許網路中的系統可以列印至一部Red Hat Linux 系統上的印表機，請遵照以下的步驟：

1. 請先建立/etc/accepthost 檔案，在這個檔案中，加入您想要允許列印存取之系統的IP 位址或主機名稱，請以一行一個IP 或主機名稱的方式輸入。
2. 在/etc/lpd.perms 檔案中取消下列這行的註解：  
ACCEPT SERVICE=X REMOTEHOST=</etc/accepthost
3. 重新啟動列印系統程式以使變更生效：  
service lpd restart

### 27.14. 轉換列印系統

如要轉換列印系統，請執行**列印系統轉換器** 應用程式，如要啟動它，請選擇面板上的『主選單按鈕』=> 『系統設定』=> 『更多系統設定』=> **列印系統轉換器**，或在shell 提示符號下（如XTerm 或GNOME 終端機）輸入redhat-switch-printer 指令。

這個程式會自動偵測是否有執行X 視窗系統，假如有的話，程式將會以圖形模式啟動（如圖形27-20 所示）。假如沒有偵測到X，則會以文字模式啟動該程式。如要強制執行文字介面的應用程式，請使用redhat-switch-printer-nox 指令。



圖形27-20. 列印系統轉換器

您可以選取**LPRng** 或**CUPS** 列印系統。在Red Hat Linux 9 中，**CUPS** 為預設值。假如您只安裝一種列印系統，這裡只會顯示這個選項(**CUPS**)。

在您選擇**確定** 來變更列印系統後，所選取的列印系統程式便會在開機時自動啟動，而未選取的列印系統程式則會被停用，所以它不會在開機時啟動。所選取的列印系統程式會啟動，而另一個則會停用，因此使得變更立即生效。

## 27.15. 其他的資源

如想了解更多關於在Red Hat Linux 中列印的資訊，請參考下列的資源。

### 27.15.1. 已安裝的說明文件

- `man printcap` — `/etc/printcap` 印表機設定檔的man page。
- `man lpr` — 使您可以從命令列列印檔案的**lpr** 指令之man page。
- `man lpd` — **LPRng** 列印系統程式的man page。
- `man lprm` — 用來移除**LPRng** 緩衝器佇列之命令列工具的man page。
- `man mpage` — 用來在一張紙上列印多頁之命令列工具的man page。
- `man cupsd` — **CUPS** 列印系統程式的man page。
- `man cupsd.conf` — **CUPS** 列印系統程式設定檔案的man page。
- `man classes.conf` — **CUPS** 的class 設定檔案的man page。

### 27.15.2. 很有用的網站

- <http://www.linuxprinting.org> — *GNU/Linux Printing* 網站中包含了關於在Linux 中列印的大量資訊。
- <http://www.cups.org/> — 關於**CUPS** 的說明文件、FAQ 以及新聞群組。

## 自動工作排程管理

在Linux中，可以設定系統的工作在一個指定的時間、日期或當系統平均負載低於指定的數據時自動執行。Red Hat Linux已預先設定好執行重要的系統工作以保持系統的更新，例如由locate指令使用的slocate資料庫是每日更新的。系統管理員可以使用自動的工作管理來執行定期的備份、監視系統與執行自訂的程式碼等等。

Red Hat Linux中含有四個自動工作管理程式：cron、anacron、at以及batch。

## 28.1. Cron

Cron是一種系統程式(daemon)，它可以依據所設定的時間、日期、月份、星期幾以及星期的結合來排程重覆性工作的執行。

Cron假設系統是在持續開機的情況下，假如在工作排定的時間，系統沒有開機，該工作將不會被執行。如要以時間的週期而不是確切的時間來設定工作的話，請參考28.2節。如要排定僅執行一次的工作，請參考28.3節。

如要使用cron的服務，您必須要安裝vixie-cron RPM套件，而且crond的服務必須在執行中。要查看該套件是否已安裝，請使用rpm -q vixie-cron指令；要查看服務是否在執行中，請使用/sbin/service crond status指令。

### 28.1.1. 設定Cron的工作排程

cron的主要設定檔案/etc/crontab包含了以下這幾行：

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

一開始的四行是用來設定cron工作要執行之環境的變數，例如SHELL變數的值將告訴系統要使用那一個shell環境（在此為bash shell），而PATH變數則定義要用來執行指令的路徑。cron工作的輸出將會以電子郵件寄到MAILTO變數所定義的使用者名稱，假如MAILTO變數定義為一個空的字串(MAILTO="")，將不會傳送任何的電子郵件。HOME變數可用來設定執行指令或程式碼時要使用的家目錄。

在/etc/crontab檔案中的每一行都代表一項工作，而且都有相同的格式：

分 時 日期 月份 星期幾 指令

- 分 — 從0到59的任何整數
- 時 — 從0到23的任何整數
- 日期 — 從1到31的任何整數（假如有指定月份的話，必須是一個有效的日期）
- 月份 — 從1到12的任何整數（或者是月份名稱的縮寫，如jan、feb等等）

- 星期幾 — 從0到7的任何整數，0或7代表星期日（或者是縮寫名稱，如sun、mon等等）
- 指令 — 要執行的指令（這裡的指令可以是一個例如ls /proc >> /tmp/proc的指令或用來執行您所撰寫之程式碼的指令。）

對於以上的任何數值，可以使用一個星號(\*)來指定所有有效的數值，例如在月份的一個星號代表在其他數值的範圍內每月執行該指令。

整數之間的一個引號(-)代表整數的一個範圍，例如1-4代表整數1, 2, 3與4。

以逗號(,)分隔開的一系列數值代表一個清單，例如3, 4, 6, 8代表這四個特定的整數。

斜線符號(/)用來代表時間間隔的數值，只要在一個數值範圍之後加上/<整數>即可在該範圍內跳過該整數所指定的數值，例如0-59/2在分鐘的欄位中可用來定義每隔兩分鐘執行一次工作。間隔的數值也可以使用一個星號，如在月份欄位的數值\*/3可以使用來每三個月執行一次工作。

任何以井號(#)開頭的行都是註解，並且都不會被執行。

如您所看到的/etc/crontab檔案，它使用run-parts程式碼來分別執行/etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly與/etc/cron.monthly目錄中以每小時、每天、每星期或每月為基礎的程式碼。這些目錄中的檔案應該都是shell程式碼。

假如一個cron的工作需要在預計的時間執行，而不是以每小時、每天、每星期或每月為基礎，可以將它增加至/etc/cron.d目錄中，在這個目錄中的所有檔案都使用與/etc/crontab檔案中相同的語法，請參考範例28-1以取得相關範例。

```
# record the memory usage of the system every monday
# at 3:30AM in the file /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# run custom script the first day of every month at 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

### 範例28-1. Crontab 的範例

root 之外的使用者可以使用crontab工具來設定cron的工作，所有使用者定義的crontabs都儲存在/var/spool/cron目錄中，並且由建立它們的使用者之使用者名稱來執行。如要以一個使用者來建立一個crontab，請以該使用者登入並輸入crontab -e指令以使用VISUAL或EDITOR環境變數所指定的編輯器來編輯使用者的crontab。這個檔案使用與/etc/crontab檔案相同的格式。在儲存crontab所作的變更後，該crontab會依據使用者名稱儲存起來，並寫入到/var/spool/cron/username檔案中。

cron系統程式會在每一分鐘檢查/etc/crontab檔案、/etc/cron.d/與/var/spool/cron目錄是否有任何的變更，假如有任何的變更，它們將會被載入記憶體。因此如果在crontab檔案更改後，並不需要重新啟動這個系統程式。

## 28.1.2. Cron 的存取控制

/etc/cron.allow與/etc/cron.deny檔案是用來限制使用者對cron的存取權限。這兩個存取控制檔案的格式是在每一行放置一個使用者名稱，兩個檔案中都不允許有空白字元。假如在修改存取控制檔案後，並不需要重新啟動cron系統程式(cron)，這些存取控制檔案將在使用者試著要增加或刪除一個cron工作時被讀取。

root使用者隨時都可以使用cron，不管使用者的名稱是否有列在存取控制檔案中。

假如cron.allow檔案存在的話，只有在其中列出的使用者允許使用cron，而cron.deny檔案便會被忽略。

假如cron.allow檔案不存在的話，所有在cron.deny檔案中列出的使用者都不允許使用cron。

### 28.1.3. 啟動與停止服務

如要啟動cron 服務，請使用/sbin/service crond start 指令。如要停止這項服務，您可以使用/sbin/service crond stop 指令。在此建議您在系統開機便啟動這項服務，請參考第14章 以取得關於在開機時自動啟動cron 服務的細節。

## 28.2. Anacron

Anacron 是一種類似cron 的工作排程器，不過它並不需要系統持續性的開機。可以使用它來執行通常由cron 執行的每天、每星期以及每月的工作。

如要使用Anacron 服務，您必須安裝anacron RPM 套件，而且anacron 的服務必須在執行中。如要知道這個套件是否已安裝，請使用rpm -q anacron 指令；如要知道這個服務是否在執行中，請使用/sbin/service anacron status 指令。

### 28.2.1. 設定Anacron 的工作

Anacron 的工作列出在/etc/anacrontab 設定檔中，這個檔案中的每一行都對應到一項工作，並且為以下這種格式：

```
period delay job-identifier command
```

- period — 要執行指令的頻率（以天表示）
- delay — 延遲的時間（以分鐘表示）
- job-identifier — 執行工作的描述，使用於Anacron 的訊息以及當作該項工作之時間戳記檔案的名稱，其內可包含任何非空白的字元（除了斜線符號外）
- command — 要執行的指令

對於每一個工作，Anacron 將會視該工作在設定檔所指定的period 的時間中是否已經執行過，假如它沒有在所給予的時間中執行的話，Anacron 會在等待delay 欄位所指定的分鐘後執行command 欄位所指定的指令。

在該工作執行完畢後，Anacron 將會紀錄日期到/var/spool/anacron 目錄下的一個時間戳記檔案。在此只會用到日期（而不是時間），而job-identifier 的值會被使用來當作該檔案的檔名。

如cron 的設定檔案，像是SHELL 與PATH 的環境變數可以定義在/etc/anacrontab 檔案的頂端。

如下為預設的設定檔案：

```
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# These entries are useful for a Red Hat Linux system.
1 5 cron.daily run-parts /etc/cron.daily
7 10 cron.weekly run-parts /etc/cron.weekly
30 15 cron.monthly run-parts /etc/cron.monthly
```

圖形28-1. 預設的anacrontab

如圖形28-1 所示，Red Hat Linux 的 `anacron` 是設定來以確定每日、每週以及每月的 `cron` 工作都能執行。

### 28.2.2. 啟動與停止服務

如要啟動 `anacron` 的服務，請使用 `/sbin/service anacron start` 指令；如要停止服務，可以使用 `/sbin/service anacron stop` 指令。在此建議您在開機時即刻啟動該項服務，請參考第14章以取得關於在開機時自動啟動 `anacron` 服務的細節。

## 28.3. At 與 Batch

`cron` 與 `anacron` 是用來排程重複發生的工作，`at` 指令是用來排定在一個特定時間執行的一項工作。`batch` 指令是用來排定當系統的平均負載低於0.8時所執行的一項工作。

如要使用 `at` 或 `batch`，您必須安裝 `at RPM` 套件，而且 `atd` 服務必須在執行中。如要查看該套件是否已經安裝，請使用 `rpm -q at` 指令；如要查看該項服務是否正在執行中，請使用 `/sbin/service atd status` 指令。

### 28.3.1. 設定 At 的工作

如要排定在一個特定時間執行的一項工作，請輸入 `at time` 指令，這裡的 `time` 就是要執行指令的時間。

引數 `time` 可以是下列的其中一種：

- `HH:MM` 格式— 舉例來說，`04:00` 表示4:00AM。假如該時間已經過了，它將會在隔天的同一時間執行。
- `midnight` — 表示12:00AM。
- `noon` — 表示12:00PM。
- `teatime` — 表示4:00PM。
- 『月份名稱日期年份』的格式— 例如，`January 15 2002` 表示2002年的1月15日，在此的年份是可省略的。
- `MMDDYY`、`MM/DD/YY` 或 `MM.DD.YY` 格式— 例如 `011502` 代表2002年1月15日。
- `now + 時間`— 以分鐘、小時、天數或週數指定時間。舉例來說，`now + 5 days` 表示該指令將會在五天後的同一時間執行。

必須先指定時間，其後再接可省略的日期，如需關於時間格式的更多資訊，請閱讀 `/usr/share/doc/at-<版本>/timespec` 的文字檔。

在輸入含有時間引數的 `at` 指令後，會出現 `at>` 提示符號，請在其後輸入要執行的指令，並按下 `[Enter]` 按鍵，再按下 `Ctrl-D`。在此可以指定一個以上的指令，只要在按下 `[Enter]` 按鍵後輸入要執行的指令即可。在輸入所有的指令之後，按下 `[Enter]` 鍵以換至下一行，再按下 `Ctrl-D` 結束。除此之外，可以在提示符號下輸入 `shell` 程式碼，在程式碼每一行的最後按下 `[Enter]` 鍵。假如輸入一個程式碼，將會使用在該使用者的 `SHELL` 環境設定的 `shell`，如使用者的登入 `shell` 或 `/bin/sh`（端視何者先被找到）。

假如這些指令或程式碼試著要顯示資訊到標準輸出，這輸出將會以電子郵件寄給使用者。

使用 `atq` 的指令來檢視等待中的工作，請參考 28.3.3 節以取得更多資訊。

您也可以限制使用 `at` 指令，請參考 28.3.5 節以取得細節。



### 28.3.2. 設定Batch 的工作

如要在系統的平均負載低於0.8時執行一個一次性的工作，請使用batch 指令。

在輸入batch 指令後，將會出現at> 提示符號，再來請輸入要執行的指令，並按下[Enter] 鍵，最後再按下Ctrl-D。在此可以指定一個以上的指令，只要在按下[Enter] 按鍵後輸入要執行的指令即可。在輸入所有的指令之後，按下[Enter] 鍵以換至下一行，再按下Ctrl-D 結束。除此之外，可以在提示符號下輸入shell 程式碼，在程式碼每一行的最後按下[Enter] 鍵。假如輸入一個程式碼，將會使用在該使用者的SHELL 環境設定的shell，如使用者的登入shell 或/bin/sh（端視何者先被找到）。當平均負載低於0.8時，將會執行這些指令或程式碼。

假如這些指令或程式碼試著要顯示資訊到標準輸出，這輸出將會以電子郵件寄給使用者。

使用atq 的指令來檢視等待中的工作，請參考 28.3.3 節 以取得更多資訊。

您也可以限制使用batch 指令，請參考 28.3.5 節 以取得細節。

### 28.3.3. 檢視等待中的工作

如要檢視等待中的at 與batch 工作，請使用atq 指令，它將列出等待中的工作，每一行顯示一項工作。每一行都為以下這種格式：工作序號、日期、小時、工作的等級與使用者名稱。每一個使用者只可以檢視他們自己設定的工作。假如是root 使用者執行atq 指令，所有使用者的全部工作都將會列出來。

### 28.3.4. 其他的命令列選項

at 與batch 的其他命令列選項包括：

選項	說明
-f	從一個檔案來讀取指令或shell 程式碼，而不是在提示符號指定它們。
-m	當工作完成後，傳送電子郵件給使用者。
-v	顯示將要執行工作的時間。

表格28-1. at 與batch 的命令列選項

### 28.3.5. At 與Batch 的存取控制

可以使用/etc/at.allow 與/etc/at.deny 檔案來限制at 與batch 指令的存取使用。這兩個存取控制檔案的格式是在每一行放置一個使用者名稱，兩個檔案中都不允許有空白字元。假如在修改存取控制檔案後，並不需要重新啟動at 系統程式(atd)，這些存取控制檔案將在使用者試著執行at 或batch 指令時被讀取。

root 使用者隨時都可以執行at 與batch 指令，不管使用者的名稱是否有列在存取控制檔案中。

假如at.allow 檔案存在的話，只有在其內有列出的使用者允許使用at 或batch，而at.deny 檔案則會被忽略。

假如at.allow 檔案不存在的話，所有在at.deny 列出的使用者都不允許使用at 或batch。

### 28.3.6. 啟動與停止服務

如要啟動at 服務，請使用/sbin/service atd start 指令；如要停止該項服務，請使用/sbin/service atd stop 指令。在此建議您在開機時即刻啟動這個服務，請參考第14章 以取得關於在開機時自動啟動cron 服務的細節。

## 28.4. 其他的資源

如要學習更多關於自動工作排程的資訊，請參考下列的資源。

### 28.4.1. 已安裝說明文件

- `cron` 的 `man page` — `cron` 的概要
- 第一與第五部份 `crontab` 的 `man page` — 在第一部份的 `man page` 包含 `crontab` 檔案的概要。在第五部份的 `man page` 則包含該檔案的格式以及一些範例的紀錄項。
- `/usr/share/doc/at-<版本>/timespec` 含有關於可以用來指定 `cron` 工作之時間的更多詳細的資訊。
- `anacron` 的 `man page` — 含有關於 `anacron` 的描述以及它的命令列選項。
- `anacrontab` 的 `man page` — `anacron` 設定檔案的概要。
- `/usr/share/doc/anacron-<版本>/README` — 描述 `Anacron` 以及它的用處。
- `at` 的 `man page` — `at` 與 `batch` 指令的描述以及它們的命令列選項。

『紀錄檔案』是含有關於系統訊息的檔案，包括其上所執行的核心、服務與應用程式。不同的紀錄檔案含有不同的資訊，舉例來說，有一個預設的系統紀錄檔案、一個專門紀錄安全性訊息的紀錄檔以及用於cron 定時工作的紀錄檔。

當您試著要故障排除系統的問題時，紀錄檔案是很有用的，例如當您試著要載入一個核心驅動程式或者要搜尋未經授權的登入嘗試。這個章節將探討紀錄檔案位於何處、如何檢視紀錄檔案，以及在紀錄檔案中該找出何種訊息。

有些紀錄檔案是由稱為syslogd 的系統程式所控制的，由syslogd 所維護的紀錄訊息清單可在/etc/syslog.conf 設定檔案中找到。

## 29.1. 尋找紀錄檔案

大部分的紀錄檔案都放置在/var/log 目錄中，例如httpd 與samba 的某些應用程式在/var/log 目錄中含有一個目錄以存放它們的紀錄檔案。

有注意到紀錄檔案目錄中的許多檔案都有一個號碼在後面，這些檔案是當紀錄檔案循環時所建立的。logrotate 套件含有一個cron 工作根據/etc/logrotate.conf 設定檔案與/etc/logrotate.d 目錄中的設定檔案來自動循環紀錄檔案。預設情況下，它是設定為每一個禮拜循環一次的，並且保留之前四個禮拜的紀錄檔案。

## 29.2. 檢視紀錄檔案

大部分的紀錄檔案都是純文字的格式，您可以使用任何的文字編輯器（如Vi 或Emacs 來檢視它們。有些紀錄檔案可被系統上的所有使用者讀取；然而需要root 權限才能讀取大部分的紀錄檔案。

如要在一個互動式的即時應用程式檢視系統紀錄檔案，您可以使用紀錄檔檢視器。如要啟動這個應用程式，請選擇面板上的『主選單按鈕』=> 『系統工具』=> 『系統紀錄』，或是在shell 提示符號下輸入redhat-logviewer 指令。



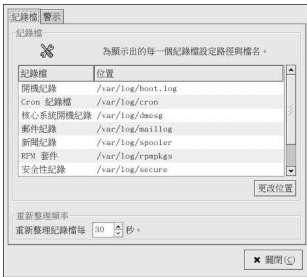
圖形29-1. 紀錄檔檢視器

這個應用程式只會顯示既有的紀錄檔案，因此這個清單也許與圖形29-1 所示的有所不同。如要檢視這個應用程式可以檢視的紀錄檔案完整清單，請參考它的設定檔案/etc/sysconfig/redhat-logviewer。

預設情況下，目前檢視中的紀錄檔案是每隔30秒重新整理一次的。如要更改這個數值，請選擇程式選單上的『編輯』=>『選項』，將會出現如圖形29-2所示的視窗。在『紀錄檔』的標籤頁中，點選重新整理頻率旁邊的上下箭號來更改它。點選關閉以回到主要的視窗，所變更的重新整理頻率將會立即生效，如要手動地重新整理目前檢視中的檔案，請選擇『檔案』=>『馬上重新整理』或按下[Ctrl]-[R]的按鈕組合。

如要以關鍵字過濾紀錄檔案的內容，請在『過濾器』的文字欄位輸入關鍵字，再點選過濾器的按鈕。點選還原以重設內容。

您也可以以在『紀錄檔』的標籤頁中更改應用程式之紀錄檔案的位置。從清單中選取紀錄檔案，再點選更改位置的按鈕，再輸入該紀錄檔案的新位置或點選瀏覽的按鈕來使用檔案選取對話窗來找出檔案的新位置。點選確定以回到『選項』的視窗，再點選關閉以回到主要的視窗。



圖形29-2. 紀錄檔案的位置

### 29.3. 檢查紀錄檔案

紀錄檔檢視器可以設定以顯示一個警示圖示在含有警示關鍵字的該行前面。如要增加警示字元，請在程式選單上選擇『編輯』=>『選項』，然後點選『警示』的標籤頁，再點選新增按鈕來增加一個警示字元。如要刪除一個警示字元，請從清單中選取一個字元，再點選刪除。



圖形29-3. 警示

Red Hat Linux 核心是由Red Hat 核心開發小組自訂建立的，以確保它與支援硬體之整合性與相容性。在Red Hat 釋放一個核心前，它必須通過一個嚴密的品質保證測試。

Red Hat Linux 核心是包裝為RPM 格式，使得使用者可以容易地升級與校驗它們。舉例來說，當安裝完一個由Red Hat, Inc. 散佈的kernel RPM 套件時，將會建立一個initrd 映像檔；因此並不需要在安裝一個不同的核心後使用mkinitrd 指令。它也會修改開機管理程式（不管是GRUB 或LILO）設定檔案來含括新安裝的核心。

這個章節只討論在x86 系統上升級核心所需進行的步驟。



警告

建立一個自訂的核心並不受到Red Hat Linux 安裝支援小組的支援，如需關於從原始碼建立自訂核心的更多資訊，請參考附錄A。

### 30.1. 2.4 版的核心

Red Hat Linux 中含有一個自訂的2.4 版核心，它提供了下列的特色：

- 核心原始碼的目錄在於/usr/src/linux-2.4/，而不是/usr/src/linux/。
- 支援ext3 檔案系統。
- 支援多處理器(SMP)。
- 支援USB。
- 初步支援IEEE 1394（也稱為FireWire™ 裝置）。

## 30.2. 準備進行升級

在升級核心之前，有幾個步驟必須先考慮一下。第一個步驟是確定該系統有一片可使用的開機片，萬一有問題發生時。假如開機管理程式沒有妥善設定以開機新的核心，在缺少開機片的情況下，系統將無法開機進入Red Hat Linux。

如要建立開機片，請在shell 提示符號下以root 登入，然後輸入以下指令：

```
/sbin/mkbootdisk `uname -r`
```



建議

請參考mkbootdisk 的man page，以取得更多選項的資訊。

使用開機片重新啟動系統，並且在繼續之前確定該開機片可以使用。

希望用不著該開機片，不過請將之存放在一個安全的地方，以防萬一。

如要找出已經安裝那一個核心套件，請在shell 提示符號下執行下列指令：

```
rpm -qa | grep kernel
```

輸出將會包含下列套件的某些或全部（取決於之前執行的安裝類型，版本號碼與套件也會有所不同）：

```
kernel-2.4.20-2.47.1
kernel-debug-2.4.20-2.47.1
kernel-source-2.4.20-2.47.1
kernel-doc-2.4.20-2.47.1
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.20-2.47.1
```

從輸出中您便可以決定該下載那一個套件以進行核心升級，至於單一處理器的系統，您只需要kernel 套件。

假如電腦中含有多個微處理器，必須安裝含有多處理器支援的kernel-smp 套件，才能使系統使用一個以上的微處理器。也強烈建議您安裝kernel 套件，以免多處理器的核心無法在系統上正常運作。

假如電腦中含有大於4GB 的記憶體容量，必須安裝kernel-bigmem 套件才能使系統使用超過4GB 的記憶體空間。而且也強烈建議您安裝kernel 套件，以當作除錯用途。kernel-bigmem 套件目前只為i686 的主機架構建立。

假如需要PCMCIA 的支援（例如筆記型電腦），您則需要kernel-pcmcia-cs 套件。

除非您需要重新編譯核心或系統是用作核心開發的，您並不需要kernel-source 套件。

kernel-doc 套件含有核心開發的說明文件（非必要的），假如系統是用作核心開發的話，則建議您安裝它。

kernel-util 套件含有可用來控制核心或系統硬體的工具程式，它也不是必要的。

Red Hat 為不同的x86 版本建立最佳化的核心。選項有用於AMD Athlon™ 與AMD Duron™ 系統的athlon、用於Intel® Pentium® II, Intel® Pentium® III 與Intel® Pentium® 4 系統的i686 以及用於Intel® Pentium® and AMD K6™ 系統的i586。假如不知道x86 系統的版本，請使用為i386 版本建立的核心；它是為所有x86 為主的系統所建立的。

x86 版本的RPM 套件包含在檔名中，舉例來說，kernel-2.4.20-2.47.1.athlon.rpm 是建立給AMD Athlon™ 與AMD Duron™ 系統使用的，而kernel-2.4.20-2.47.1.i686.rpm 是建立給Intel® Pentium® II, Intel® Pentium® III 與Intel® Pentium® 4 系統使用的。在決定好需要那一個套件以用作核心升級後，請為kernel, kernel-smp 與kernel-bigmem 套件選取適當的主機架構，而對其他的套件使用i386 版本。

### 30.3. 下載欲升級的核心

有許多種方法可用來決定是否有系統可使用的更新核心。

- 請連線至<http://www.redhat.com/apps/support/errata/>，並選擇Red Hat Linux 適當的版本，然後檢視其中的errata。核心的errata 通常是在**Security Advisories** 部份中，從errata 清單中點選核心errata 以檢視詳細的errata 報告。在errata 報告中，有一個必要的RPM 套件清單，以及一個連結以從Red Hat 的FTP 站台下載。您也可以從Red Hat 的FTP 映射站台下載它們，映射站台的清單可在以下網址找到：<http://www.redhat.com/download/mirror.html>。
- 使用Red Hat Network 來下載核心的RPM 套件，並且安裝它。Red Hat Network 將會下載最新的核心，還會升級系統中的核心，甚至建立一個初始的虛擬磁碟(RAM disk)映像檔（假如需要的話），並且設定開機管理程式以啟動新的核心。如需更多資訊，請參考 <http://www.redhat.com/docs/manuals/RHNetwork/> 的 *Red Hat Network User Reference Guide*。

假如您是從Red Hat Linux errata 網頁下載RPM 套件，或者您只是使用Red Hat Network 來下載套件，請往後參閱 30.4 節。假如您使用Red Hat Network 來下載以及安裝更新的套件，請遵照 30.5 節與 30.6 節中的指示，除了不變更預設要啟動的核心，因為Red Hat Network 已經自動變更預設啟動的核心為較新的版本。

## 30.4. 執行核心升級

在取得所有需要的套件後，您便可開始升級現有的核心了。請以root身份在shell提示符號下，轉換至含有核心RPM套件的目錄，然後遵照以下步驟。



**重要**

強烈建議您保留舊的核心，以免新的核心有任何的問題。

請使用-i的引數在rpm指令中以保留舊的核心，假如您使用-U選項來升級kernel套件，將會覆寫目前已安裝的核心。（核心版本與x86版本也許會不同）：

```
rpm -ivh kernel-2.4.20-2.47.1.i386.rpm
```

假如系統是一部多處理器的系統，也請您安裝kernel-smp套件（核心版本與x86版本也許會不同）：

```
rpm -ivh kernel-smp-2.4.20-2.47.1.i386.rpm
```

假如該系統是i686為主的，並且含有超過4GB的記憶體，也請您安裝專為i686主機架構建立的kernel-bigmem套件（核心版本也許會不同）：

```
rpm -ivh kernel-bigmem-2.4.20-2.47.1.i686.rpm
```

假如您也要升級kernel-source, kernel-docs或kernel-utils套件，也許並不需要舊的版本，您可以使用下列指令來升級這些套件（版本號碼也許會不同）：

```
rpm -Uvh kernel-source-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-docs-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-utils-2.4.20-2.47.1.i386.rpm
```

假如系統需要PCMCIA支援（如一部筆記型電腦），請您安裝kernel-pcmcia-cs套件，並保留舊的版本。假如您使用-i選項，通常會傳回套件衝突，因為舊的核心需要這個套件來啟動含有PCMCIA支援的系統。為了要避免這種情況，請使用--force選項（版本號碼也許會不同）：

```
rpm -ivh --force kernel-pcmcia-cs-3.1.24-2.i386.rpm
```

下一步便是確認是否已建立初始的虛擬磁碟映像檔，請參考 30.5節以得到更詳細資訊。

## 30.5. 校驗初始的虛擬磁碟映像檔

假如系統使用ext3檔案系統或一個SCSI控制器，您便需要一個初始的虛擬磁碟映像檔。這個初始虛擬磁碟的目的是在核心存取通常放置模組的裝置前，使得模組化的核心可以存取開機時所需的模組。

您可以使用mkinitrd指令來建立初始的虛擬磁碟，然而如果您是使用由Red Hat, Inc. 散佈的RPM套件來進行安裝或升級核心以及相關的套件，這個步驟已經自動執行過了；因此您並不需要手動地執行它。如要確定是否已經建立，請使用ls -l /boot指令以查看已經建立了initrd-2.4.20-2.47.1.img檔案（版本號碼必須符合剛剛安裝的核心版本）。

下一步是確認開機管理程式是否已經設定為啟動新安裝的核心，請參考 30.6節以取得詳細資訊。

### 30.6. 校驗開機管理程式

假如有安裝開機管理程式的話，kernel RPM 套件將設定GRUB 或LILO 以啟動全新安裝的核心。然而它並不設定開機管理程式預設開機新的核心。

最好要確定開機管理程式已經正確地設定，這是很重要的步驟，假如開機管理程式設定不正確，系統將無法正確地開機進入Red Hat Linux。假如發生這種情況，請以先前建立的開機片啟動系統，然後試著再次設定開機管理程式。

#### 30.6.1. GRUB

假如使用GRUB 當作開機管理程式，請確認/boot/grub/grub.conf 檔案中含有與剛才安裝之kernel 套件相同版本的一個title 部份（假如也有安裝kernel-smp 或kernel-bigmem 套件，該部份也會存在）：

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
#   all kernel and initrd paths are relative to /boot/, eg.
#   root (hd0,0)
#   kernel /vmlinuz-version ro root=/dev/hda2
#   initrd /initrd-version.img
#boot=/dev/hda
default=3
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-2.47.1)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-2.47.1 ro root=LABEL=/
    initrd /initrd-2.4.20-2.47.1.img
title Red Hat Linux (2.4.20-2.30)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-2.30 ro root=LABEL=/
    initrd /initrd-2.4.20-2.30.img
```

假如有建立另一個/boot 分割區，核心與initrd 映像檔的路徑則會對應到該/boot 分割區。

請注意預設值並非設定為新的核心，如要設定GRUB 預設啟動新的核心，請更改default 變數的數值為含有新核心之標題號碼。該號碼以0 開始記數，例如新的核心是位於第二個部份，請設定default 的值为1。

藉由重新啟動電腦來開始測試新的核心，並監視開機訊息以確定有正確偵測到系統的硬體。

#### 30.6.2. LILO

假如使用LILO 當作開機管理程式，請確認/etc/lilo.conf 檔案中含有與剛才安裝之kernel 套件相同版本的一個image 部份（假如也有安裝kernel-smp 或kernel-bigmem 套件，該部份也會存在）：

```
prompt
timeout=50
default=2.4.20-2.30
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear

image=/boot/vmlinuz-2.4.20-2.47.1
    label=2.4.20-2.47.1
```



```
initrd=/boot/initrd-2.4.20-2.47.1.img
read-only
append="root=LABEL=/"

image=/boot/vmlinuz-2.4.20-2.30
label=2.4.20-2.30
initrd=/boot/initrd-2.4.20-2.30.img
read-only
append="root=LABEL=/"
```

請注意預設值並非設定為新的核心，如要設定LILO預設啟動新的核心，請更改default的數值為含有新核心之image部份的label數值。然後以root身份執行/sbin/lilo指令以使變更生效。該指令的輸出將會如下所示：

```
Added 2.4.20-2.47.1 *
Added linux
```

在2.4.20-2.47.1之後的\*符號代表位於該部份的核心是LILO將預設啟動的核心。

藉由重新啟動電腦來開始測試新的核心，並監視開機訊息以確定有正確偵測到系統的硬體。



Linux 核心是一種模組化的設計，在開機時只有一個最小的常駐核心會被載入到記憶體中。因此當使用者要求常駐核心中不存在的特色時，便會動態地載入一個『核心模組』（有時候稱為一個『驅動程式』）到記憶體中。

在安裝過程中，會偵測系統上的硬體，依據這次的偵測以及由使用者提供的資訊，安裝程式會決定那些模組需要在開機時載入。安裝程式會設定一個動態的載入機制以方便運作。

假如在安裝完成後加入新的硬體，而該硬體需要一個核心模組，系統需要經過設定以為新的硬體載入適當的核心模組。當含有新硬體的系統開機時，便會執行 **Kudzu** 程式來偵測新的硬體（假如有受支援的話），並且為其設定一個模組。您也可以編輯 `/etc/modules.conf` 模組設定檔案來手動地指定模組。



#### 請注意

使用來顯示 X 視窗系統介面的顯示卡是 `XFree86` 套件的一部分，並不屬於核心，因此這個章節不適用它們。

舉例來說，假如一部系統含有一個 `SMC EtherPower 10 PCI` 網路介面卡，模組設定檔案將會包含以下這一行：

```
alias eth0 tulip
```

假如新增第二張網路卡到系統上，並且該卡與第一張卡相同，請新增以下這一行到 `/etc/modules.conf` 檔案中：

```
alias eth1 tulip
```

請參閱 *Red Hat Linux* 參考手冊 以找出以字母順序排列的核心模組清單，以及模組所支援的硬體。

### 31.1. 核心模組工具程式

假如有安裝 `modutils` 套件，您便可以使用一組用來管理核心模組的指令，請使用這些指令以決定模組是否被成功載入，或者當您為一個新的硬體測試不同的模組時。

`/sbin/lsmmod` 指令將會顯示目前已經載入的模組清單，例如：

Module	Size	Used by	Not tainted
<code>iptable_filter</code>	2412	0 (autoclean)	(unused)
<code>ip_tables</code>	15864	1 [iptable_filter]	
<code>nfs</code>	84632	1 (autoclean)	
<code>lockd</code>	59536	1 (autoclean)	[nfs]
<code>sunrpc</code>	87452	1 (autoclean)	[nfs lockd]
<code>soundcore</code>	7044	0 (autoclean)	
<code>ide-cd</code>	35836	0 (autoclean)	
<code>cdrom</code>	34144	0 (autoclean)	[ide-cd]
<code>parport_pc</code>	19204	1 (autoclean)	
<code>lp</code>	9188	0 (autoclean)	
<code>parport</code>	39072	1 (autoclean)	[parport_pc lp]
<code>autofs</code>	13692	0 (autoclean)	(unused)
<code>e100</code>	62148	1	
<code>microcode</code>	5184	0 (autoclean)	
<code>keybdev</code>	2976	0 (unused)	

```

mousedev      5656 1
hid           22308 0 (unused)
input         6208 0 [keybdev mousedev hid]
usb-uhci      27468 0 (unused)
usbcore       82752 1 [hid usb-uhci]
ext3          91464 2
jbd           56336 2 [ext3]

```

每一行中的第一個欄位是模組的名稱，第二個欄位是模組的大小，而第三個欄位是用量的記數。

最後一個欄位中的資訊對於每一個模組都有些許不同。假如模組的該欄位列出(unused)，表示該模組目前並不在使用中。如果是(autoclean)，表示該模組可以由rmmod -a 指令自動清理(autocleaned)，在執行這個指令後，任何被標示為autoclean 的模組將會被卸載（如果從上一次autoclean 的動作後都沒有被使用）。Red Hat Linux 並不預設執行這個autoclean 的動作。

假如在一行的最後列出一個以括號括住的模組名稱，該模組是依附於該行第一個欄位中所列出的模組。舉例來說：

```
usbcore       82752 1 [hid usb-uhci]
```

hid 與usb-uhci 核心模組是依附於usbcore 模組。

/sbin/lsmmod 指令的輸出與檢視/proc/modules 檔案的內容是相同的。

如要載入一個核心模組，請使用/sbin/modprobe 指令再加上核心模組的名稱。預設情況下，modprobe 會試著從/lib/modules/<核心版本>/kernel/drivers/ 的子目錄載入模組，在其中每一種類型的模組都放置於一個子目錄中，如net/ 子目錄會存放網路介面驅動程式。有些核心模組有模組相依性的情況，這表示必須先載入其他模組才能載入這個模組。/sbin/modprobe 指令將會檢查這些相依性，並且於載入特定模組前先載入相依的模組。

舉例來說：

```
/sbin/modprobe hid
```

這個指令會載入任何的相依模組，然後再載入hid 模組。

如要在螢幕上列出所有指令一如/sbin/modprobe 執行它們，請使用-v 選項，例如：

```
/sbin/modprobe -v hid
```

會顯示類似如下的輸出：

```

/sbin/insmod /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Using /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'

```

/sbin/insmod 指令也可用來載入核心模組，然而它並不解決相依性的問題，因此還是建議您使用/sbin/modprobe 指令。

如要卸載核心模組，請使用/sbin/rmmod 指令再加上模組名稱。rmmod 指令只能卸載不在使用中的模組，而且該模組並不依附於其他使用中的模組。

例如這個指令

```
/sbin/rmmod hid
```

將會卸載hid 核心模組。

另一個好用的核心模組工具是modinfo，請使用/sbin/modinfo 指令來顯示關於一個核心模組的資訊，一般的語法是：

```
/sbin/modinfo [選項] <模組名稱>
```

包含 `-d` 選項將會秀出該模組的一個簡短的描述，而 `-p` 選項則會列出該模組所支援的參數。如要取得完整的選項清單，請參考 `modinfo` 的 `man page` (`man modinfo`)。

## 31.2. 其他的資源

如需關於核心模組與其工具程式的更多資訊，請參考下列資源。

### 31.2.1. 已安裝的說明文件

- `lsmod` 的 `man page` — 描述與解釋它的輸出。
- `insmod` 的 `man page` — 命令列選項的清單與說明。
- `modprobe` 的 `man page` — 命令列選項的清單與說明。
- `rmmmod` 的 `man page` — 命令列選項的清單與說明。
- `modinfo` 的 `man page` — 命令列選項的清單與說明。
- `/usr/src/linux-2.4/Documentation/modules.txt` — 如何編譯與使用核心模組。

### 31.2.2. 好用的網站

- <http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html> — 源自Linux Documentation Project 的 *Linux Loadable Kernel Module HOWTO*。



## V. 套件管理

Red Hat Linux 系統上的所有軟體被劃分為可用來安裝、升級或移除的RPM 套件。這個章節說明如何使用圖形與命令列工具來管理Red Hat Linux 系統上的RPM 套件。

### 內容目錄

32章使用RPM 做套件管理 .....	233
33章套件管理工具 .....	243
34章Red Hat Network.....	247





## 使用RPM 做套件管理

RPM Package Manager (RPM) 是一種開放的套件包裝系統，每一個人都可以使用，可以使用在Red Hat Linux 以及其他的Linux 與UNIX 系統。Red Hat, Inc. 鼓勵其他的公司使用RPM 在他們自己的產品中。可以在遵守GPL 的條款下自由散佈RPM。

對於終端使用者來說，RPM 簡易了系統的更新，只需要短短的指令便可以進行安裝、解除安裝與升級RPM 套件。RPM 維護了一個含有已安裝之套件與其檔案的資料庫，所以您可以在您的系統上調用功能強大的查詢與驗證。假如您較喜歡一個圖形的介面，您可以使用**套件管理工具**來執行許多的RPM 指令，請參考第33章 以取得詳細資訊。

在升級階段中，RPM 小心地處理設定檔案，使得您從來不會遺失您的自訂設定— 這是您使用一般的.tar.gz 檔案所作不到的。

對於程式開發者，RPM 讓您可以使用軟體的原始碼，並將它包裝成原始與二元套件，以提供終端使用者使用。這個過程是相當簡單的，只需使用一個單一的檔案以及您所建立的程式修正（可選的）。當新版本的軟體釋放出來時，在原始程式碼與您的程式修正之間清楚的輪廓，以及建立包裝檔的指示，這兩種特色將簡化套件軟體的維護工作。



### 請注意

因為RPM 將對您的系統做變更，因此您必須是root 才能進行安裝、移除或升級一個RPM 套件。

## 32.1. RPM 設計的宗旨

為了要了解如何使用RPM，先知道一下RPM 的設計宗旨也許對您很有幫助：

### 可升級性

藉由使用RPM，您不用重新安裝整個系統便可升級系統中個別的元件。當您取得一個以RPM 為基礎的新版作業系統（如Red Hat Linux），您並不需要重新安裝到您的機器上（在以其他包裝系統為基礎的作業系統上，您則必須要做的事）。RPM 將使用一種智慧型且完全自動化的方式來升級您的系統，套件的設定檔案將在升級過程中被保留下來，所以您將不會遺失您的自訂設定。並不需要任何特殊的升級檔案來升級一個套件，因為您可以使用相同的RPM 檔案來做安裝與升級系統上的套件。

### 功能強大的查詢

RPM 是設計來提供強力的查詢選項，您可以透過整個資料庫來查詢套件或某些檔案，您也可以輕易地找出一個檔案所屬的套件，以及該套件來自何處。一個RPM 套件所包含的檔案是儲存在一個經過壓縮的歸檔中，並含有關於該套件與其內容的一個自訂二元表頭，使得您可以更快更容易地來查詢個別的套件。

### 系統校驗

另一個功能強大的特色是校驗套件的能力，假如您擔心刪除了某個套件的重要檔案，請對該套件進行校驗。您將會被提示任何異常的狀態。在此時您可以視需求重新安裝該套件，任何您所修改過的設定檔案將會在重新安裝過程中保留下來。

『純淨』的原始碼

一個很重要的設計宗旨便是讓您使用該軟體的原始作者所散佈出來的『純淨』的原始軟體程式碼。使用RPM，您可擁有『純淨』的原始碼以及曾經用過的任何程式修正，加上完整的套件建立指示。這是針對許多種理由的一個重要的優點，舉例來說，假如一個程式的新版本面世後，您並不需要從頭開始來將它進行編譯，您可以檢視程式修正來看看您所需要做的事情。使用RPM的技術便可以很容易的看出為了正確建立該軟體所有編譯進來的預設值與所有做過的變更。

將原始程式碼保持原封不動的目的，也許只對程式開發者比較重要，不過對消費者來說這也會造成更高品質的軟體。我們非常感謝來自BOGUS distribution的高手們，他們提供了許多意見構想，例如將程式碼保留『純淨』的觀念等等。

## 32.2. 使用RPM

RPM有五個基本的操作模式（不包括套件包裝）：安裝、解除安裝、升級、查詢與校驗。這個部份包含每一種模式的概要，如需完整的細節與選項，請使用`rpm --help`，或翻閱至 32.5 節以取得更多關於RPM的資訊。

### 32.2.1. 搜尋RPM 套件

在開始使用RPM之前，您必須先知道要在何處取得它們。網際網路的搜尋將會傳回許多RPM的檔案庫，不過假如您要的是由Red Hat所建立的RPM套件，您可以在下列的位置找到它們：

- Red Hat Linux 的光碟片
- 位於<http://www.redhat.com/apps/support/errata/>的Red Hat Errata 網頁
- 位於<http://www.redhat.com/download/mirror.html>的Red Hat FTP 映射站台
- Red Hat Network — 請參考第34章 以取得更多關於Red Hat Network的詳細資訊

### 32.2.2. 安裝中

RPM 套件典型的檔案名稱會類似`foo-1.0-1.i386.rpm`，檔名中含有套件的名稱(`foo`)、版本(1.0)、發行(1)以及主機架構(`i386`)。只要以`root`身份登入並在`shell`提示符號下輸入下列指令便可安裝一個套件：

```
rpm -Uvh foo-1.0-1.i386.rpm
```

假如安裝成功後，您將會看到下列的安裝進度：

```
Preparing...          ##### [100%]
 1:foo                 ##### [100%]
```

如您所見，RPM 會列出套件的名稱，然後在套件安裝時印出連續的井字號當作安裝的進度。

從RPM 4.1 版開始，當安裝或升級一個套件時，將會檢查該套件的數位簽章，假如簽章的驗證失敗，您將會看到一個如下的錯誤訊息：

```
error: V3 DSA signature: BAD, key ID 0352860f
```

假如它是新的且僅有表頭的簽章，您將會看到如下的錯誤訊息：

```
error: Header V3 DSA signature: BAD, key ID 0352860f
```

假如您沒有安裝適當的金鑰來驗證簽章，錯誤訊息將會含有`NOKEY`：

warning: V3 DSA signature: NOKEY, key ID 0352860f

請參考 32.3 節 以取得更多關於檢查套件簽章的資訊。



#### 請注意

假如您要安裝一個核心套件，您應該要使用 `rpm -ivh`，如需詳細資訊，請參考第30章。

安裝套件的背後含意是力求簡單的，不過有時候還是會有錯誤發生。

#### 32.2.2.1. 套件已安裝

假如相同版本的套件已經安裝了，您將會看到：

```
Preparing... ##### [100%]
package foo-1.0-1 is already installed
```

假如在這種情況下，您仍然想安裝該套件，您可以使用 `--replacepks` 選項來告知RPM 忽視錯誤的存在：

```
rpm -ivh --replacepks foo-1.0-1.i386.rpm
```

當不小心刪除由RPM 安裝的檔案，或者您想要來自該RPM 的原始設定檔案，您便可以使用這個選項。

#### 32.2.2.2. 衝突的檔案

假如您試著要安裝一個套件，而該套件含有一個由另一套件或之前版本的相同套件所安裝的檔案，您將會看到下列訊息：

```
Preparing... ##### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package bar-2.0.20
```

如要使RPM 忽視這個錯誤，請使用 `--replacefiles` 選項：

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

#### 32.2.2.3. 未解決的相依性問題

RPM 套件也許會『相依』於另一個套件，也就是說，它們需要系統安裝其他套件以使它們能過順利執行。假如您試著要安裝含有未解決之相依性問題得套件，您將會看到如下所示：

```
Preparing... ##### [100%]
error: Failed dependencies:
  bar.so.2 is needed by foo-1.0-1
Suggested resolutions:
  bar-2.0.20-3.i386.rpm
```

假如您要安裝一個Red Hat Linux 的套件，通常會建議您所需的套件以用來解決相依性的問題。請在Red Hat Linux 光碟片上或從Red Hat 的FTP 站台（或映射網站），並且將之加入到指令：

```
rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
```

假如兩個套件的安裝都已成功，您將會看到下列的訊息：

```
Preparing... ##### [100%]
 1:foo      ##### [ 50%]
 2:bar      ##### [100%]
```

假如沒有建議用來解決相依性問題的套件，您可以使用`--redhatprovides` 選項以決定那些套件含有所需的檔案，您需要安裝`rpmdb-redhat` 套件以使用這個選項。

```
rpm -q --redhatprovides bar.so.2
```

假如包含`bar.so.2` 檔案的套件是來自`rpmdb-redhat` 套件所安裝的資料庫，將會顯示該套件的名稱：

```
bar-2.0.20-3.i386.rpm
```

假如您仍然想要強制進行安裝（最好不要，因為套件也許無法正常運作），您可以使用`--nodeps` 選項。

### 32.2.3. 解除安裝

解除安裝一個套件就像安裝一個套件一樣簡單，請在`shell` 提示符號下輸入下列指令：

```
rpm -e foo
```



#### 請注意

請特別注意，在此我們使用套件名稱 `foo`，而不是原始套件檔案的名稱 `foo-1.0-1.i386.rpm`。如要解除安裝一個套件，您需要以原始套件的套件名稱取代 `foo`。

假如另一個已安裝的套件相依於您正要移除的套件，您則會遇到相依性問題的錯誤。舉例來說：

```
Preparing... ##### [100%]
error: removing these packages would break dependencies:
  foo is needed by bar-2.0.20-3.i386.rpm
```

如要使RPM 忽視這個錯誤，並且解除安裝這個套件（不建議您如此做，因為相依於它的套件也許會無法正常運作），您可以使用`--nodeps` 選項。

### 32.2.4. 升級

升級一個套件與安裝一個套件很類似，只需在`shell` 提示符號下輸入下列指令：

```
rpm -Uvh foo-2.0-1.i386.rpm
```

在以上的例子中您所看不到的是，任何較舊版本的`foo` 套件都被RPM 自動解除安裝了。事實上，您可以總是使用`-U` 來安裝套件，因為即使沒有安裝之前版本的該套件，也可以順利運作。

因為RPM 執行一種包括設定檔案的智慧式套件升級，您也許會看到下列的訊息：

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

這個訊息代表您在設定檔案所做的變更也許無法“向前相容”於套件中新的設定檔案，所以RPM 儲存原本的設定檔案，再安裝一個新的檔案。您應該仔細檢查兩個設定檔案的相異處，並且盡快的解決它們，也確保系統能繼續正常運作。

升級操作實際上是解除安裝與安裝的結合，所以在RPM 升級階段，您也許會遇到解除安裝與安裝的錯誤，以及當您試著要升級到一個含有較舊版本號碼的套件時，您將會看到：

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

如要強迫RPM 執行所謂的"升級"，請使用`--oldpackage` 選項：

```
rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
```

### 32.2.5. 更新(Freshening)

Freshening 一個套件相當類似套件升級，請在shell 提示符號下輸入下列指令：

```
rpm -Fvh foo-1.2-1.i386.rpm
```

RPM 的`freshen` 選項檢查命令列上所指定的套件版本與已經安裝到您系統上的套件版本，當RPM 的`freshen` 選項處理到一個已安裝套件的較新版本，將會升級該套件到較新的版本。然而假如之前沒有安裝相同名稱的套件，RPM 的`freshen` 選項將不會安裝該套件，這是與RPM 升級選項不同的地方，因為不管一個較舊版本的套件是否已安裝，升級選項仍將會安裝該套件。

RPM 的`freshen` 選項可使用在單一的套件或群組的套件。假如您剛剛下載很多不同的套件，而您只想要升級那些已經安裝到系統中的套件，此時您便可以使用`freshen` 的選項。假如您使用`freshening`，在您使用RPM 之前您並不需要從群組中刪除任何不想要的套件。

在這個例子，您可以執行下列的指令：

```
rpm -Fvh *.rpm
```

RPM 將只會自動升級已經安裝的套件。

### 32.2.6. 查詢

使用`rpm -q` 指令來查詢已安裝套件的資料庫，`rpm -q foo` 指令將會列出已安裝套件`foo` 的套件名稱、版本與發行號碼：

```
foo-2.0-1
```



#### 請注意

請留意我們使用套件的名稱`foo`，如要查詢一個套件您必須以真實的套件名稱取代`foo`。

除了指定套件名稱之外，您可以使用下列的選項加上`-q` 來指定想要查詢的套件，這些稱為套件規格選項。

- `-a` 查詢目前已安裝的所有套件。
- `-f <file>` 將查詢擁有`<file>` 檔案的套件。當您要指定一個檔案時，必須指定該檔案的完整路徑(如`/usr/bin/lis`)。
- `-p <packagefile>` 將查詢`<packagefile>` 套件。

有許多種方式可用來指定關於套件查詢所顯示的資訊，下列的選項可使用來選擇您要搜尋的資訊種類，這些稱為資訊選擇選項。

- `-i` 顯示套件的資訊，包括名稱、說明、發行大小、建立日期、安裝日期、發行廠商以及其他的未分類資訊。
- `-l` 顯示套件所含的檔案清單。
- `-s` 顯示套件所包括之所有檔案的狀態。
- `-d` 顯示標示為說明文件的檔案清單（如man pages, info pages 與READMEs 等等）。
- `-c` 顯示標示為設定檔的檔案清單，這些是您在安裝完後更改以適用於您系統的檔案（如sendmail.cf, passwd 與inittab 等等）。

對於用來顯示檔案清單的選項，您可以加上`-v`到指令上來顯示類似`ls -l`格式的檔案清單。

### 32.2.7. 校驗

校驗套件將會比較從一個套件安裝之檔案的資訊與從相同的原始套件安裝的資訊，除此之外，套件的校驗將會比較每一檔案的大小、MD5 校驗值、權限設定、種類、擁有者與群組。

`rpm -V` 指令將會校驗一個套件，您可以使用任何所列出的套件選擇選項來查詢您所指定要做校驗的套件。當您使用如`rpm -V foo`的簡單指令將會校驗foo 套件中的所有檔案是否與原本安裝時的狀態一樣。例如：

- 如要校驗含括一個特定檔案的套件：  
`rpm -Vf /bin/vi`
- 如要校驗所有安裝的套件：  
`rpm -Va`
- 如要針對一個RPM 套件檔案來校驗一個已安裝的套件：  
`rpm -Vp foo-1.0-1.i386.rpm`

假如您懷疑RPM 資料庫已經毀損時，可以使用這個指令。

假如校驗的過程順利，將不會有任何的輸出。如果有任何的差異存在，將會顯示出來。輸出的格式為含有8 個字元的字串（c 代表一個設定檔案）以及檔案名稱。這8 個字元中的每一個都代表檔案的一個屬性與RPM 資料庫中所紀錄之屬性數值的比較結果。一個單一的.（句號）代表測試通過。下列的字元代表某種失敗的測試：

- 5 — MD5 校驗值
- S — 檔案大小
- L — 符號連結
- T — 檔案修改時間
- D — 裝置
- U — 使用者
- G — 群組
- M — 模式（包括權限設定與檔案類型）
- ? — 無法讀取的檔案

假如您看到任何的輸出，請使用您的判斷力來決定是否您需要移除或重新安裝該套件，或者以其他方式來修復問題。

### 32.3. 檢查一個套件的簽章

假如您想要確認一個套件是否已經毀損或被竄改，只需要在shell 提示符號下輸入以下指令加上RPM 套件的檔案名稱來檢查md5sum：

```
rpm -K --nogpg <rpm-file>
```

您將會看到下列訊息<rpm-file>：md5 OK。這個簡短的訊息表示檔案在下載過程中沒有毀損，如想看到更多的訊息，請在指令中以-Kvv 取代-K 選項。

另外，建立這個套件的程式開發者是可以信賴的嗎？假如該套件已簽署該程式開發者的GnuPG 金鑰，您便知道這個開發者就是開發該程式的本人了。

可以使用Gnu Privacy Guard（或GnuPG）來簽署一個RPM 套件，以幫助您確定下載的套件是可信賴的。

GnuPG 是用來做安全通訊的一種工具，它是PGP（一種電子的私密性程式）加密技術的一個完整且免費的替代品。藉由使用GnuPG，您可以認證文件的有效性，以及加密與解密與其他聯絡人的通訊資料。GnuPG 也可用來解密與校驗PGP 5.x 的檔案。

在Red Hat Linux 的安裝過程中，已預設安裝GnuPG，這樣您便可以馬上開始使用GnuPG 來檢驗從Red Hat 接收到的任何套件。首先您必須匯入Red Hat 所釋出的公鑰。

#### 32.3.1. 匯入金鑰

如要檢驗Red Hat 的套件，您必須匯入Red Hat 的GPG 金鑰，請在shell 提示符號下輸入下列指令：

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

如要顯示用於RPM 校驗的所有已安裝的金鑰清單，請執行下列指令：

```
rpm -qa gpg-pubkey*
```

關於Red Hat 的金鑰，輸出將會含有：

```
gpg-pubkey-db42a60e-37ea5438
```

如要顯示關於一個特定金鑰的詳細資訊，請使用rpm -qi 指令再加上前一指令的輸出：

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

#### 32.3.2. 檢驗套件的簽章

在匯入建立者的GnuPG 金鑰後，如要檢查一個RPM 檔案的GnuPG 簽章，請使用下列指令（以RPM 套件的檔案名稱取代<rpm-file>）：

```
rpm -K <rpm-file>
```

假如一切進行順利，您將會看到這個訊息：md5 gpg OK。這表示該套件的簽章已經確認，而且沒有毀損。



#### 建議

如需關於GnuPG 的更多資訊，請參考附錄B。

### 32.4. 使用RPM 讓您的朋友對您另眼相看

RPM 是用來管理您的系統與診斷並修復問題很有用的工具，為了要多了解所有它的選項最好的方法是來看看一些範例。

- 或許您意外的刪除了一些檔案，不過您不確定您刪除了什麼，您可以試試下列的指令：

```
rpm -Va
```

假如某些檔案遺失或似乎已毀損，您或許應該要重新安裝套件或解除安裝它，然後再重新安裝該套件。

- 在某些地方您也許會看到不曾見過的檔案，如要找出那一個套件擁有它，您可以輸入：

```
rpm -qf /usr/X11R6/bin/ghostview
```

輸出將如下所示：

```
gv-3.5.8-22
```

- 我們可以結合以上兩個例子到下列的狀況下，譬如您的 `/usr/bin/paste` 檔案有問題，您想要確認擁有該程式的套件，不過您不知道那一個套件擁有 `paste`，只要輸入以下指令即知道解答：

```
rpm -Vf /usr/bin/paste
```

相關的套件將會被檢驗。

- 您想要找出關於一個特定程式的更多資訊嗎？您可以試試下列指令來找出擁有該程式之套件所附的說明文件：

```
rpm -qdf /usr/bin/free
```

輸出將如下所示：

```
/usr/share/doc/procps-2.0.11/BUGS
/usr/share/doc/procps-2.0.11/NEWS
/usr/share/doc/procps-2.0.11/TODO
/usr/share/man/man1/free.1.gz
/usr/share/man/man1/oldps.1.gz
/usr/share/man/man1/pgrep.1.gz
/usr/share/man/man1/pkill.1.gz
/usr/share/man/man1/ps.1.gz
/usr/share/man/man1/skill.1.gz
/usr/share/man/man1/snice.1.gz
/usr/share/man/man1/tload.1.gz
/usr/share/man/man1/top.1.gz
/usr/share/man/man1/uptime.1.gz
/usr/share/man/man1/w.1.gz
/usr/share/man/man1/watch.1.gz
/usr/share/man/man5/sysctl.conf.5.gz
/usr/share/man/man8/sysctl.8.gz
/usr/share/man/man8/vmstat.8.gz
```

- 您手上有一個新的RPM，不過您不知道它的用處是什麼？如要找出關於它的更多資訊，請使用下列指令：

```
rpm -qip crontabs-1.10-5.noarch.rpm
```

輸出將如下所示：

```
Name      : crontabs                Relocations: (not relocateable)
Version   : 1.10                  Vendor: Red Hat, Inc.
Release   : 5                   BuildDate: Fri 07 Feb 2003 04:07:32 PM EST
Install date: (not installed)   BuildHost: porky.devel.redhat.com
Group     : System Environment/Base Source RPM: crontabs-1.10-5.src.rpm
Size      : 1004                License: Public Domain
Signature : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
Packager  : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary   : Root crontab files used to schedule the execution of programs.
Description:
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
```



cron daemon. The cron daemon checks the crontab files to see when particular commands are scheduled to be executed. If commands are scheduled, then it executes them.

- 現在也許您想要知道crontabs RPM 安裝了那些檔案，請您輸入以下指令：  
rpm -qlp crontabs-1.10-5.noarch.rpm

輸出將如下所示：

```
Name       : crontabs                Relocations: (not relocateable)
Version    : 1.10                  Vendor: Red Hat, Inc.
Release    : 5                    BuildDate: Fri 07 Feb 2003 04:07:32 PM EST
Install date: (not installed)      BuildHost: porky.devel.redhat.com
Group      : System Environment/Base Source RPM: crontabs-1.10-5.src.rpm
Size       : 1004                 License: Public Domain
Signature  : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
Packager   : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary    : Root crontab files used to schedule the execution of programs.
Description:
The crontabs package contains root crontab files. Crontab is the
program used to install, uninstall, or list the tables used to drive the
cron daemon. The cron daemon checks the crontab files to see when
particular commands are scheduled to be executed. If commands are
scheduled, then it executes them.
```

這裡只是一些範例，當您開始使用它時，您將會漸漸發現RPM 好用的地方。

## 32.5. 其他的資源

RPM 是一種相當複雜的工具，它含有許多選項與方法可讓您用來查詢、安裝、升級與移除套件，請參考下列的資源以對RPM 有更進一步的了解。

### 32.5.1. 已安裝的說明文件

- rpm --help — 這個指令會顯示RPM 參數的快速索引。
- man rpm — RPM 的man page 將向您顯示比rpm --help 指令更詳細的RPM 參數資訊。

### 32.5.2. 好用的網站

- <http://www.rpm.org/> — RPM 的官方網站。
- <http://www.redhat.com/mailling-lists/rpm-list/> — RPM 的郵遞論壇所在處，如要訂閱，請傳送一封在主題欄含有subscribe 字眼的電子郵件到<rpm-list-request@redhat.com>。

### 32.5.3. 相關的書籍

- 由Ed Bailey 撰寫; Red Hat Press 發行的*Maximum RPM* — 這本書的線上版本可在以下位址取得：<http://www.rpm.org/> 與<http://www.redhat.com/docs/books/>。



在安裝過程中，使用者選擇如『**工作站**』或『**伺服器**』的安裝類型，軟體套件將依據這個選擇來進行安裝。由於每一個人使用他們電腦的方式不同，使用者也許會想要在系統安裝後進行安裝或移除套件。**套件管理工具** 將可幫助使用者達到這個目的。

執行**套件管理工具** 需要X視窗系統，如要啟動這個應用程式，請選擇面板上的『**主選單按鈕**』=>『**系統設定**』=>『**新增/移除應用程式**』，或在shell提示符號下輸入`redhat-config-packages`指令。

此時會出現與您放入Red Hat Linux 第一片光碟時相同的介面。



圖形33-1. 套件管理工具

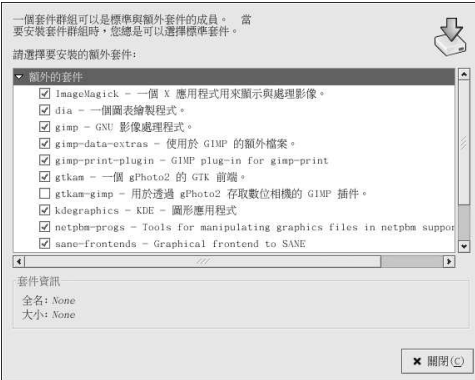
這個應用程式的介面類似在安裝程式中所使用的，所有套件被區分為套件群組，其中含有一系列享有共同功能性之標準的套件與額外的套件。舉例來說，『**圖形化網際網路**』群組包含一個網頁瀏覽器、電子郵件用戶端以及其他使用來連線到網際網路的圖形化程式。除非移除整個套件群組，否則無法移除標準的套件。而只要有選取該套件群組，便可選取要安裝或移除額外的套件。

主要的視窗會顯示套件群組的清單，假如一個套件群組旁的選取盒有打勾的記號，表示目前已經安裝該群組中的套件。如要檢視群組中的個別套件清單，請點選旁邊的**詳細資訊** 按鈕。含有打勾記號的個別套件是已經安裝的。

### 33.1. 安裝套件

如要安裝目前尚未安裝之套件群組中的標準套件，請點選旁邊的選取盒。如要自訂群組中要安裝的套件，請點選右邊的**詳細資訊** 按鈕，將會顯示如圖形33-2 所示的標準與額外的套件清單。點選套件名稱將會在視窗底端顯示出安裝該套件所需的磁碟空間，選取套件名稱旁的選取盒以示要安裝該套件。

您也可以選取已安裝之套件群組中的個別套件，只要點選**詳細資訊** 的按鈕，然後點選尚未安裝的任何額外套件。



圖形33-2. 選取個別套件

在選取要安裝的套件群組與個別套件後，請點選主要視窗中的**更新**按鈕，應用程式將會開始計算安裝套件所需的磁碟空間，以及任何的套件相依性問題，並顯示一個摘要視窗。假如有相依性問題的套件存在，所需的套件將會被自動加入到欲安裝的套件清單中，點選**顯示詳細資訊**按鈕來檢視要安裝的套件清單。



圖形33-3. 套件安裝摘要

點選**繼續**以開始套件安裝過程，完成後會出現一個『**完成更新**』的對話窗。



#### 建議

假如您使用**Nautilus**來瀏覽電腦中的檔案與目錄，您也可以使用它來安裝套件。在**Nautilus**中前往含有一個RPM套件（通常以`.rpm`為副檔名）的目錄，然後雙點選該RPM圖示。

## 33.2. 移除套件

如要移除套件群組中所有已安裝的套件，請取消選取旁邊的選取盒。如要移除個別套件，請點選套件群組右邊的**詳細資訊**按鈕，然後取消選取個別的套件。

當您完成選取要移除的套件，請點選主要視窗中的**更新**按鈕，應用程式將會開始計算即將釋放的磁碟空間，以及軟體套件的相依性問題。假如其他的套件依附您選取要移除的套件，將會自動將它們加入到要移除的套件清單。請點選**顯示詳細資訊**的按鈕來檢視欲移除的套件清單。



圖形33-4. 套件移除摘要

點選**繼續**來開始套件移除程序，完成後會出現一個『**完成更新**』的對話窗。

**建議**

您可以結合套件的安裝與移除程序，只要選取要安裝或移除的套件群組或套件，然後再點選**更新**即可。『**完成系統準備**』的視窗將會顯示要安裝與移除的套件數。



## Red Hat Network

Red Hat Network 是用來管理一或多部Red Hat Linux 系統的一種網際網路解決方案，所有的安全性警告、程式錯誤修正警告以及功能性加強警告（統稱為Errata Alerts）都可以使用Red Hat 更新代理程式應用程式或透過RHN的網站位於<http://rhn.redhat.com/> 來直接下載。



圖形34-1. 您的RHN

Red Hat Network 替使用者節省很多時間，因為當更新的套件公佈後，使用者們會收到電子郵件。使用者便不需要搜尋網路上的更新套件或安全性警告。預設情況下，Red Hat Network 也會安裝下載的套件，使用者不需要學習如何使用RPM 或煩惱該如何解決軟體套件的相依性問題，RHN 都幫您做好了。

每一個Red Hat Network 帳號都含有：

- Errata Alerts — 這是當安全性警告、程式錯誤修正警告以及功能性加強警告透過基本介面發佈給您的網路中所有系統時，您將會收到的訊息



圖形34-2. 相關的Errata

- 自動電子郵件通知— 當一個Errata Alert 發放給您的系統時，將收到一封電子郵件的通知
- 排程Errata 更新— 排定Errata 更新的傳送時程
- 套件安裝— 藉由點選一個按鈕來排程在一或多部系統上的套件安裝
- **Red Hat 更新代理程式**— 使用**Red Hat 更新代理程式** 來下載適用於您系統的更新軟體套件（還可以一併安裝套件）
- Red Hat Network 網站— 用來管理多部系統、下載個別套件以及排定從任何電腦透過一個安全的網頁瀏覽器進行Errata 更新的行程

如需開始使用Red Hat Network，請遵照以下三個基本的步驟：

1. 使用下列的其中一種方法來建立一個系統資料檔：
  - 安裝系統第一次開機時，在**設定代理程式** 中向RHN 註冊您的系統。
  - 在您的桌面上選擇『**主選單按鈕**』 => 『**系統工具**』 => **Red Hat Network**。
  - 從shell 提示符號執行up2date 指令。
2. 再來請登入位於<http://rhn.redhat.com/> 的RHN，並且給予您的系統我們所提供的服務。每個人都享有一部系統的一個免費的Red Hat Network 帳號，您還可以購買額外的帳號。
3. 您便可透過RHN 網站開始排程更新或者使用**Red Hat 更新代理程式** 來下載與安裝Errata 更新。

如需更詳細的指示，請閱讀在<http://www.redhat.com/docs/manuals/RHNetwork/> 的**Red Hat Network User Reference Guide**。



**建議**

Red Hat Linux 包含了 **Red Hat Network 警示提示工具**，它是一個很好用的面板圖示，當有程式更新適合您的 Red Hat Linux 系統時，它會顯示一個明顯的警示符號。請參考以下的網址以取得關於這個面板小程序的更多資訊：<http://rhn.redhat.com/help/basic/applet.html>



## VI. 附錄

這個部份含有從Red Hat, Inc. 提供的原始碼檔案建立一個自訂核心的指示，也包含一個章節說明Gnu Privacy Guard，它是可用來做安全通訊的一種工具。

### 內容目錄

A. 建立一個自訂的核心.....	253
B. 開始使用Gnu Privacy Guard .....	257



## 建立一個自訂的核心

許多Linux的新手常常會問--我為何需要建立自己的核心？對進階的使用者來說，他們可以運用核心模組來做到。然而對這個問題的最正確答覆應該是--除非您已經知道為何您需要建立自己的核心，否則您或許不需要惹這個麻煩。

Red Hat Linux 提供的核心以及透過Red Hat Linux 的Errata 系統將對大部分當代的硬體與核心特色提供支援。對大部分的使用者來說，並不需要重新編譯核心。對於想要重新編譯核心以及想要編譯實驗性的特色到核心中的使用者們，這個附錄將提供一個指引以幫助他們學習更多資訊。

如要使用由Red Hat, Inc. 散佈的核心套件來升級核心，請參考第30章。



### 警告

建立一個自訂的核心並不被Red Hat Linux 安裝支援小組所支援，如需關於使用由Red Hat, Inc. 散佈的核心套件來升級核心，請參考第30章。

### A.1. 準備建立

在建立一個自訂核心前，請務必確定已經建立一片可用的緊急開機磁片，以免任何的錯誤的發生。如要建立一片使用目前執行中核心的開機磁片，請執行以下指令：

```
/sbin/mkbootdisk `uname -r`
```

在建立好磁片後，請先做測試以確定它可以啟動系統。

如要重新編譯核心，必須已安裝kernel-source 套件，請執行指令

```
rpm -q kernel-source
```

以確定它是否已經安裝。如果沒有的話，請從Red Hat Linux 的安裝光碟片、Red Hat 的FTP 站台：[ftp://ftp.redhat.com](http://ftp.redhat.com)（在<http://www.redhat.com/mirrors.html> 有映射網站的清單）或從Red Hat Network 來進行安裝。如需關於安裝RPM 套件的更多資訊，請參考 V 部。

### A.2. 建立核心

這個部份的指示適用於建立一個自訂的模組化核心，如要建立一個集成式(monolithic)的核心，請參閱 A.3 節，以取得另一方面關於建立與安裝一個集成式核心的解釋。



### 請注意

這個例子使用2.4.20-2.47.1 當作核心的版本（核心版本也許會不同），如要得知核心版本請輸入uname -r 指令，並以所傳回的核心版本取代2.4.20-2.47.1。

如要為x86 的主機架構建立一個自訂的核心，請遵照以下步驟（以root 身份執行所有步驟）：

1. 開啟一個shell 提示符號並轉換至/usr/src/linux-2.4/ 目錄，在此以後的所有指令都必須在這個目錄中執行。

2. 在狀況明瞭的原始碼目錄樹中開始核心的建立是很重要的，因此建議您先執行`make mrproper`指令以移除散佈在目錄樹中任何之前的建立所遺留下的設定檔案。假如一個既有的設定檔案存在於`/usr/src/linux-2.4/.config`，請在執行這個指令前將之備份到另一個目錄，然後在完成後再將之複製回來。
3. 建議您使用預設的Red Hat Linux 核心的設定當作一個起點，請從`/usr/src/linux-2.4/configs/`目錄複製製適用系統架構的設定檔案到`/usr/src/linux-2.4/.config`，假如系統中擁有超過4GB的記憶體，也請您複製含有關鍵字**bigmem**的檔案。
4. 下一步便是自訂您的設定，假如可以使用X 視窗系統，建議您使用`make xconfig`指令來執行**Linux Kernel Configuration**。



#### 請注意

如要使用`make xconfig`指令來啟動圖形化的工具，必須已經安裝提供`wish`指令的`tk`套件。如需關於安裝RPM 套件的更多資訊，請參考 V 部。

Code maturity level options	Fusion MPT device support	Sound
Loadable module support	IEEE 1394 (FireWire) support (EXPERIMENTAL)	USB support
Processor type and features	I2O device support	Additional device driver support
General setup	Network device support	Bluetooth support
Memory Technology Devices (MTD)	Amateur Radio support	Printing support
Parallel port support	IrDA (infrared) support	Kernel hacking
Plug and Play configuration	ISDN subsystem	Library routines
Block devices	Old CD-ROM drivers (not SCSI, not IDE)	
Multi-device support (RAID and LVM)	Input core support	
Cryptography support (CryptAPI)	Character devices	
Networking options	Multimedia devices	Save and Exit
Telephony Support	Crypto Hardware support	Quit Without Saving
ATA/IDEM/FRMLL support	File systems	Load Configuration from File
SCSI support	Console drivers	Store Configuration to File

圖形A-1. 配置核心組件類別

如圖形A-1 所示，請以點選的方式選取要設定的類別，每一個類別中尚含有組成元件。選取元件旁的**y** (yes)、**m** (module) 或 **n** (no) 來將之編譯到核心、編譯為一個核心模組或是不編譯它。如要更加了解這些元件，請點選旁邊的**Help** 按鈕。

點選**Main Menu** 以回到類別的清單。

在完成設定後，請點選主要選單視窗中的**Save and Exit** 按鈕以建立`/usr/src/linux-2.4/.config`設定檔案，並且離開**Linux Kernel Configuration** 程式。即使對任何的設定都沒有做變更，在繼續之前務必要執行`make xconfig`指令（或者是用來做核心設定的其中一種方法）。

其他用作核心設定的方法有：

- `make config` — 一個互動式的文字模式程式，元件是以線性的格式呈現，並且一次只能操作一個。這個方法並不需要X 視窗系統，而且不允許您改變之前問題的答案。
- `make menuconfig` — 一個文字模式且含有選單的程式。元件是以類別的選單呈現，使用在文字模式的Red Hat Linux 安裝程式中相同的選取元件方式。選取對應到要收錄之項目的標記：**[\*]**（嵌入）、**[ ]**（排除）、**<M>**（模組）或**< >**（可用的模組）。這種方式不需要X 視窗系統。
- `make oldconfig` — 這是一個用來設定組態檔案以包含預設設定的非互動式命令稿。假如系統是使用預設的Red Hat Linux 核心，這將為適用該主機架構的Red Hat Linux 所附之核心建立一個設定檔案。這個方法很適合用來設定核心為已知的運作預設值，然後關閉不用的特色。



### 請注意

如要使用kmod 與核心模組，請在設定過程中回答**Yes** 給kmod support 與module version (CONFIG\_MODVERSIONS) support。

5. 在建立/usr/src/linux-2.4/.config 檔案之後，請使用make dep 指令來正確地設定相依性。
6. 使用make clean 指令來準備原始碼目錄以便建立。
7. 建議您使用一個不同的版本號碼在自訂的核心上，以免既有的核心被覆寫。這裡描述的方法是用來回復不幸事件的最簡單方式。至於其他的方法，您可以在以下的網站中：<http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html> 或在/usr/src/linux-2.4 目錄下的Makefile 檔案中找到。  
預設狀況下，/usr/src/linux-2.4/Makefile 附加custom 在以EXTRAVERSION 開頭的該行最後面。藉由附加這個字串將使得系統同時擁有已運作中的舊核心與新的核心（版本2.4.20-2.47.lcustom）。  
假如系統中含有一個以上的自訂核心，最好在後面加上一個日期（或其他的標識符）。
8. 使用make bzImage 建立核心。
9. 建立使用make modules 所設定的任何模組。
10. 使用make modules\_install 指令來安裝核心模組（即使並沒有真正建立任何東西），請特別注意指令中的底線符號(\_)。這將會安裝核心模組到/lib/modules/<KERNELVERSION>/kernel/drivers 目錄中（這裡的KERNELVERSION 就是Makefile 中所指定的版本）。在這個例子中，應該是/lib/modules/2.4.20-2.47.lcustom/kernel/drivers/。
11. 使用make install 以複製新的核心與相關的檔案到適當的目錄中。  
除了安裝核心檔案到/boot 目錄，這個指令也執行/sbin/new-kernel-pkg 命令稿來建立一個新的initrd 映像檔，並且在開機管理程式的設定檔案中加入一個新的紀錄。  
假如系統有一張SCSI 控制卡，而且SCSI 驅動程式已被編譯為一個模組，或者核心已被建立含有ext3 的模組支援（Red Hat Linux 中的預設值），您便需要這個initrd 映像檔。
12. 即使都已經完成initrd 映像檔與開機管理程式的修改，請再一次確認設定都是正確的，並且記得使用自訂的核心版本（而不是2.4.20-2.47.1）。請參考 30.5 節 與 30.6 節 以取得關於確認這些修改的指示。

## A.3. 建立一個集成式的核心

如要建立一個集成式的核心，請遵照建立一個模組化核心的相同步驟，僅有一些些的不同點。

- 在配置核心階段，請勿編譯任何元件為一個模組，也就是說，只對問題回答**Yes** 或**No**。而且請記得對kmod support and module version (CONFIG\_MODVERSIONS) support 元件回答**No**。
- 略過下列步驟：  
make modules  
make modules\_install
- 使用nomodules 指令來附加kernel 一行到grub.conf 檔案中，或者編輯lilo.conf 檔案以包含append=nomodules 一行。

## A.4. 其他的資源

如需更多關於Linux 核心的資訊，請參考下列資源。

### A.4.1. 已安裝的說明文件

- `/usr/src/linux-2.4/Documentation` — 關於Linux 核心與其模組的進階說明文件，這些文件是專門為有興趣貢獻核心原始碼以及了解核心如何運作的人所撰寫的。

### A.4.2. 好用的網站

- <http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html> — 源自Linux Documentation Project 的 *The Linux Kernel HOWTO*。
- <http://www.kernel.org/pub/linux/docs/lkml/> — linux-kernel 郵遞論壇。



## 開始使用Gnu Privacy Guard

您是否曾經想過您的郵件在傳送過程中可能被其他人讀取？很不幸的，完全陌生的人也很有可能會截取甚至竄改您的電子郵件。

傳統的郵件（也稱為“snail”），信件通常是以信封封住，貼上郵票後再寄到郵局，然後再傳送到其他的分局直到到達收件人。不過透過網際網路傳送電子郵件比較起來較不安全，在伺服器與伺服器之間，電子郵件通常是以未加密的文字傳送，並沒有採取特別的方式來保護您的訊息，以免遭到其他人截取或竄改。

為了幫您保護您的隱私權，Red Hat Linux 9 收錄了GnuPG (*GNU Privacy Guard*)，在一個典型的Red Hat Linux 安裝將會預設安裝這個套件，它也被稱為*GPG*。

GnuPG 是一個用於安全通訊的工具，它是一個完整且免費的加密技術替代品，將用來取代PGP (Pretty Good Privacy - 一個相當受到歡迎的加密應用程式)。藉由使用GnuPG，您可以將您的資料與通訊進行加密，以及透過『數位簽章』的方式來認證您的通訊。GnuPG 也可用來解密與驗證PGP 5.x。

因為GnuPG 相容於其他的加密標準，您的安全信件將可以相容於其他作業系統（如Windows 與Macintosh）的電子郵件應用程式。

GnuPG 使用『公鑰密碼技術』來提供使用者一個安全的資料交換，藉由使用公鑰密碼技術，您將產生兩個金鑰：一個公鑰與一個私鑰。您可以與您的通信者或金鑰伺服器交換您的公鑰，而您絕不能暴露您的私鑰。

加密完全仰賴金鑰的使用，在傳統的或對稱式的編碼上，資料處理的兩端都有相同的金鑰，可使他們用來解密彼此傳送的訊息。而在公鑰的編碼上，公鑰與私鑰將共同存在。個人或公司必須秘密保存他們的私鑰，而公開他們的公鑰。以公鑰加密的資料只能使用私鑰將之解密；以私鑰加密的資料只能使用公鑰將之解密。

**重要**

請記得，您可以將您的公鑰給予您想要透過安全通訊的任何人，不過您絕不可以將您的私鑰洩露出去。

絕大部分的密碼學都已經超越這本書的範圍，市面上已經有許多關於這個主題的書籍。然而，在這個章節中，我們希望您能獲得關於GnuPG 足夠的認識，以開始使用密碼加密在您的信件上。假如您想要學習更多關於GnuPG、PGP 以及密碼技術的資訊，請參考 B.8 節。

### B.1. 設定檔案

在您第一次執行GnuPG 指令時，在您的家目錄會建立一個.gnupg 目錄。從1.2 版本開始，設定檔案的名稱已經從.gnupg/options 改為.gnupg/gpg.conf。假如在您的家目錄中找不到.gnupg/gpg.conf 檔案，則會使用.gnupg/options 檔案。假如您只使用1.2 或更新的版本，建議您使用下列的指令重新命名您的設定檔案：

```
mv ~/.gnupg/options ~/.gnupg/gpg.conf
```

假如您是由1.0.7 之前的版本升級的話，您可以在您的金鑰環建立簽章快取以減少金鑰環的存取時間。如要執行這項操作，請執行一次下列的指令：

```
gpg --rebuild-keydb-caches
```

## B.2. 警告訊息

當您執行GnuPG 指令時，您也許會看到以下訊息：

```
gpg: Warning: using insecure memory!
```

這個警告訊息是因為非root 的使用者不能鎖定記憶體分頁。假如一般使用者可以鎖定記憶體分頁的話，他們可能會執行導致記憶體不足(out-of-memory) 的阻絕服務攻擊(DoS)，因此這很有可能是一個安全性的問題。如需詳細資訊，請參考<http://www.gnupg.org/en/documentation/faqs.html#q6.1>。

您也有可能會看到下列的訊息：

```
gpg: WARNING: unsafe permissions on configuration file "/home/username/.gnupg/gpg.conf"
```

假如設定檔案的權限設定允許其他人讀取，就會顯示以上訊息。假如有出現這個警告，建議您執行下列指令來更改檔案的權限設定：

```
chmod 600 ~/.gnupg/gpg.conf
```

另一個常見的警示訊息如下：

```
gpg: WARNING: unsafe enclosing directory permissions on configuration file
"/home/username/.gnupg/gpg.conf"
```

假如含有設定檔案的目錄之權限設定允許其他人讀取它的內容，就會顯示這個訊息。假如有出現這個警告，建議您執行下列指令來更改它的權限設定：

```
chmod 700 ~/.gnupg
```

假如您是由先前版本的GnuPG 升級的，您也許會看到以下的訊息：

```
gpg: /home/username/.gnupg/gpg.conf:82: deprecated option "honor-http-proxy"
gpg: please use "keyserver-options honor-http-proxy" instead
```

會出現這個警告是因為您的~/.gnupg/gpg.conf 檔案含有下列這一行：

```
honor-http-proxy
```

1.0.7 以上的版本使用不同的語法，請更改為如下所示：

```
keyserver-options honor-http-proxy
```

## B.3. 產生一副鑰匙對(Keypair)

要開始使用GnuPG，您必須先產生一副新的鑰匙對：一個公鑰與一個私鑰。

如要產生一副鑰匙對，請在shell 提示符號下輸入以下指令：

```
gpg --gen-key
```

因為您最常使用您的使用者帳號，您應該在登入您的使用者帳號（非root 帳號）時執行這個動作。

您將會看到一個含有金鑰選項（包括一個建議選項）的簡介畫面，如下所示：

```
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
```

Please select what kind of key you want :

- (1) DSA and ElGamal (default)
- (2) DSA (sign only)
- (5) RSA (sign only)

Your selection?

大部份需要您選擇一個選項的畫面都會在括號中列出預設的選項，您可以按下[Enter] 鍵來接受預設的選項。

在第一個畫面，您應該要接受預設的選項：(1) DSA and ElGamal。這個選項將允許您建立一個數位簽章，並且以兩種類型的技術來加密（以及解密）。請輸入1 然後按下[Enter] 鍵。

再來，請選擇金鑰的大小或金鑰的長度。一般來說，金鑰的長度越長，對您的訊息遭受攻擊的保護越高。對大部分的使用者來說，預設的大小1024 位元應該可提供足夠的保護，所以請按下[Enter]。

下一個選項要您指定金鑰的有效期限，通常您只要使用預設值(0 = key does not expire)即可，假如您確實選擇一個失效的日期，請記得任何與您有交易您公鑰的人，都必須要知會他們金鑰的失效日期，並且屆時提供他們一個新的公鑰。假如您沒有選擇一個失效的日期，您必須要再一次確認您的選擇，請按下[y] 來確認您的選擇。

下一個動作是提供一個使用者的ID，包括您的姓名、電子郵件位址以及一個可選的備註。在您完成後，您將可以看到您所輸入資訊的摘要。

在接受您輸入的資訊後，您必須要輸入一個密碼(passphrase)。



#### 建議

如同您的帳號密碼，要提供GnuPG 中的最佳安全性，一個良好的密碼是絕對必要的。例如，在您的密碼中參雜大小寫的字母，並使用數字或標點符號。

在您輸入並確認您的密碼後，就會開始產生您的金鑰，您將會看到類似如下的訊息：

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++.+++++.+++++. . . ++++++. .+++++.+++++.+++++.
+++.....+++++
```

當畫面的動作停止時，您新的金鑰就建立好了，並放置在您家目錄的 .gnupg 目錄下。如要列出您的金鑰，請使用下列指令：

```
gpg --list-keys
```

您將會看到類似如下的訊息：

```
/home/username/.gnupg/pubring.gpg
-----
pub 1024D/B7085C8A 2000-06-18 Your Name <you@example.com>
sub 1024g/E12AF9C4 2000-06-18
```

假如您使用1.0.6 以下的版本來建立GnuPG 金鑰，請匯出您的私鑰，再將它匯入到一個新的私鑰，您必須明確的信任(trust)您自己的金鑰以使用1.0.7 以上的版本來簽署您的訊息。如要信任您的金鑰，請輸入以下的指令（請使用適當的取值代<user-id>）：

```
gpg --edit-key <user-id>
```

在Command> 提示符號下輸入**trust**，並選擇5 = I trust ultimately 以信任您自己的金鑰。

## B.4. 產生一個廢止的憑證

在您建立您的鑰匙對之後，您應該為您的公鑰建立一個廢止憑證。當您忘記您的密碼或該公鑰被破解後，您可以發佈這個憑證以通知使用者們不要再使用您的公鑰。



### 注意

當您建立一個廢止憑證後，您並沒有廢止您剛建立的金鑰，而是在您忘記您的密碼、變更ISP（電子郵件位址）或遭到硬碟毀損等情況時，給予您自己一個安全的方式以撤除大眾使用您的金鑰。這個廢止憑證可以被使用來撤銷您的公鑰。

在您的金鑰撤銷之前，對於閱讀您訊息的其他人，您的簽章仍然有效，而且您也可以解密接收到的訊息。如要產生一個廢止憑證，請使用--gen-revoke 選項：

```
gpg --output revoke.asc --gen-revoke <you@example.com>
```

請注意，假如您省略--output revoke.asc 選項，您的廢止憑證將會轉為標準的輸出，目前也就是您的螢幕畫面。雖然您可以複製輸出的內容並使用文字編輯器來貼到一個檔案中，不過將輸出轉成您登入目錄下的一個檔案也許較容易。使用這種方法，您可以保留這個憑證以便將來使用，或將它儲存在軟碟片並存放在安全的地方。

輸出將如下所示：

```
sec 1024D/823D25A9 2000-04-26 Your Name <you@example.com>
```

```
Create a revocation certificate for this key?
```

按下[Y] 鍵為列出的金鑰建立一個廢止憑證，再來您將會被問及以選取要廢止的理由，並提供一個可選的說明。在確認廢止理由後，請輸入您使用來產生金鑰的密碼。

在您的廢止憑證建立好後(revoke.asc)，它將會被放置在您的登入目錄。您應該要複製該憑證到一張軟碟片，並存放在一個安全的地方。（假如您不知道該如何在Red Hat Linux 下複製檔案到軟碟片，請參考Red Hat Linux 使用手冊。）

## B.5. 匯出您的公鑰

在您使用公鑰的加密法之前，其他人必須擁有您的公鑰，如要傳送您的金鑰到您的聯絡人或到一部金鑰伺服器，您必須匯出您的金鑰。

如要匯出您的金鑰，以使您可以將它放在網頁上或電子郵件上，請輸入下列的指令：

```
gpg --armor --export <you@example.com> > mykey.asc
```

您將不會看到任何的輸出，因為您已匯出您的公鑰並將輸出重導至一個稱為mykey.asc 的檔案。（如果沒有加上> mykey.asc，金鑰的內容將會以標準輸出的方式顯示在螢幕的畫面上。）

現在，mykey.asc 檔案就可以被放入電子郵件或匯出到一部金鑰伺服器上。如要讀取這個金鑰的內容，請輸入less mykey.asc 以在頁面調度程式(pager)中開啟該檔案（按下[q] 鍵以離開該程式）。您所看到的應該如以下所示：

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.1 (GNU/Linux)
```

Comment: For info see <http://www.gnupg.org>

```
mQGIBDkHP3URBACKWGsYh43pkXU9wj/XlG67K8/DSr185r7dNtHNFLL/ewill10k2
q8saWJn26QZPsDVqdUJModHfJ6kQTAtn9NzQbGcVrxLYNfgeBsvkHF/POtnYcZrGLt
z66syBBws8JB4xt5V09iJSGAMPUQE8Jpdn2aRXPapdoDwl179LM8Rq6r+gwcg5ZZa
pGNlkgFu24WM5wC1zg4QTbMD/3MJCSxfL99Ek5HXcB3yhj+o0LmIrGAVBgoWdrRd
BIGjQQFhV1NSwC8YhN/4nGHWpaTxgEtnb4CI1wI/G3DK9o1YMyrJinkGJ6XYfP3b
cCQmgATDF5ugIAmdditnw7deXqn/eavaMxRXJM/RQSGjJyVpbA020qKe6L6Inb5H
kjcZA/9obTm499dDMRQ/CNR92fA5pr0zriy/ziLUow+cqI59nt+bEb9nY1mfmUN6
SW0jCH+pIQH51erV+oookyOyq3ocUdjerYF/d2j19xmeSyL2H3tDvnuE6vgqFU/N
sdvby4B2Iku7S/h06W6GPQAE+pzdyX9vS+Pnf8osu7W3j60WprQkUGFLbcBHYWxs
YwdoZXIgpPHBhdWxnYwxsQHJ1ZGhhdc5jb20+iFYEEExECABYFAjkHP3UECwoEAwMV
AwIDFgIBAheAAoJEJECmVGCPSWpMjQAoNF2zvRgdR/8or9pBhu95zeSnbk7AKCm
/uXVS0a5KON7J61/1vEwx1lpoLkBDQQ5Bz+MEAQA8ztcWRJjW8cHCgLaE402jyqQ
37gDT/n4VS66nU+YItzDFScVmgMuFRzhibLb1f09TpZzxEbSF3T6p9hLLnHCQ1bD
HRsKfh0eJYMMqB3+HyUpNeqCMEEd9AnWD9P4rQt07Pes38sV01X00SvsTyMG9wEB
vSNZk+R1+phA5r1s8cAAwUEAJjqazvk0bgFrw1OPG9m7fEeD1vPSV6HSA0fvz4w
c7ckfpuxg/URQNF3TJA00Acprk8Gg8J2CtebAyR/sP5IsrK511luGdk+10M85FpT
/cen2OdtToAF/6fGnIkeCeP105aWTbDgdAUHBRykpDWU3GJ7NS6923fVg5kHQWg
uwrA1EYEBECAAyFAjkHP4wACgkQkQKa8YI9JamliwCfXox/HjlorMKNQRJkeBcZ
iLyPH1QAOI33Ft/0HBqLtqdtP4vWYQRbijW
=BMEC
-----END PGP PUBLIC KEY BLOCK-----
```

### B.5.1. 匯出到一部金鑰伺服器

假如您只是與少數人做安全性的通訊，您可以匯出您的公鑰，並單獨地郵寄公鑰給他們。假如您是與很多人做這方面的聯絡，將您的公鑰發佈給他們會很費時，不過您可以使用一部金鑰伺服器的方式來輕易做到。

金鑰伺服器是一個位於網際網路的儲存位置，可用它來存放並發放您的公鑰給任何需要它的人。有許多的金鑰伺服器可以使用，其中的大部分都試著要進行同步化，這也使得您只要將您的金鑰傳送至一部金鑰伺服器，該伺服器便會自動傳送至其他所有的伺服器。您的聯絡人可以從一部金鑰伺服器要求您的公鑰，並將之匯入到他們的金鑰環，然後他們就可以和您進行安全的通訊了。



#### 建議

因為大部分的金鑰伺服器都已同步化，將您的公鑰傳送至一部金鑰伺服器就如同將之傳送至全部的伺服器。然而您可以找到不同的金鑰伺服器，以下這個 **Keyserver.Net** 網站可以讓您開始您的搜尋並且提供您更多的相關資訊：<http://www.keyserver.net>。

您可以從 `shell` 提示符號或瀏覽器來傳送您的公鑰，當然您必須有網際網路連線才可以從金鑰伺服器傳送與接收金鑰。

- 在 `shell` 提示符號下輸入以下指令：  
`gpg --keyserver search.keyserver.net --send-key you@example.com`
  - 使用您的瀏覽器，連線至 **Keyserver.Net** (<http://www.keyserver.net>)，然後選擇要加入您 PGP 公鑰的選項。
- 下一步，您可以複製與貼上您的公鑰到網頁上的適當區域，假如您需要如何做到的指示，請遵照以下的步驟：
- 請使用一個頁面調度程式來開啟您所匯出的公鑰檔案（如在 B.5 節建立的 `mykey.asc`）——例如，使用 `less mykey.asc` 指令。

- 使用您的滑鼠，反白選取BEGIN PGP 與END PGP 記號之間的部份來複製這個檔案（請參考圖形B-1）。
- 點選您滑鼠中間的按鈕（如果您是使用兩鍵式的滑鼠，請同時按下左右兩鍵）來貼上mykey.asc 檔案的內容到Keyserver.Net 網頁上的適當區域。然後在金鑰伺服器的網頁上選擇Submit 按鈕。（假如您犯了任何的錯誤，請按下網頁上的Reset 按鈕來清除所貼上的金鑰內容。）



圖形B-1. 複製您的公鑰

請注意，假如您要傳送您的金鑰到另一部網頁界面的金鑰伺服器，基本上都會類似以上的步驟。

這就是您需要做的所有事情，不管您是使用shell 提示符號或透過網頁的介面，您都會看到一個訊息告訴您金鑰已經成功傳送了——從此以後，想要與您安全通訊的使用者都可以匯入您的公鑰並將之加入到他們的金鑰環。

## B.6. 匯入一個公鑰

在金鑰交易的另一端就是匯入其他人的公鑰到您的金鑰環——這和匯出金鑰一樣容易。當您匯入別人的公鑰時，您可以將他們的電子郵件解密，然後針對您金鑰環上的公鑰來核對他們的數位簽章。

匯入金鑰最簡單的其中一種方法是從一個網站下載金鑰然後儲存它。

在下載金鑰然後將它儲存到一個檔案key.asc 後，請使用下列的指令來將它加入您的金鑰環。

```
gpg --import key.asc
```

另一個儲存金鑰的方法是使用瀏覽器的『另存新檔』特色。假如您是使用如Mozilla 的瀏覽器，而您在一部金鑰伺服器找到金鑰，您可以儲存該頁面為一個文字檔案（請選擇File => Save Page As）。在Files of Type 旁的下拉式選單中選擇Text Files (\*.txt)。然後您便可以匯入該金鑰——不過請記得您所儲存的檔案名稱。舉例來說，假如您儲存一個金鑰為一個稱為newkey.txt 的文字檔案，如要匯入該檔案，請在shell 提示符號下輸入以下指令：

```
gpg --import newkey.txt
```

該指令的輸出將會如下所示：

```
gpg: key F78FFE84: public key imported
gpg: Total number processed: 1
```

```
gpg:      imported: 1
```

如要檢查該過程成功與否，請使用 `gpg --list-keys` 指令；您應該會看到您新匯入的金鑰在您的金鑰環上。

當您匯入一個公鑰時，您便已經將它加入您的金鑰環（存放公鑰與私鑰的一個檔案）。然後當您從一個地方下載一個文件或檔案時，您可以針對您增加至金鑰環的金鑰來檢查該文件的有效性與正確性。

## B.7. 數位簽章是什麼？

數位簽章可用來相較於您的親筆簽名。它不像傳統的通訊方式，您的親筆簽名有可能會被竄改，數位簽章是無法偽造的。那是因為該簽章是使用您獨有的私鑰所建立的，然後它可被您的收件人使用您的公鑰來做確認。

一個數位簽章也會標記一個文件的時間戳記；基本上這代表您簽署該文件的時間也是該簽章的一部分。所以當任何人試著要修改該文件時，數位簽章的驗證將會失敗。某些電子郵件的應用程式，例如**Exmh**或**KDE**的**KMail**也都包含了在應用程式介面中使用**GnuPG**來簽署文件的功能。

有兩種好用的數位簽章類型，它們是**clearsigned**文件以及分離的簽章。兩種類型的簽章都合併相同的真實性安全機制，並不需要您的收件人對整個訊息進行解密。

在一個**clearsigned**的訊息中，您的簽名會以一個文字區塊出現在您信件的本文中；而一個分離的簽章是以一個分離的檔案附加在您的信件中與其一併傳送。

## B.8. 其他的資源

除了在此簡單介紹**GnuPG**以外，還有很多關於加密技術的資料，以下列出一些您可以參考的種種資源。

### B.8.1. 已安裝的說明文件

- `man gpg` 與 `info gpg` — **GnuPG** 指令以及選項的快速檢索。

### B.8.2. 有用的網站

- <http://www.gnupg.org> — **GnuPG** 的官方網站，其中含有最新發行之**GnuPG**的連結、一個完整的使用者手冊以及其他密碼學的種種資源。
- <http://hotwired.lycos.com/webmonkey/backend/security/tutorials/tutorial1.html> — 請造訪**Webmonkey**的**Encryption Tutorial**以學習更多關於密碼學以及如何套用加密的技術。
- <http://www.eff.org/pub/Privacy> — 電子前鋒基金會(**The Electronic Frontier Foundation**) "**Privacy, Security, Crypto, & Surveillance**" 的資料中心。

### B.8.3. 相關的書籍

- 由Philip R. Zimmerman 著作，MIT Press 出版的**The Official PGP User's Guide**
- 由Simon Garfinkel 著作，O'Reilly & Associates, Inc. 出版的**PGP: Pretty Good Privacy**
- 由Bruce Schneier 著作，John Wiley & Sons 出版的**E-Mail Security: How to Keep Your Electronic Messages Private**





# 索引

## Symbols

- /dev/shm, 190
- /etc/auto.master, 117
- /etc/cups/, 195
- /etc/exports, 120
- /etc/fstab, 2, 117
- /etc/fstab 檔案
  - 啟用磁碟配額使用, 21
- /etc/hosts, 92
- /etc/httpd/conf/httpd.conf, 137
- /etc/named.custom, 161
- /etc/printcap, 195
- /etc/printcap.local, 195
- /etc/sysconfig/dhcpd, 134
- /etc/sysconfig/iptables, 99, 102
- /proc 目錄, 193
- /var/spool/cron, 214
- 乙太網路連線
  - (見網路設定)
- 分割區
  - 加上標籤
    - e2label, 17
  - 建立, 16
  - 重新調整大小, 19
  - 格式化
    - mkfs, 17
  - 移除, 18
  - 製作
    - mkpart, 17
  - 檢視清單, 16
- 主控台
  - 使檔案可存取從, 176
- 主控台存取
  - 定義, 176
  - 停用, 175
  - 停用所有, 176
  - 啟用, 177
  - 設定, 175
- 主開機紀錄(MBR), 67
- 加密
  - 使用GnuPG, 257
- 平行儲存
  - RAID 的原理, 9
- 列印系統轉換器, 211
- 印表機設定, 195
  - CUPS, 195
  - GNOME 列印管理員, 207
    - 更改印表機設定, 208
  - IPP 印表機, 197
  - JetDirect 印表機, 201
  - Novell NetWare (NCP) 印表機, 200
  - Samba (SMB) 印表機, 199
  - 分享, 209

- 文字介面的應用程式, 195
- 本機印表機, 196
- 共享
  - 可存取的主機, 210
  - 全系統性選項, 210
  - 使用LPReq, 211
- 刪除既有的印表機, 203
- 取消列印工作, 209
- 命令列選項, 206
  - 回復設定, 205
  - 移除一部印表機, 207
  - 新增一部印表機, 206
  - 儲存設定, 205
- 重要的設定, 205
- 重新命名既有的印表機, 204
- 修改既有的印表機, 203
- 從命令列中進行列印, 209
- 提示圖示, 208
- 測試頁, 203
- 匯出設定, 205
- 新增
  - CUPS (IPP) 印表機, 197
  - IPP 印表機, 197
  - JetDirect 印表機, 201
  - LPD 印表機, 198
  - Novell NetWare (NCP) 印表機, 200
  - Samba (SMB) 印表機, 199
  - 本機印表機, 196
- 預設印表機, 203
- 管理列印工作, 207
- 網路連線的CUPS (IPP) 印表機, 197
- 遠端的LPD 印表機, 198
- 編輯既有的印表機, 203
- 編輯驅動程式, 204
- 儲存設定到檔案, 205
- 檢視列印緩衝器, 208
- 檢視列印緩衝器、命令列, 209
- 驅動程式選項, 204
  - GhostScript pre-filtering, 205
  - Media Source, 205
  - 有效的過濾器區域性, 205
  - 頁面大小, 205
  - 假定未知的資料為文字, 204
  - 傳送End-of-Transmission (EOT), 204
  - 傳送Form-Feed (FF), 204
  - 預先處理Postscript, 205
  - 轉換文字成Postscript, 205
- 印表機設定工具
  - (見印表機設定)
- 回應, iv
- 安全伺服器
  - URLs, 158
  - URLs 用於, 158
  - 已安裝的文件, 159
  - 升級從, ??
  - 存取, 158

- 安全性
  - 的解釋, 153
- 安全性的解釋, 153
- 安裝, 151
- 金鑰
  - 產生, 155
- 套件, 151
- 書籍, 159
- 連接埠號, 158
- 連線至, 158
- 提供一個憑證用於, 153
- 網站, 159
- 憑證
  - 之前已有的, 153
  - 在升級後移動它, 154
  - 自我簽署的, 157
  - 要求的建立, 156
  - 測試, 158
  - 測試(test) vs. 簽署(signed) vs. 自我簽署(self-signed), 154
  - 機關, 154
  - 選擇一個CA, 154
- 安全性, 105
- 安全等級
  - (見安全等級設定工具)
- 安全等級設定工具
  - iptables 服務, 102
- 安全等級
  - 中安全性, 98
  - 高安全性, 97
  - 無防火牆, 98
- 自訂信任裝置, 98
- 自訂進入的服務, 98
- 安裝
  - kickstart
    - (見kickstart 安裝)
  - LVM, 75
  - 軟體RAID, 71
- 自動工作排程管理, 213
- 系統回復, 67
- 一般問題, 67
  - 忘記root 密碼, 67
  - 無法開機進入Red Hat Linux, 67
  - 硬體/軟體問題, 67
- 系統服務設定工具, 106
- 系統資訊
  - 收集, 187
  - 記憶體用量, 189
  - 硬體, 191
  - 程序, 187
  - 正在執行中, 187
  - 檔案系統, 190
    - /dev/shm, 190
    - 監視, 191
- 防火牆設定
  - (見GNOME Lokkit)
- 使用者
  - (見使用者設定)
- 使用者設定
  - 命令列設定, 182
    - passwd, 182
    - useradd, 182
  - 修改使用者, 180
  - 修改使用者的群組, 180
- 密碼
  - 強迫過期, 183
  - 密碼失效日期, 181
  - 設定使用者帳號的有效期限, 181
  - 新增使用者, 179
  - 過濾使用者清單, 179
  - 增加使用者到群組中, 181
  - 檢視使用者清單, 179
  - 鎖定使用者帳號, 181
  - 變更全名, 181
  - 變更家目錄, 181
  - 變更密碼, 181
  - 變更登入shell, 181
- 使用者管理員
  - (見使用者設定)
- 命令列選項
  - 列印從, 209
- 服務
  - 控制存取, 105
- 紀錄檔案, 219
  - (另見紀錄檔檢視器)
  - syslogd, 219
  - 尋找, 219
  - 循環的, 219
  - 說明, 219
  - 檢查, 220
  - 檢視, 219
- 紀錄檔檢視器
  - 紀錄檔案的位置, 220
  - 重新整理頻率, 219
  - 搜尋, 220
  - 過濾, 220
  - 警示, 220
- 套件
  - 小技巧, 240
  - 升級, 236
  - 安裝
    - 使用套件管理工具, 243
  - 安裝中, 234
  - 找出說明文件給, 240
  - 決定檔案擁有權使用, 240
  - 使用RPM 做freshening, 237
  - 取得檔案清單, 241
  - 保留設定檔案, 236
  - 查詢, 237
  - 查詢解除安裝的, 240
  - 相依性問題, 235
  - 校驗, 238

- 移除, 236
  - 使用套件管理工具, 244
- 搜尋已刪除的檔案從, 240
- 套件管理工具, 243
  - 安裝套件, 243
  - 移除套件, 244
- 核心
  - 下載, 222
  - 升級, 221
  - 多處理器支援, 222
  - 自訂, 253
  - 建立, 253
  - 超大記憶體支援, 222
  - 集成式, 255
    - 自訂, 255
    - 建立, 255
  - 模組, 227
  - 模組化, 253
- 核心模組
  - 列出, 227
  - 卸載, 228
  - 載入, 228
- 記號環狀網路連線
  - (見網路設定)
- 記憶體用量, 189
- 動態主機設定協定
  - (見DHCP)
- 執行等級, 105
- 執行等級1, 69
- 密碼
  - 有效期限, 183
  - 強迫過期, 183
  - 密碼過期、強迫, 183
- 掛載
  - NFS 檔案系統, 117
- 救援模式
  - 可使用的工具, 69
  - 定義, 67
- 組態設定
  - 主控台存取, 175
- 設定
  - NFS, 117
- 軟體RAID
  - (見RAID)
- 單一使用者模式, 69
- 硬體
  - 檢視, 191
- 硬體RAID
  - (見RAID)
- 硬體瀏覽器, 191
- 程序, 187
- 郵件用戶代理(Mail User Agent), 171
- 郵件傳送代理
  - (見MTA)
- 郵件傳送代理轉換器, 171
  - 以文字模式啟動, 171
- 開發套件, 151
- 開機
  - 救援模式, 67
  - 單一使用者模式, 69
  - 緊急模式, 70
- 開機片, 221
- 匯出NFS 檔案系統, 118
- 群組
  - (見群組設定)
  - 軟碟片、使用, 178
- 群組設定
  - groupadd, 183
  - 修改使用者的群組, 180
  - 修改群組中的使用者, 182
  - 修改群組內容, 181
  - 新增群組, 181
  - 過濾群組清單, 179
  - 檢視群組清單, 179
- 解密
  - 使用GnuPG, 257
- 資訊
  - 關於您的系統, 187
- 載入核心模組, 227
- 實體磁區, 13, 75
- 實體範圍, 76
- 慣用形式
  - 文件, ii
- 磁區群組, 13
- 磁碟分割區表
  - 檢視, 16
- 磁碟容量
  - (見磁碟配額)
- 磁碟配額, 21
  - 其他的資源, 25
  - 非強制性限制, 23
  - 指定給每一個使用者, 22
  - 指定給每一個群組, 23
  - 指定給每一個檔案系統, 23
  - 停用, 25
  - 強制性限制, 23
  - 啟用, 21, 25
    - /etc/fstab、修改, 21
    - quotacheck、執行, 22
    - 建立配額檔案, 22
  - 管理, 24
    - quotacheck 指令、用來檢查, 24
    - 報告, 24
  - 寬限期, 23
- 磁碟儲存空間
  - parted
    - (見parted)
- 緊急模式, 70
- 網路設定
  - CIPE 連線, 89
  - DHCP, 82
  - ISDN 連線, 83

- 啟用, 84
- PPPoE 連線, 86
- xDSL 連線, 86
  - 啟用, 88
- 乙太網路連線, 82
  - 啟用, 83
- 記號環狀網路連線, 88
  - 啟用, 89
- 啟用裝置, 93
- 無線網路連線, 90
  - 啟用, 91
- 概要, 82
- 裝置別名, 95
- 資料檔, 94
  - 啟用, 95
- 管理/etc/hosts 檔案, 92
- 管理DNS 設定, 91
- 管理主機, 92
- 數據機連線, 85
  - 啟用, 86
- 靜態IP, 82
  - 邏輯網路裝置, 94
- 網路裝置控制, 93, 95
- 網路管理工具
  - (見網路設定)
- 網路認證設定工具, 167
  - 使用者資訊, 167
    - Hesiod, 168
    - LDAP, 168
    - NIS, 168
  - 緩衝貯存, 167
  - 命令列版本, 169
  - 認證, 168
    - Kerberos 支援, 169
    - LDAP 支援, 168
    - MD5 編碼, 168
    - shadow 密碼, 168
    - SMB 支援, 169
- 網路檔案系統
  - (見NFS)
- 網際網路連線
  - (見網路設定)
- 認證, 167
- 說明文件
  - 搜尋已安裝的, 240
- 數據機連線
  - (見網路設定)
- 檔案系統, 190
  - ext2
    - (見ext2)
  - ext3
    - (見ext3)
  - LVM
    - (見LVM)
  - NFS
    - (見NFS)

- 監視, 191
- 簡介, i
- 關機
  - 停用CtrlAltDel , 175
- 邏輯群組, 75
- 邏輯磁區, 13, 76
- 邏輯磁區群組, 13, 75
- 邏輯磁區管理員
  - (見LVM)

## A

- anacron
  - 其他的資源, 218
- Apache HTTP 伺服器
  - (見HTTP 設定工具)
  - 其他的資源, 149
  - 保全, 153
  - 相關的書籍, 150
- APXS, 151
- at, 216
  - 其他的資源, 218
- authconfig
  - (見網路認證設定工具)
- authconfig-gtk
  - (見網路認證設定工具)
- autofs, 117
  - /etc/auto.master, 117

## B

- batch, 216
  - 其他的資源, 218
- BIND 組態設定, 161
  - 套用變更, 161
  - 新增一個反解主網域, 163
  - 新增一個正解主網域, 161
  - 新增一個次網域, 165
  - 預設目錄, 161

## C

- CA
  - (見安全伺服器)
- chage 指令
  - 強迫密碼過期使用, 183
- chkconfig, 108
- CIPE 連線
  - (見網路連線)
- Cron, 213
  - crontabs 的範例, 214
  - 使用者定義的工作, 214
  - 其他的資源, 218
  - 設定檔案, 213
- crontab, 213
- CtrlAltDel
  - 關機、停用, 175
- CUPS, 195

## D

- df, 190
- DHCP, 131
  - dhcpd.conf, 131
  - dhcpd.leases, 134
  - dhcrelay, 135
  - group, 132
  - shared-network, 132
  - subnet, 132
  - 用戶端設定, 135
  - 全域性的參數, 132
  - 伺服器設定, 131
  - 使用的原因, 131
  - 其他的資源, 136
  - 命令列選項, 134
  - 停止伺服器, 134
  - 啟動伺服器, 134
  - 連線至, 135
  - 選項, 131
  - 轉接代理, 135
- dhcpd.conf, 131
- dhcpd.leases, 134
- dhcrelay, 135
- diskcheck, 191
- DSA 金鑰keys
  - 產生, 114
- DSOs
  - 載入, 151
- du, 190

## E

- e2fsck, 2
- e2label, 17
- exports, 120
- ext2
  - 從ext3 還原, 2
- ext3
  - 建立, 1
  - 特色, 1
  - 從ext2 轉換, 2

## F

- floppy 群組、使用, 178
- free, 189
- ftp, 111

## G

- GNOME Lokkit
  - DHCP, 101
  - iptables 服務, 102
  - 本地端主機, 100
  - 基本的防火牆設定, 100
  - 啟動防火牆, 102
  - 設定一般的服務, 101
  - 郵件轉送, 102
- GNOME 列印管理員, 207
  - 更改印表機設定, 208
- GNOME 系統監控, 188
- gnome-lokkit
  - (見GNOME Lokkit)
- gnome-system-monitor, 188
- Gnu Privacy Guard
  - (見GnuPG)
- GnuPG
  - 不安全的記憶體警告, 258
  - 其他的資源, 263
  - 產生一個廢止的憑證, 260
  - 產生一副鑰匙對, 258
  - 匯入一個公鑰, 262
  - 匯出公鑰, 260
    - 至金鑰伺服器, 261
  - 數位簽章, 263
  - 檢查RPM 套件的簽章, 239
  - 簡介, 257, 257
  - 警告訊息, 258
- GPG
  - (見GnuPG)

## H

hesiod, 168

HTTP 指令

DirectoryIndex, 139

ErrorDocument, 140

ErrorLog, 141

Group, 148

HostnameLookups, 141

KeepAlive, 148

KeepAliveTimeout, 148

Listen, 138

LogFormat, 141

LogLevel, 141

MaxClients, 148

MaxKeepAliveRequests, 148

Options, 139

ServerAdmin, 138

ServerName, 138

TimeOut, 148

TransferLog, 141

User, 147

HTTP 設定工具

指令

(見HTTP 指令)

傳輸紀錄檔, 140

模組, 137

錯誤紀錄檔, 140

httpd, 137

hwbrowser, 191

## I

insmod, 228

ISDN 連線

(見網路設定)

## K

Kerberos, 169

kickstart

如何找到該檔案, 48

kickstart 安裝, 29

LVM, 37

光碟為主的, 47

安裝目錄, 48

開始, 48

從第一片光碟以及一片磁片, 48

從開機片, 48

從開機光碟, 48

磁片為主的, 47

網路為主的, 47, 48

檔案位置, 47

檔案格式, 29

Kickstart 設定程式, 51

%post 程式碼, 64

%pre 程式碼, 63

root password, 51

root 密碼

加密, 51

X 組態設定, 59

互動模式, 52

文字模式安裝, 52

防火牆組態設定, 59

重新開機, 52

時區, 51

基本選項, 51

開機管理程式, 53

開機管理程式選項, 53

滑鼠, 51

預覽, 51

磁碟分割, 54

軟體RAID, 55

網路組態設定, 57

語言, 51

語言支援, 52

認證選項, 58

選取套件, 62

選擇安裝方式, 52

儲存, 65

鍵盤, 51

kickstart 檔案

%include, 43

%post, 45

%pre, 44

auth, 30

authconfig, 30

autostep, 30

bootloader, 32

clearpart, 33

device, 33

deviceprobe, 34

driverdisk, 34

firewall, 34

install, 35

interactive, 36

keyboard, 36

lang, 36

langsupport, 36

lilo, 37

lilocheck, 37

logvol, 37

mouse, 37

network, 38

part, 39

partition, 39

raid, 41

reboot, 41

rootpw, 41

skipx, 42

text, 42

timezone, 42  
 upgrade, 42  
 volgroup, 43  
 xconfig, 42  
 zerombr, 43  
 光碟為主的, 47  
 安裝方式, 35  
 含括另一檔案的內容, 43  
 前置安裝的組態設定, 44  
 建立, 30  
 後續安裝的組態設定, 45  
 套件選擇的指定, 43  
 格式, 29  
 磁片為主的, 47  
 網路為主的, 47, 48  
 選項, 30  
 檔案看起來像什麼, 29

## L

LDAP, 168, 168  
 logrotate, 219  
 lpd, 196  
 LPRng, 195  
 lsmod, 227  
 lspci, 192  
 LVM, 13  
   安裝過程中設定LVM, 75  
   使用kickstart, 37  
   解釋, 13  
   實體磁區, 13, 75  
   實體範圍, 76  
   邏輯磁區, 13, 76  
   邏輯磁區群組, 13, 75

## M

Maximum RPM, 241  
 MD5 編碼, 168  
 mkfs, 17  
 mkpart, 17  
 modprobe, 228  
 modules.conf, 227  
 MTA  
   使用郵件傳送代理轉換器轉換, 171  
   預設設定, 171  
 MUA, 171

## N

named.conf, 161  
 neat  
   (見網路設定)  
 netcfg  
   (見網路設定)  
 NFS  
   /etc/fstab, 117  
   autofs  
     (見autofs)  
   主機名稱的格式, 121  
   伺服器的狀態, 121  
   其他的資源, 122  
   命令列設定, 120  
   停止伺服器, 121  
   掛載, 117  
   啟動伺服器, 121  
   設定, 117  
   匯出, 118  
 NFS 伺服器設定工具, 118  
 NIS, 168  
 ntsysv, 108

## O

O'Reilly & Associates, Inc., 122, 150, 263  
 OpenLDAP, 168, 168  
 openldap-clients, 168  
 OpenSSH, 111  
   DSA 金鑰  
     產生, 114  
   RSA 版本1的金鑰  
     產生, 114  
   RSA 金鑰  
     產生, 113  
   ssh-add, 115  
   ssh-agent, 115  
     在GNOME 中, 114  
   ssh-keygen  
     DSA, 114  
     RSA, 113  
     RSA 版本1, 114  
   用戶端, 111  
     scp, 112  
     sftp, 113  
     ssh, 112  
   伺服器, 111  
     /etc/ssh/sshd\_config, 111  
     啟動與停止, 111  
   其他的資源, 115  
   產生金鑰對, 113  
 OpenSSL  
   其他的資源, 115

## P

- pam\_smbpass, 128
- pam\_timestamp, 177
- parted, 15
  - 建立分割區, 16
  - 指令表, 15
  - 重新調整分割區的大小, 19
  - 移除分割區, 18
  - 概要, 15
  - 選取裝置, 16
  - 檢視磁碟分割區表, 16
- PCI 裝置
  - 列表, 192
- postfix, 171
- PPPoE, 86
- printconf
  - (見印表機設定)
- printtool
  - (見印表機設定)
- ps, 187

## Q

- quotacheck, 22
  - quotacheck 指令
    - 使用來檢查磁碟配額的正確性, 24
- quotaoff, 25
- quotaon, 25

## R

- RAID, 9
  - level 0, 10
  - level 1, 10
  - level 4, 10
  - level 5, 10
  - 使用的原因, 9
  - 設定軟體RAID, 71
  - 軟體RAID, 9
  - 硬體RAID, 9
    - 解釋, 9
    - 模式, 10
- RAM, 189
- rcp, 112
- Red Hat Network, 247
- Red Hat 更新代理程式, 247
- redhat-config-httpd
  - (見HTTP 設定工具)
- redhat-config-kickstart
  - (見Kickstart 設定程式)
- redhat-config-network
  - (見網路設定)
- redhat-config-network-cmd, 95
- redhat-config-network-tui

- (見網路設定)
- redhat-config-packages
  - (見套件管理工具)
- redhat-config-printer
  - (見印表機設定)
- redhat-config-securitylevel
  - (見安全等級設定工具)
- redhat-config-users
  - (見使用者設定and 群組設定)
- redhat-control-network
  - (見網路裝置控制)
- redhat-logviewer
  - (見紀錄檔檢視器)
- redhat-switch-mail
  - (見郵件傳送代理轉換器)
- redhat-switch-mail-nox
  - (見郵件傳送代理轉換器)
- redhat-switch-printer
  - (見列印系統轉換器)
- resize2fs, 2
- RHN
  - (見Red Hat Network)
- rmmod, 228
- RPM, 233
  - freshen, 237
  - freshening 套件, 237
  - GnuPG, 239
  - md5sum, 239
  - 小技巧, 240
  - 升級, 236
  - 安裝
    - 使用套件管理工具, 243
  - 安裝中, 234
  - 決定檔案擁有權使用, 240
  - 使用, 234
  - 其他的資源, 241
  - 保留設定檔案, 236
  - 查詢, 237
  - 查詢解除安裝的套件, 240
  - 查詢檔案清單, 241
  - 相依性問題, 235
  - 相關的書籍, 241
  - 校驗, 238
  - 設計的宗旨, 233
  - 搜尋已刪除的檔案使用, 240
  - 解除安裝, 236
    - 使用套件管理工具, 244
  - 圖形介面, 243
  - 網站, 241
  - 說明文件使用, 240
  - 檔案衝突
    - 解決, 235
  - 檢查套件的簽章, 239
- RPM Package Manager
  - (見RPM)
- RSA 版本1 的金鑰



產生, 114  
 RSA 金鑰  
 產生, 113

## S

Samba, 123  
 pam\_smbpass, 128  
 共享資源  
   使用Nautilus 連線至, 129  
   連線到, 129  
 伺服器的狀態, 128  
 使用passwd 同步密碼syncing passwords with  
 passwd, 128  
 使用Windows NT 4.0, 2000, ME 與XP, 127  
 使用的原因, 123  
 其他的資源, 130  
 停止伺服器, 128  
 密碼加密, 127  
 啟動伺服器, 128  
 設定, 123, 127  
   smb.conf, 123  
   預設, 123  
 圖形化的設定, 123  
   配置伺服器設定, 124  
   新增共享, 126  
   管理Samba 使用者, 125

scp  
 (見OpenSSH)

sendmail, 171

sftp  
 (見OpenSSH)

shadow 密碼, 168

SMB, 123, 169

smb.conf, 123

ssh  
 (見OpenSSH)

ssh-add, 115

ssh-agent, 115  
 在GNOME 中, 114

swap 空間, 5  
   建議值, 5  
   移除, 6  
   移動, 7  
   解釋, 5  
   增加, 5

syslogd, 219

## T

TCP 包裹程式, 106  
 telinit, 106  
 telnet, 111  
 top, 187  
 tune2fs  
   還原到ext2 使用, 2  
   轉換為ext3 使用, 2

## U

useradd 指令  
   建立使用者帳號使用, 182

## V

VeriSign  
   使用既有的憑證, 153

## W

Windows  
   檔案與列印共享, 123

Windows 2000  
   使用Samba 連線至共享, 127

Windows 98  
   使用Samba 連線至共享, 127

Windows ME  
   使用Samba 連線至共享, 127

Windows NT 4.0  
   使用Samba 連線至共享, 127

Windows XP  
   使用Samba 連線至共享, 127

## X

xDSL 連線  
 (見網路設定)

xinetd, 106

## Y

ypbind, 168



Red Hat Linux 手冊是以DocBook SGML v4.1 格式撰寫的。HTML 與PDF 格式的手冊是使用自訂的DSSSL stylesheets 與自訂的jade wrapper 程式碼所產生的。DocBook SGML 檔案是在Emacs 程式中所撰寫（加上PSGML 模式的輔助）。

提示的圖像（如『請注意』、『建議』、『重要』、『警示』以及『警告』）是由Garrett LeSage 所製作。它們可以隨著Red Hat 的說明文件一起自由散佈。

Red Hat Linux 產品的說明文件團隊是由以下的成員組成：

Sandra A. Moore — *Red Hat Linux x86* 安裝手冊的主要作者與維護者；*Red Hat Linux* 使用手冊的作者群之一

Tammy Fox — *Red Hat Linux* 用戶自訂手冊的主要作者與維護者；*Red Hat Linux* 使用手冊的作者群之一；自訂DocBook stylesheets 與程式碼的作者與維護者

Edward C. Bailey — *Red Hat Linux* 系統管理入門的主要作者與維護者；*Red Hat Linux x86* 安裝手冊的作者群之一

Johnray Fuller — *Red Hat Linux* 參考手冊的主要作者與維護者；*Red Hat Linux* 安全性設定手冊的共同作者/共同維護者；*Red Hat Linux* 系統管理入門的作者群之一

John Ha — *Red Hat Linux* 使用手冊的主要作者與維護者；*Red Hat Linux* 安全性設定手冊的共同作者/共同維護者；*Red Hat Linux* 系統管理入門的作者群之一

Ben Wu — *Red Hat Linux x86* 安裝手冊、*Red Hat Linux* 使用手冊、*Red Hat Linux* 用戶自訂手冊的繁體中文翻譯者

