

SUSE Linux Enterprise Server

11 SP3

www.suse.com

2013 年 6 月 10 日

管理指南



管理指南

版權所有 © 2006-2013 SUSE LLC 和貢獻者。保留所有權利。

根據 GNU 自由文件授權 (GNU Free Documentation License) 1.2 版或 1.3 版 (自由選擇)，使用者可以複製、散佈與/或修改本文件；「恆常章節」為此著作權聲明與授權。「GNU 自由文件授權」一節中包含 1.2 版授權的一份副本。

如需 SUSE 和 Novell 商標之相關資訊，請參閱 Novell 商標和服務標誌清單 <http://www.novell.com/company/legal/trademarks/tmlist.html>。所有其他協力廠商商標，為各所有人所有之財產。商標符號 (®、™ 等) 代表 SUSE 或 Novell 的商標；星號 (*) 則代表協力廠商的商標。

本手冊中所有資訊在編輯時，都已全力注意各項細節。但這不保證百分之百的正確性。因此，SUSE LLC 及其附屬公司、作者或譯者都不需對任何錯誤或造成的結果負責。

目錄

關於本指南	xiii
1 可用文件	xiv
2 意見反應	xv
3 文件慣例	xvi
 I 支援與一般任務	 1
1 YaST 線上更新	3
1.1 線上更新對話方塊	4
1.2 安裝修補程式	7
1.3 自動線上更新	8
 2 收集系統資訊以供支援所用	 11
2.1 綜覽	11
2.2 使用 Supportconfig 收集資訊	11
2.3 向 Novell 提交資訊	13
2.4 如需更多資訊	15
 3 文字模式的 YaST	 17
3.1 在模組中瀏覽	18
3.2 組合鍵的限制	20
3.3 YaST 指令行選項	20

4 使用 Snapper 執行快照/復原	23
4.1 要求	23
4.2 使用 Snapper 復原系統變更	24
4.3 手動建立和管理快照	34
4.4 限制	38
4.5 常見問題解答	39
4.6 對簡易佈建的 LVM 磁碟區使用 Snapper	40
5 透過 VNC 進行遠端存取	41
5.1 一次性 VNC 工作階段	41
5.2 永久 VNC 工作階段	43
6 使用指令行工具管理軟體	47
6.1 使用 Zypper	47
6.2 RPM — 套件管理員	60
7 Bash 和 Bash 程序檔	71
7.1 什麼是「外圍程序」?	71
7.2 寫入外圍程序程序檔	77
7.3 重新指向指令事件	78
7.4 使用別名	79
7.5 使用 Bash 中的變數	79
7.6 分組與組合指令	82
7.7 使用通用流程建構元	83
7.8 如需更多資訊	84
II 系統	85
8 64 位元系統環境的 32 位元和 64 位元應用程式	87
8.1 執行期間支援	87

8.2 軟體開發	88
8.3 Biarch 平台的軟體編譯	89
8.4 核心規格	90
9 啟動及設定 Linux 系統	93
9.1 Linux 開機程序	93
9.2 init 程序	97
9.3 透過 /etc/sysconfig 設定系統組態	105
10 開機載入程式 GRUB	109
10.1 使用 GRUB 開機	110
10.2 使用 YaST 設定開機載入程式	119
10.3 解除安裝 Linux 開機載入程式	125
10.4 建立開機 CD	126
10.5 圖形化 SUSE 畫面	127
10.6 疑難排解	127
10.7 如需更多資訊	129
11 UEFI (整合可延伸韌體介面)	131
11.1 安全開機	132
11.2 更多資訊	138
12 特殊系統功能	139
12.1 特殊軟體套件的資訊	139
12.2 虛擬主控台	146
12.3 鍵盤配置	146
12.4 語言與國家專用的設定	147
13 印表機操作	151
13.1 列印系統的工作流程	152

13.2 連接印表機的方法和通訊協定	153
13.3 安裝軟體	153
13.4 網路印表機	154
13.5 由指令行開始列印	156
13.6 SUSE Linux Enterprise Server 中的特殊功能	156
13.7 疑難排解	159
14 使用 udev 進行動態核心設備管理	167
14.1 /dev 目錄	167
14.2 核心 uevent 和 udev	168
14.3 驅動程式、核心模組和設備	168
14.4 開機和初始設備設定	169
14.5 監控執行中的 udev 精靈	169
14.6 透過 udev 規則影響核心設備事件的處理	170
14.7 永久設備命名	177
14.8 udev 使用的檔案	177
14.9 如需更多資訊	178
15 X Window System	179
15.1 手動設定 X Window System	179
15.2 安裝與設定字型	185
15.3 如需更多資訊	191
16 使用 FUSE 存取檔案系統	193
16.1 設定 FUSE	193
16.2 可用的 FUSE 外掛程式	193
16.3 如需更多資訊	194

III 行動電腦 195

17 Linux 的行動計算功能 197

17.1 筆記型電腦	197
17.2 行動硬體	204
17.3 行動電話和 PDA	204
17.4 如需更多資訊	204

18 無線區域網路 207

18.1 WLAN 標準	207
18.2 運作模式	208
18.3 驗證	209
18.4 加密	210
18.5 使用 YaST 進行設定	211
18.6 設定 WLAN 的秘訣與技巧	218
18.7 疑難排解	220
18.8 如需更多資訊	221

19 電源管理 223

19.1 省電功能	223
19.2 進階組態與電源介面 (ACPI)	224
19.3 硬碟的休眠	226
19.4 疑難排解	228
19.5 如需更多資訊	229

20 使用 Tablet PC 231

20.1 安裝 Tablet PC 套件	232
20.2 設定手寫板設備	233
20.3 使用虛擬鍵盤	233
20.4 旋轉顯示器	233

20.5 使用筆勢辨識	234
20.6 使用筆來做筆記和素描	236
20.7 疑難排解	238
20.8 如需更多資訊	239

IV 服務 241

21 基本網路 243

21.1 IP 位址與路由	246
21.2 IPv6—下一代的網際網路	249
21.3 名稱解析	257
21.4 使用 YaST 手動設定網路連線	258
21.5 NetworkManager	280
21.6 手動設定網路連線	281
21.7 設定 Bonding 設備	296
21.8 smpppd 做為撥號助理	300

22 網路中的 SLP 服務 303

22.1 安裝	303
22.2 啟用 SLP	304
22.3 SUSE Linux Enterprise Server 中的 SLP 前端	304
22.4 透過 SLP 安裝	304
22.5 透過 SLP 提供服務	305
22.6 如需更多資訊	306

23 使用 NTP 進行時間同步化 307

23.1 使用 YaST 設定 NTP 用戶端	307
23.2 手動設定網路中的 NTP	311
23.3 執行時期的動態時間同步	311

23.4 設定本地參考時鐘	312
23.5 將時鐘與外部時間參考 (ETR) 同步	313

24 網域名稱系統 315

24.1 DNS 詞彙	315
24.2 安裝	316
24.3 使用 YaST 進行設定	316
24.4 啟動 BIND 名稱伺服器	324
24.5 /etc/named.conf 組態檔案	326
24.6 區域檔案	330
24.7 區域資料的動態更新	333
24.8 安全交易	334
24.9 DNS 安全性	335
24.10 如需更多資訊	335

25 DHCP 337

25.1 使用 YaST 設定 DHCP 伺服器	338
25.2 DHCP 軟體套件	349
25.3 DHCP 伺服器 dhcpd	350
25.4 如需更多資訊	353

26 使用 NetworkManager 355

26.1 NetworkManager 的使用案例	355
26.2 啟用或停用 NetworkManager	356
26.3 設定網路連線	357
26.4 使用 KNetworkManager	359
26.5 使用 GNOME NetworkManager Applet	364
26.6 NetworkManager 與 VPN	366
26.7 NetworkManager 和安全性	367

26.8 常見問題解答	368
26.9 疑難排解	370
26.10 如需更多資訊	371
27 Samba	373
27.1 術語	373
27.2 啟動和停止 Samba	375
27.3 設定 Samba 伺服器	375
27.4 設定用戶端	382
27.5 做為登入伺服器的 Samba	382
27.6 含 Active Directory 的網路中之 Samba 伺服器	383
27.7 如需更多資訊	385
28 使用 NFS 共享檔案系統	387
28.1 術語	387
28.2 安裝 NFS 伺服器	388
28.3 設定 NFS 伺服器	388
28.4 設定用戶端	396
28.5 如需更多資訊	399
29 檔案同步化	401
29.1 可用的資料同步化軟體	401
29.2 選取程式時所要考慮的決定性因素	402
29.3 CVS 簡介	405
29.4 rsync 簡介	408
29.5 如需更多資訊	409
30 Apache HTTP 伺服器	411
30.1 快速入門	411
30.2 設定 Apache	413

30.3 啟動和停止 Apache	427
30.4 安裝、啟用和設定模組	429
30.5 啟用 CGI 程序檔	437
30.6 設定提供 SSL 的安全網頁伺服器	439
30.7 避免安全性問題	446
30.8 疑難排解	448
30.9 如需更多資訊	449
31 使用 YaST 設定 FTP 伺服器	451
31.1 啟動 FTP 伺服器	452
31.2 FTP 一般設定	453
31.3 FTP 效能設定	454
31.4 驗證	454
31.5 進階設定	455
31.6 更多資訊	455
32 Squid 代理伺服器	457
32.1 關於代理快取的說明	457
32.2 系統需求	459
32.3 啟動 Squid	460
32.4 /etc/squid/squid.conf 組態檔案	463
32.5 設定操作順暢的代理	467
32.6 cachemgr.cgi	470
32.7 squidGuard	472
32.8 使用 Calamaris 產生快取報告	473
32.9 如需更多資訊	474
33 透過 SFCB 實作的網路企業管理	475
33.1 簡介與基本概念	475

33.2 設定 SFCB	476
33.3 SFCB CIMOM 組態	482
33.4 進階 SFCB 任務	495
33.5 如需更多資訊	503

V 疑難排解 **505**

34 說明和文件 **507**

34.1 文件目錄	508
34.2 線上文件	510
34.3 Info 頁面	511
34.4 線上資源	511

35 一般問題和解決方案 **513**

35.1 尋找並收集資訊	513
35.2 安裝問題	516
35.3 開機問題	525
35.4 登入問題	527
35.5 網路問題	534
35.6 資料問題	538
35.7 IBM System z: 使用 initrd 做為救援系統	551

A 網路範例 **555**

B GNU Licenses **557**

B.1 GNU Free Documentation License	557
--	-----

關於本指南

本指南的主要對象為操作 SUSE® Linux Enterprise 期間的專業網路和系統管理員。因此，本指南的重點只在於確保 SUSE Linux Enterprise 的設定正確，而且網路所需服務都已備妥，讓它可以像初始安裝一樣正常運作。至於如何確保 SUSE Linux Enterprise 能夠與您企業的應用程式軟體正確相容，或其核心功能能否符合您的要求，則不在本指南的討論範圍。本文假設您可符合完整需求，且需要安裝或檢測是否符合完整需求的測試安裝。

本指南包含下列內容：

支援與一般任務

SUSE Linux Enterprise 提供範圍廣泛的工具，可針對系統的各個方面進行自定。這個部分介紹其中幾項。為了讓管理員對系統有初步的瞭解，本指南分析了可用的設備技術、高度可用性的組態和進階的管理可能性。

系統

學習這部份，進一步瞭解作業系統基礎。SUSE Linux Enterprise 支援多種硬體結構，您可以此自行打造可執行於 SUSE Linux Enterprise 上的應用程式。開機載入程式和開機程序資訊會協助您瞭解 Linux 系統的運作方式，以及您個人的自定程序檔和應用程式如何與作業系統融合。

行動電腦

需要特別注意筆記型電腦以及行動設備 (例如 PDA 或行動電話與 SUSE Linux Enterprise) 之間的通訊。請注意省電，並留心不同設備與不斷變化的網路環境的整合。另外，請瞭解提供所需功能的背景技術。

服務

SUSE Linux Enterprise 的設計目的是要做為網路作業系統。它提供範圍廣泛的網路服務 (如 DNS、DHCP、網頁、代理和驗證服務)，並充分整合到異質的環境中，包括 MS Windows 用戶端和伺服器。

疑難排解

提供一份綜覽，指出當您需要更多資訊或要對系統執行特定任務時可在何處尋找說明和其他文件。另外還編纂了一份常見問題和故障列表，供您瞭解如何自行解決這些問題。

本手冊的許多章節包含連到其他文件資源的連結。這包括系統和網際網路上所提供的其他文件。

如需適用於產品的文件與最新文件更新的綜覽，請參閱 <http://www.suse.com/doc>。

1 可用文件

我們提供不同語言的 HTML 和 PDF 版本的書籍。下列使用者和管理員手冊適用於本產品：

部署指南 (↑部署指南)

顯示如何安裝單個或多個系統，以及如何利用產品內在功能部署基礎結構。從本地安裝或使用網路安裝伺服器，到使用遠端控制、高度自訂及自動安裝技術進行大量部署，有各式各樣的做法供您選擇。

管理指南 [i頁]

描述系統管理任務，如維護、監控及自定初始安裝的系統。

Security Guide (↑Security Guide)

介紹系統安全性的基本概念，涵蓋了本地安全性與網路安全性方面。顯示如何利用產品內含的 AppArmor 等安全性軟體 (可讓您根據程式指定該程式可能會讀取、寫入及執行的檔案) 以及可以可靠地收集關於所有安全性相關事件資訊的稽核系統。

Security and Hardening Guide (↑Security and Hardening Guide)

說明安裝和設定安全 SUSE Linux Enterprise Server 的詳情，以及進一步保護和強化該安裝所需的其他安裝後程序。為管理員提供安全性相關的選項和決策。

系統分析與調整指南 (↑系統分析與調整指南)

用於偵測、解決及最佳化問題的管理員指南。其中描述了如何透過監控工具檢查並最佳化系統，以及如何有效管理資源。該指南還概述了常見問題與解決方案，以及其他說明與文件資源。

Virtualization with Xen (↑Virtualization with Xen)

介紹了產品的的虛擬化技術。它提供各種應用程式和每個 SUSE Linux Enterprise Server 支援平台的安裝類型概觀，以及安裝程序的簡短說明。

Virtualization with KVM for IBM System z (↑*Virtualization with KVM for IBM System z*)

介紹如何在 SUSE Linux Enterprise Server 上使用 KVM (基於核心的虛擬機器) 設定和管理虛擬化。瞭解如何使用 libvirt 或 QEMU 管理 KVM。本指南還包含有關要求、限制和支援情況的詳細資訊。

AutoYaST (↑*AutoYaST*)

AutoYaST 這套系統可借助包含安裝和組態資料的 AutoYaST 設定檔，在不需要使用者介入的情況下自動安裝一或多個 SUSE Linux Enterprise 系統。該手冊會指引您完成自動安裝的基本步驟：準備、安裝及設定。

儲存管理指南 (↑*儲存管理指南*)

提供關於如何管理 SUSE Linux Enterprise Server 上之儲存設備的資訊。

除綜合性手冊外，還提供了以下幾個快速入門指南：

安裝快速入門 (↑*安裝快速入門*)

列出系統要求，並提供透過 DVD 或 ISO 影像安裝 SUSE Linux Enterprise Server 的逐步指南。

Linux Audit 快速入門

簡要說明如何啟用和設定稽核系統，以及如何執行關鍵任務，例如設定稽核規則、產生報告和分析記錄檔案等。

AppArmor 快速入門

可幫助您理解 AppArmor® 背後的主要概念。

Virtualization with Linux Containers (LXC) (↑*Virtualization with Linux Containers (LXC)*)

提供 LXC (一種精簡的「虛擬化」方法) 的簡介，並展示如何設定 LXC 主機和 LXC 容器。

大部分產品手冊的 HTML 版本位於所安裝系統的 `/usr/share/doc/manual` 目錄下，或桌面系統的說明中心中。<http://www.suse.com/doc> 中提供了最新的文件更新，您可於此處下載 PDF 或 HTML 版本的產品手冊。

2 意見反應

以下為可供使用的數種意見回應管道：

錯誤與增強功能要求

如需產品適用的服務與支援選項，請參閱 <http://www.suse.com/support/>。

若要報告產品元件的錯誤，請登入 Novell Customer Center (<http://www.suse.com/support/>)，然後選取「我的支援」>「服務要求」。

使用者意見

我們希望得到您對本手冊以及本產品隨附之其他文件的意見和建議。請使用線上文件每頁底部的「使用者備註」功能，或造訪 <http://www.suse.com/doc/feedback.html> 在其中輸入您的意見。

郵件

如需本產品文件的回饋，您還可以傳送郵件至 doc-team@suse.de。請務必包含文件標題、產品版本以及文件發行日期。若要報告錯誤或對增強功能提出建議，請提供問題的簡短描述，並指出對應的章節編號及頁碼(或URL)。

3 文件慣例

本手冊使用下列印刷慣例：

- `/etc/passwd`：目錄名稱與檔名
- `placeholder`：以實際的值來取代 `placeholder`
- `PATH`：環境變數 `PATH`
- `ls`、`--help`：指令、選項和參數
- `user`：使用者或群組
- `Alt`、`Alt + F1`：供人按下的按鍵或案件組合；顯示的按鍵與鍵盤上一樣為大寫
- 「檔案」、「檔案」>「另存新檔」：功能表項目、按鈕
- ► **amd64 em64t ipf**：本段落內容僅與 `amd64`、`em64t` 及 `ipf` 架構相關。箭頭標示了文字區塊的開頭與結尾。 ◀

► **ipseries zseries:** 本段落內容僅與 System z 及 ipseries 架構相關。箭頭標示了文字區塊的開頭與結尾。 ◀

- *Dancing Penguins* (章節 *Penguins*, ↑其他手冊): 這是對其他手冊某章節的參考。

I. 支援與一般任務

YaST 線上更新

Novell 為您的產品提供持續的軟體安全性更新。依預設，更新 Applet 可以讓您的系統保持最新狀態。如需有關更新 Applet 的詳細資訊，請參閱第 9.4 節「使系統保持最新」(第 9 章「安裝或移除軟體」, ↑部署指南)。本章介紹了用於更新軟體套件的替代工具：YaST 線上更新。

SUSE® Linux Enterprise Server 的最新修補程式可從更新軟體儲存庫取得。如果在安裝期間已註冊了產品，則表明已設定更新儲存庫。如果未註冊 SUSE Linux Enterprise Server，則可以按照以下方式進行註冊：在 YaST 中執行「軟體」>「線上更新組態」，然後啟動「進階」>「註冊以獲得支援，並獲得更新儲存庫」。或者，您可以從信任的來源手動新增更新儲存庫。若要新增或移除儲存庫，請透過 YaST 中的「軟體」>「軟體儲存庫」啟動儲存庫管理員。第 9.3 節「管理軟體儲存庫與服務」(第 9 章「安裝或移除軟體」, ↑部署指南) 中提供了有關儲存庫管理員的詳細資訊。

注意：存取更新目錄時發生錯誤

如果您無法存取更新目錄，可能表示訂閱已過期。SUSE Linux Enterprise Server 通常提供一年或三年的訂閱，您可以在這個時間段內存取更新目錄。一旦訂閱期結束，此存取權將被拒絕。

存取更新目錄遭拒絕時，系統會顯示一則警告訊息，建議您造訪 Novell Customer Center 以查看您的訂閱。可在 <http://www.novell.com/center/> 上找到 Novell Customer Center。

Novell 提供了具有不同關聯層級的更新：

安全性更新
修復嚴重的安全性問題，必須予以安裝。

推薦性更新
修復可能會破壞電腦的問題。

選擇性更新
修復與安全性無關的問題或提供增強功能。

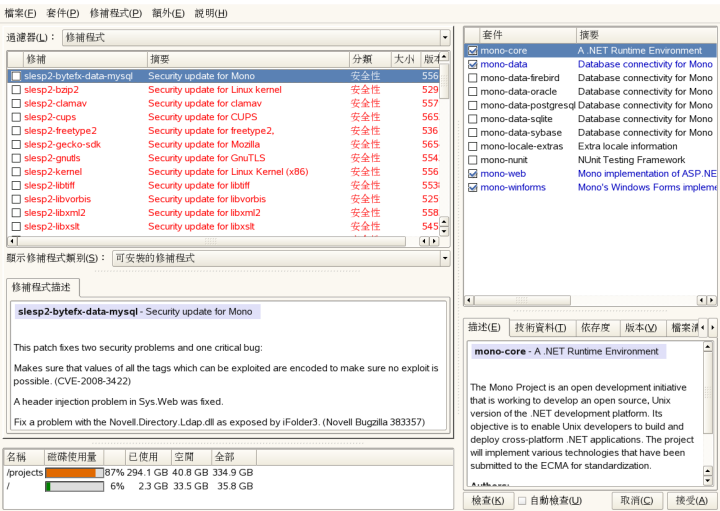
1.1 線上更新對話方塊

以下兩種類別的工具套件中包含 YaST 的「線上更新」對話方塊：GTK (適用於 GNOME) 和 Qt (適用於 KDE)。這兩種介面的外觀與感覺有所不同，但提供的功能基本相同。以下幾節將簡單介紹每一種介面。若要開啟對話方塊，請啟動 YaST，然後選取「軟體」>「線上更新」。或者，也可以在指令行中使用 `yast2 online_update` 指令進行啟動。

1.1.1 KDE 介面 (Qt)

「線上更新」視窗包含四個區段。

圖形 1.1 YaST 線上更新 - Qt 介面



左側的「摘要」區段列出了 SUSE Linux Enterprise Server 可用的修補程式。修補程式根據安全性關聯程度 (安全性、建議和選擇性) 進行排序。您可以從「顯示修補程式類別」中選取以下其中一個選項，以變更「摘要」區段的檢視窗：

「需要的修補程式」(預設檢視窗)

適用於系統上安裝的套件，但尚未安裝的修補程式。

「不需要的修補程式」

適用於系統上未安裝之套件的修補程式，或已滿足其執行要求的修補程式 (相關套件已從其他來源進行更新)。

「所有修補程式」

可用於 SUSE Linux Enterprise Server 的所有修補程式。

「摘要」區段中的每個清單項目包含一個符號和修補程式名稱。有關可用符號及其含義的綜覽，請按 **Shift + F1**。「安全性」和「建議」狀態的修補程式所要求的動作已自動預設。這些動作包括「自動安裝」、「自動更新」和「自動刪除」。

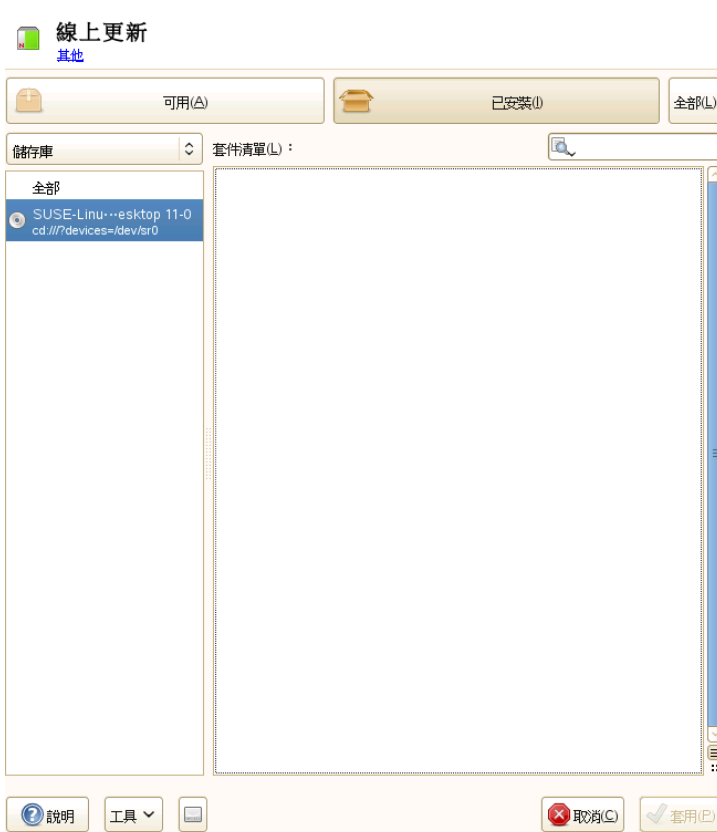
如果從更新儲存庫以外的其他儲存庫安裝最新的套件，則可以使用此安裝來滿足此套件之修補程式的需求。在此情況下，會有一個核取標記顯示在修補程式摘要的前面。僅當您將修補程式標示為已安裝時，該修補程式才會顯示在清單中。事實上這並沒有安裝修補程式 (因為套件已經是最新的)，而是將修補程式標示為已安裝。

在「摘要」區段中選取一個項目，可在對話方塊的左下角看到簡短的「修補程式描述」。右上方的區段列出了所選修補程式中包含的套件 (一個修補程式可以包含多個套件)。按一下右上方區段中的項目，可檢視修補程式中包含的各套件的詳細資料。

1.1.2 GNOME 介面 (GTK)

「線上更新」視窗包含四個主要區段。

圖形 1.2 YaST 線上更新 - GTK 介面



右上方的區段中列出了 SUSE Linux Enterprise Server 可用的 (或已安裝的) 修補程式。若要根據修補程式的安全性關聯程度 (安全性、建議、選擇性或所有修補程式) 對其進行過濾，請按一下視窗左上方區段中的「優先程度」項目。

如果所有可用的修補程式均已安裝，則右上方區段的「套件清單」將不顯示任何項目。左下方區段中的方塊顯示可用修補程式和已安裝修補程式的數目，並允許您將檢視窗切換至「可用」或「已安裝」修補程式。

在「套件清單」區段中選取一個項目，可在對話方塊的右下角看到修補程式描述及其他詳細資料。由於修補程式可能包含多個套件，按一下右下方區段中的「套用至」項目，可查看各修補程式中所包含的套件。

按一下修補程式項目可開啟詳細描述視窗底部修補程式的資訊列。此處可檢視修補程式的詳細描述及可用版本。您也可以選擇「安裝」選擇性修補程式—系統已預先選取安全性與推薦的修補程式以進行安裝。

1.2 安裝修補程式

YaST 的「線上更新」對話方塊可讓您同時安裝所有可用的修補程式，或者手動選取要套用至系統的修補程式。您還可以回復已套用至系統的修補程式。

依預設，目前您系統可用的所有新修補程式 (選擇性修補程式除外) 均已標示為即將安裝。按一下「接受」或「套用」後，這些修補程式將自動套用。

過程 1.1 使用 YaST 線上更新套用修補程式

- 1 啟動 YaST，然後選取「軟體」>「線上更新」。
- 2 若要自動套用目前您系統可用的所有新修補程式 (選擇性修補程式除外)，請接著按「套用」或「接受」，開始安裝預先選取的修補程式。
- 3 若要先對已選擇進行套用的修補程式範圍進行修改：
 - 3a 使用 GTK 和 Qt 介面提供的各種過濾器 and 檢視窗。如需詳細資訊，請參閱第 1.1.1 節「KDE 介面 (Qt)」[4 頁] 和第 1.1.2 節「GNOME 介面 (GTK)」[5 頁]。
 - 3b 根據您的需求和意願選取或取消選取修補程式，方法是啟用或停用相應的核取方塊 (GNOME)，或者在修補程式上按一下滑鼠右鍵，然後從內容功能表 (KDE) 中選擇相應的動作。

重要：始終套用安全性更新

不過，如果沒有非常充分的理由，請不要取消選取任何與安全性相關的修補程式。因為這些修補程式可以修復嚴重的安全性問題，並防止系統被入侵。

- 3c 大部分的修補程式都會包含多套件的更新。若要變更對單一套件所執行的動作，請在套件檢視窗中的套件上按一下滑鼠右鍵，然後選擇一個動作 (KDE)。

3d 若要確認您的選擇並套用所選修補程式，請接著按一下「套用」或「接受」。

- 4** 安裝完成後，請按一下「完成」離開 YaST 「線上更新」。您的系統現在已是最新狀態。

提示：禁用 `deltarpm`

依預設更新將做為 `deltarpm` 下載。由於從 `deltarpm` 重建 `rpm` 套件需要佔用大量的記憶體和 CPU 時間，出於效能考量，某些設定或硬體組態可能要求您停用 `deltarpm`。

若要禁用 `deltarpm`，請編輯檔案 `/etc/zypp/zypp.conf`，並將 `download.use_deltarpm` 設定為 `false`。

1.3 自動線上更新

YaST 還可以設定於每日、每週或每月執行的自動更新。若要使用相應的模組，您需要先安裝 `yast2-online-update-configuration` 套件。

過程 1.2 設定自動線上更新

- 1** 安裝後，啟動 YaST 並選取「軟體」>「線上更新組態」。

您也可以在指令行中使用 `yast2 online_update_configuration` 指令啟動模組。

- 2** 啟用「自動線上更新」。
- 3** 選擇是否執行「每日」、「每週」或「每月」更新。

某些修補程式 (例如核心更新或需要授權合約的套件) 需要使用者互動，而這可能會讓自動更新程序停止下來。

- 4** 如果您要更新程序繼續以完全自動化的方式執行，可以選取「跳過互動式修補程式」。

重要：跳過修補程式

如果您選擇跳過需要互動的所有套件，請經常執行手動「線上更新」，以便這些修補程式也能予以安裝。否則，您可能會錯過部分重要的修補程式。

- 5 若要自動接受所有授權合約，請啟用「*同意授權*」。
- 6 若要自動安裝已更新套件推薦的所有套件，請啟用「*包含推薦的套件*」。
- 7 若要根據類別 (例如安全性或推薦) 過濾修補程式，請啟用「*根據類別過濾*」並新增清單中的相應修補程式類別。系統將會只安裝所選類別的修補程式，跳過其他類別。
- 8 按一下「*確定*」確認您的組態。

收集系統資訊以供支援所用

如果發生問題，會使用 `supportconfig` 指令建立一份系統報告。此工具將收集系統的相關資訊，例如目前的核心版本、硬體、已安裝的套件、分割區設定等。此報告將幫助 Novell 技術服務找出您所報告的問題或提供協助。該指令由預設安裝的套件 `supportutils` 提供。

2.1 綜覽

Novell 支援連結 (NSL) 是 SUSE Linux Enterprise Server 的新功能，此工具會收集系統資訊，並可讓您將所收集的資料上載到其他伺服器以進行進一步分析。

有兩種方式可以使用 Novell 支援連結：

1. 使用 YaST 支援模組。
2. 使用指令行公用程式 `supportconfig`。

YaST 支援模組會呼叫 `supportconfig` 來收集系統資訊。

2.2 使用 `Supportconfig` 收集資訊

以下幾節描述如何透過 YaST 或指令行使用 `supportconfig`，以及您可以使用的其他選項。

2.2.1 使用 YaST

要使用 YaST 收集系統資訊，請執行下列步驟：

- 1 開啟 URL <http://www.novell.com/center/eservice>，然後建立服務要求號碼。
- 2 啟動 YaST。
- 3 開啟「支援」模組。
- 4 按一下「建立報告 *Tar* 聚合檔」。
- 5 從選項按鈕清單中選取選項。如果要先進行測試，請使用「僅收集最少量的資訊」。按「下一步」繼續。
- 6 輸入您的聯絡人資訊。使用來自 步驟 1 [12頁] 的服務要求號碼，將其輸入到標示為「Novell 11 位數服務要求號碼」的文字欄位中。按「下一步」繼續。
- 7 系統即開始收集資訊。該程序完成後，按「下一步」繼續。
- 8 檢閱資料收集。按「下一步」繼續。
- 9 儲存 *Tar* 聚合檔。如果要上載至 Novell Customer Center，請確定啟用「將記錄檔案 *Tar* 聚合檔上載至 URL」。按「下一步」完成操作。

2.2.2 直接使用 Supportconfig

若要在指令行中使用 supportconfig，請執行下列步驟：

- 1 開啟外圍程序，切換為 root 身分。
- 2 執行 supportconfig，且不使用任何選項。此操作會收集預設的系統資訊。
- 3 等待工具完成操作。
- 4 預設歸檔位於 /var/log 中，檔案名稱格式為 `nts_主機_日期_時間.tbz`

2.2.3 Supportconfig 通用選項

呼叫 `supportconfig` 公用程式時通常不會顯示任何選項。請使用 `supportconfig --help` 顯示所有選項的清單，或參閱 `man` 頁面。下面的清單簡要概述了一些較為常見的情況：

- 使用精簡選項 (`-m`) 可以縮小所收集之資訊的大小：

```
supportconfig -m
```

- 在輸出中包含其他聯絡人資訊 (全部在一行上)：

```
supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

- 進行疑難排解時，您可能只想收集目前要解決之問題所在區域的資訊。例如，如果 LVM 有問題，且您是在最近使用預設 `supportconfig` 輸出時發現的該問題。在對其進行變更之後，您希望收集目前的 LVM 資訊。以下指令僅收集最精簡的 `supportconfig` 資訊與 LVM。

```
supportconfig -i LVM
```

要檢視完整的功能清單，請執行：

```
supportconfig -F
```

如果您需要相對區域，請使用 `-x` 排除區域。選項 `-i` 和 `-x` 可以結合使用。

- 收集已輪替的記錄檔案。這對記錄量大的環境或在重新開機後 `syslog` 輪替記錄時核心發生當機之後的情況特別有用。

```
supportconfig -l
```

2.3 向 Novell 提交資訊

可以使用 YaST 支援模組或 `supportconfig` 指令行公用程式向 Novell 提交系統資訊。當您遇到伺服器問題，希望獲取 Novell 的協助時，您將需要開啟服務要求並向 Novell 提交您的伺服器資訊。下文將描述使用 YaST 與指令行這兩種方法。

注意：隱私權聲明

Novell 將系統報告視為機密資料。請參閱我們的隱私權承諾以瞭解詳細資料，網址為：<http://www.novell.com/company/legal/privacy/>。

過程 2.1 使用 YaST 向 Novell 提交資訊

- 1 開啟 URL <http://www.novell.com/center/eservice>，然後建立服務要求號碼。
 - 2 記下您的 11 位數服務要求號碼。以下範例假設服務要求號碼為 12345678901。
 - 3 在 YaST 的支援模組視窗中按一下「建立報告 Tar 聚合檔」。
 - 4 選取「使用自定」選項圓鈕。按「下一步」繼續。
 - 5 輸入聯絡人資訊，填寫「Novell 11 位數服務要求號碼」及 Novell 的上載目標 URL。
 - 對於安全上載目標，請使用：<https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}>。
 - 對於一般 FTP 上載目標，請使用 <ftp://ftp.novell.com/incoming> (美國客戶) 或 <ftp://support-ftp.suse.com/in> (EMEA，即歐洲、中東和非洲客戶)。
- 按「下一步」繼續。系統即開始收集資訊。該程序完成後，按「下一步」繼續。
- 6 檢閱資料集合，並使用「從資料移除」移除任何您不想上載到 Novell 之 Tar 聚合檔的檔案。按「下一步」繼續。
 - 7 依預設，/root 中會儲存一份 Tar 聚合檔的副本。確認您使用的是上文描述的其中一個 Novell 上載目標，並且「將記錄檔案 Tar 聚合檔上載至 URL」已啟用。按「下一步」完成操作。
 - 8 按一下「完成」。

過程 2.2 使用 *supportconfig* 將資訊提交至 Novell

- 1 開啟 URL <http://www.novell.com/center/eservice>，然後建立服務要求號碼。
- 2 記下您的 11 位數服務要求號碼。以下範例假設服務要求號碼為 12345678901。
- 3 伺服器連接至網際網路：

3a 要使用預設上載目標，請執行：

```
supportconfig -ur 12345678901
```

3b 對於安全上載目標，請在同一行上使用以下指令：

```
supportconfig -r 12345678901 -U  
'https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}'
```

- 4 伺服器未連接至網際網路

4a 執行以下指令：

```
supportconfig -r 12345678901
```

4b 將 `/var/log/nts_SR12345678901*tbz` Tar 聚合檔手動上載到 FTP 伺服器 (美國客戶請使用 <ftp://ftp.novell.com/incoming>；歐洲、中東和非洲客戶請使用 <ftp://support-ftp.suse.com/in>)。

4c 也可以使用服務要求 URL <http://www.novell.com/center/eservice>，將 Tar 聚合檔附加至服務要求。

- 5 Tar 聚合檔一旦位於 FTP 伺服器的內送目錄，便會自動附加到服務申請中。

2.4 如需更多資訊

下列文件提供了關於收集系統資訊的詳細資訊：

- `man supportconfig` — `supportconfig` 的 `man` 頁面

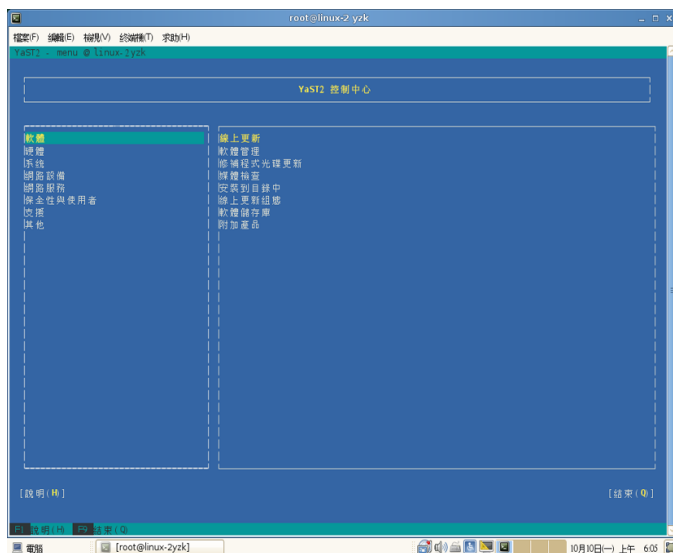
- `man supportconfig.conf` — `supportconfig` 組態檔案的 `man` 頁面
- <http://www.novell.com/communities/print/node/4097> — 使用 `Supportconfig` 進行基本伺服器狀態檢查
- <http://www.novell.com/communities/print/node/4827> — 建立自己的 `Supportconfig` 外掛程式
- <http://www.novell.com/communities/print/node/4800> — 建立中心 `Supportconfig` 儲存庫

文字模式的 YaST

本章節對象為未在其系統上執行 X 伺服器，且依賴以文字為基礎的安裝工具的系統管理員及進階使用者。這裡提供了一些基本資訊，說明如何在文字模式中啟動與操作 YaST。

文字模式下的 YaST 使用 ncurses 程式庫來提供簡單的虛擬圖形使用者介面。依預設，ncurses 程式庫已安裝。若要執行 YaST，終端模擬器的大小不能小於 80x25 個字元。

圖形 3.1 文字模式下的 YaST 主視窗



在文字模式中啟動 YaST 時，會顯示 YaST 控制中心 (請參閱圖形 3.1)。主要視窗包含 3 個區域。左框架內包含各種模組所屬的類別。此框架在 YaST 啟動時處於使用中狀態，因此會以白色的粗框線標示。作用中的類別會反白顯示。右框架內包含作用中類別可以使用的各個模組的綜覽。下方框架中有「說明」按鈕與「結束」按鈕。

啟動 YaST 控制中心時，會自動選取「軟體」類別。您可以使用 ↓ 與 ↑ 來變更類別。若要從類別中選取模組，可以使用 → 啟動右框架，然後使用 ↓ 和 ↑ 選取模組。您可以按住方向鍵不放來捲動可用模組清單。選取的模組會反白顯示。按 Enter 可以啟動作用中的模組。

模組中的各個按鈕或選項欄位中，都有一個反白顯示的字母 (預設為黃色)。您可以使用 Alt + 反白的字母直接選取按鈕，而不必再使用 Tab 導覽至該處。按 Alt + Q 或選取「結束」並按 Enter 來結束 YaST 控制中心。

提示：重新整理 YaST 對話視窗

如果 YaST 對話視窗遭毀損或破壞 (例如在調整視窗大小時)，請按 Ctrl + L 重新整理並還原其內容。

3.1 在模組中瀏覽

以下對 YaST 模組的控制元件做出說明，假設所有的功能鍵及 Alt 組合鍵都起作用，且未被指定不同的全域功能。如需有關可能的例外狀況的資訊，請參閱第 3.2 節「組合鍵的限制」[20 頁]。

在按鈕與選項清單中瀏覽

使用 Tab 可以在按鈕與包含選項清單的框架之間進行瀏覽。若要反向瀏覽，請使用 Alt + Tab 組合或 Shift + Tab 組合。

在選項清單中瀏覽

在作用中且包含選項清單的框架中，您可以使用方向鍵 (↑ 和 ↓) 以便在其中的個別元件之間進行瀏覽。如果框架中個別項目超出其寬度，您可以使用 Shift + → 或 Shift + ← 以水平方式向右及向左捲動。或者使用 Ctrl + E 或 Ctrl + A。如果使用 → 或 ← 導致作用中的框架或目前的選項清單發生變更 (如同在控制中心內)，您也可以使用此組合鍵。

按鈕、圓形按鈕以及核取方塊

如果要選取有空白方括號 (核取方塊) 的按鈕，或是有空白括號 (選項圓鈕) 的按鈕，請按空格鍵或 Enter 鍵。或者，也可以使用 Alt + 反白的字母選取選項圓鈕與核取方塊。在此狀況中，您不需按 Enter 來做確認。如果您使用 Tab 瀏覽至某個項目，按 Enter 即可執行所選取的動作或啟用個別的功能表項目。

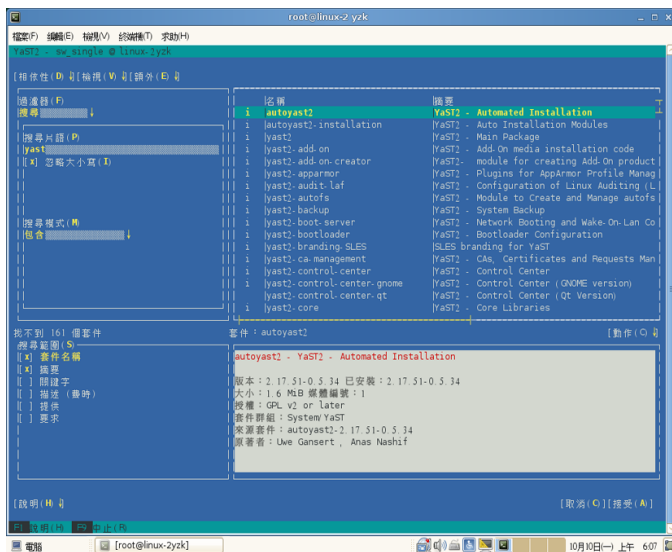
功能鍵

F 鍵 (F1 到 F12) 可用來快速存取不同的按鈕。可用的 F 鍵捷徑顯示在 YaST 螢幕的結算底線中。因為不同的模組提供不同的按鈕 (詳細資料、資訊、新增、刪除等等)，所以各個功能鍵實際對應的按鈕視作用中的 YaST 模組而有所不同。您可以將 F10 當作「接受」、「確定」、「下一步」以及「完成」來使用。按 F1 可存取 YaST 說明。

在 ncurses 模式中使用導覽樹狀結構

某些 YaST 模組使用視窗左側的導覽樹狀結構來選取組態對話方塊。使用方向鍵 (↑ 和 ↓) 可以在樹狀結構中進行導覽。使用空格鍵可以開啟或關閉樹狀結構中的項目。在 ncurses 模式下，從導覽樹狀結構中進行選取後，必須按 Enter 才能顯示選取的對話方塊。這樣做的目的是為了在導覽樹狀結構時省去費時的重新描繪程序。

圖形 3.2 軟體安裝模組



3.2 組合鍵的限制

如果您的視窗管理員使用了全部的 **Alt** 組合，則 **YaST** 中的 **Alt** 組合可能無效。像是 **Alt** 或 **Shift** 等鍵也可能事先已由終端機的設定所佔用。

以 **Esc** 取代 **Alt**

您可以使用 **Esc** 來取代 **Alt**，而不使用 **Alt**。例如，**Esc-H** 可取代 **Alt + H**。(先按 **Esc**，然後按 **H**。)

您可以使用 **Ctrl + F** 與 **Ctrl + B** 來往前瀏覽和往後瀏覽

如果 **Alt** 和 **Shift** 組合已先由視窗管理員或終端機所佔用，則請使用 **Ctrl + F** 組合 (往前) 與 **Ctrl + B** 組合 (往後) 來代替。

功能鍵的限制

有些功能會使用 **F** 鍵。有些特定的功能鍵可能已由終端機所佔用，無法供 **YaST** 使用。不過，在純文字主控台中，應該都可以使用各種的 **Alt** 組合鍵與功能鍵。

3.3 YaST 指令行選項

除文字模式介面之外，**YaST** 還提供了純指令行介面。若要取得 **YaST** 指令行選項的清單，請輸入：

```
yast -h
```

3.3.1 啟動個別模組

如果要節省時間，您可以直接啟動個別的 **YaST** 模組。若要啟動模組，請輸入：

```
yast <module_name>
```

使用 `yast -l` 或 `yast --list`，則可以檢視一個清單，其中包含您系統中所有可用的模組名稱。例如，使用 `yast lan` 可啟動網路模組。

3.3.2 透過指令行安裝套件

如果您知道套件名稱，並且此套件是由某個使用中的安裝儲存庫所提供，則可以使用指令行選項 `-i` 來安裝套件：

```
yast -i <package_name>
```

或

```
yast --install <package_name>
```

套件名稱可以是單個套件的簡短名稱，例如 `gvim` (安裝時會進行相依性檢查)，也可以是 `rpm` 套件的完整路徑 (安裝時不進行相依性檢查)。

如果您需要以指令行為基礎的軟體管理公用程式以及 YaST 無法提供的功能，可以考慮使用 `zypper`。這個新的公用程式使用相同的軟體管理程式庫，此程式庫也是 YaST 套件管理員的基礎。第 6.1 節「使用 Zypper」[47頁] 中介紹了 `zypper` 的基本用法。

3.3.3 YaST 模組的指令行參數

為使用程序檔中的 YaST 功能，YaST 提供了可支援個別模組的指令行。並不是所有模組都有指令行支援。若要顯示某模組的可用選項，請輸入：

```
yast <module_name> help
```

如果某模組未提供指令行支援，則此模組將在文字模式中啟動，並且系統會顯示以下訊息：

```
This YaST module does not support the command line interface.
```


使用 Snapper 執行快照/復原

在 Linux 上建立檔案系統快照以執行復原的功能是過去使用者常常要求的一項功能。現在，Snapper 與 Btrfs 檔案系統或簡易佈建的 LVM 磁碟區合用，填補了這個空白。

Btrfs 是一個適用於 Linux 的全新寫時複製檔案系統，它支援子磁碟區 (每個實體分割區中的一或多個可獨立掛接的檔案系統) 的檔案系統快照 (子磁碟區於特定時間點之狀態的副本)。Snapper 可讓您管理這些快照。Snapper 包含一個指令行和一個 YaST 介面。

依預設，SUSE Linux Enterprise Server 上的 Snapper 與 Btrfs 設為用作 YaST 與 zypper 所執行之系統變更的「復原工具」。在執行 YaST 模組或 zypper 的前後，系統會分別建立一個快照。Snapper 可讓您比較這兩個快照，並提供回復這兩個快照之間的差異的方法。這些工具還提供系統備份，方法是建立系統子磁碟區的每小時快照。

4.1 要求

由於 Btrfs 是 SUSE Linux Enterprise Server 上唯一一個支援快照的檔案系統，因此要「建立快照」的所有分割區或子磁碟區上都需要它。

4.1.1 快照與磁碟空間

建立快照時，快照和原件都會指向檔案系統中的同一區塊。因此，快照最初並不佔用額外的磁碟空間。如果原始檔案系統中的資料經過修改，則會複製變更

後的資料區塊，同時保留快照的舊資料區塊。因此，快照便會佔用與已修改資料相同的空間。這樣，經過一段時間之後，快照配置的空間不斷增大。因而，從包含快照的 Btrfs 檔案系統刪除檔案可能無法釋放磁碟空間！

注意：快照位置

快照永遠位於「已建立快照」的同一分割區或子磁碟區上，而無法儲存到其他分割區或子磁碟區上。

因此，包含快照的分割區必須比「一般」分割區更大。確切大小很大程度上取決於保留的快照數和資料修改量。一般來說，您應該考慮使用比平常大兩倍的大小。

提示：釋放空間/磁碟使用量

為了釋放包含快照之 Btrfs 分割區上的空間，您需要刪除不需要的快照，而不是檔案。與新快照相比，較舊的快照佔用的空間更多。

由於 `df` 無法正確顯示 Btrfs 檔案系統上的磁碟使用量，因此您需要使用指令 `btrfs filesystem df 掛接點`。目前，Btrfs 工具無法顯示快照配置的磁碟空間量。

從一個 Service Pack 升級到另一個 Service Pack 會導致快照佔用系統子磁碟區上的大量磁碟空間，這是因為有許多資料進行了變更 (套件更新)。一旦快照不再需要，建議您手動刪除它們。

Snapper 還可用於在格式為 ext3 或 XFS 之簡易佈建的 LVM 磁碟區上建立和管理快照 (請參閱第 4.6 節「對簡易佈建的 LVM 磁碟區使用 Snapper」[40頁])。

4.2 使用 Snapper 復原系統變更

SUSE Linux Enterprise Server 上的 Snapper 已預先設定為用作供您復原 zypper 和 YaST 所執行之變更的工具。為此，Snapper 設定為在每次執行 zypper 和 YaST 的前後建立一對快照。此外，Snapper 還可讓您還原遭意外刪除或修改的系統檔案。對此會建立每小時備份。

預設會為根分割區及其子磁碟區設定上述的自動快照。為了讓這些快照可供其他分割區 (例如 /home) 使用，您可以建立自定組態。

4.2.1 復原 YaST 和 zypper 變更

如果您在安裝期間使用 `Btrfs` 設定根分割區，系統將會自動安裝 **Snapper** (已預先設定用於復原 YaST 或 zypper 的變更)。每當您啟動 YaST 模組或 zypper 交易時，都會建立兩個快照：啟動模組之前會建立用於擷取檔案系統狀態的「前快照」；完成模組之後會建立「後快照」。

利用 YaST **Snapper** 模組或 `snapper` 指令行工具，您可以透過從「前快照」還原檔案來復原 YaST/zypper 所執行的變更。比較兩個快照時，這些工具還可讓您查看哪些檔案已經過變更。此外，您還可以顯示某檔案的兩個版本之間的差異 (diff)。

由於 Linux 是一個多工作業系統，因此 YaST 或 zypper 以外的其他程序可以在前快照與後快照之間的時間範圍內修改資料。若是如此，完全回復為前快照還將會復原其他程序執行的變更。在大多數情況下，並不希望發生這種情況—因此，強烈建議您在啟動復原之前，先仔細檢閱這兩個快照之間的變更。如果有其他程序的變更要保留，請選取要復原的檔案。

重要：限制

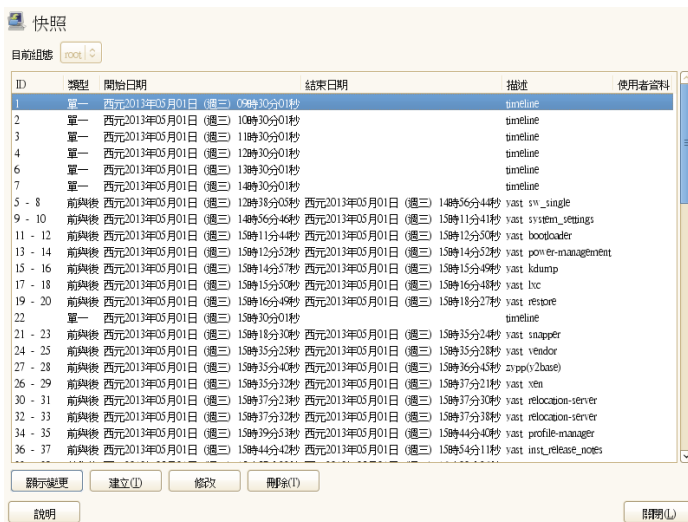
請確定在嘗試使用 **Snapper** 的復原機制之前，您知悉 **Snapper** 的局限性。如需詳細資料，請參閱第 4.4 節「限制」[38頁]。

注意：快照的儲存時間

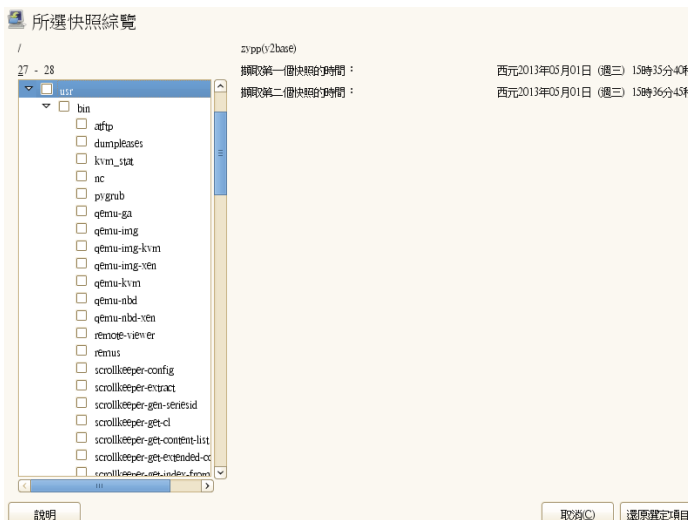
依預設，系統會保留最後 100 個 YaST 和 zypper 快照。如果超出此數目，系統將會刪除最舊的快照。

過程 4.1 使用 YaST 「*Snapper*」 模組復原變更

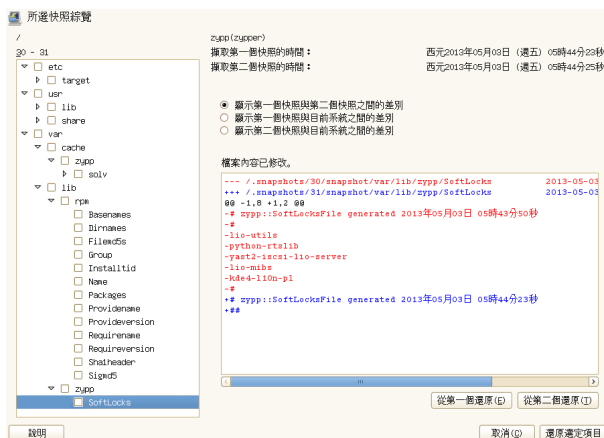
- 1 從 YaST 的「其他」區段或透過輸入 `yast2 snapper` 啟動「*Snapper*」模組。
- 2 請確定「目前組態」設為「根」。除非您手動新增了自己的 **Snapper** 組態，否則應始終如此設定。
- 3 從清單中選擇一對前快照和後快照。YaST 與 zypper 快照對的類型均屬「前與後」。在「描述」欄中，YaST 快照標示為 `yast 模組名稱`；zypper 快照則標示為 `zypp (zypper)`。



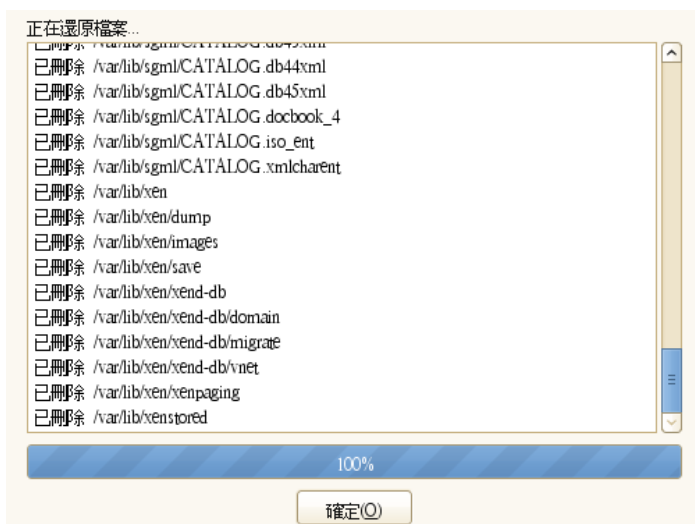
- 4 按一下「顯示變更」以開啟兩個快照之間不同的檔案清單。下列影像顯示了新增使用者 tester 之後已變更的檔案清單。



- 5 檢閱檔案清單。若要顯示檔案的前版本與後版本之間的「差異」，請從清單中選取它。下列影像顯示了新增使用者 `tester` 之後對 `/etc/passwd` 的變更。



- 6 若要還原一組檔案，請勾選相應的核取方塊來選取相關的檔案或目錄。按一下「還原選定項目」，然後按一下「是」確認該動作。



若要還原單個檔案，請按一下其名稱以啟動差異比對檢視。按一下「從第一個還原」，然後按一下「是」確認您的選擇。

過程 4.2 使用 *snapper* 指令復原變更

- 1 執行 `snapper list -t pre-post` 取得 YaST 與 zypper 快照的清單。在「描述」欄中，YaST 快照標示為 `yast` 模組名稱；zypper 快照則標示為 `zypp (zypper)`。

```
~ # snapper list -t pre-post
  Pre # | Post # | Pre Date                  | Post Date                  | Description
-----+-----+-----+-----+-----+
    4   |    5   | Tue Jan 10 14:39:14 2012 | Tue Jan 10 14:39:33 2012 | yast system_settings
    65   |   66   | Thu Jan 12 17:18:10 2012 | Thu Jan 12 17:18:23 2012 | zypp(zypper)
    68   |   69   | Thu Jan 12 17:25:46 2012 | Thu Jan 12 17:27:09 2012 | zypp(zypper)
    73   |   74   | Thu Jan 12 17:32:55 2012 | Thu Jan 12 17:33:13 2012 | yast system_settings
    75   |   76   | Thu Jan 12 17:33:56 2012 | Thu Jan 12 17:34:42 2012 | yast users
    77   |   92   | Thu Jan 12 17:38:36 2012 | Thu Jan 12 23:13:13 2012 | yast snapper
    83   |   84   | Thu Jan 12 22:10:33 2012 | Thu Jan 12 22:10:39 2012 | zypp(zypper)
    85   |   86   | Thu Jan 12 22:16:58 2012 | Thu Jan 12 22:17:09 2012 | zypp(zypper)
    88   |   89   | Thu Jan 12 23:10:42 2012 | Thu Jan 12 23:10:46 2012 | zypp(zypper)
    90   |   91   | Thu Jan 12 23:11:40 2012 | Thu Jan 12 23:11:42 2012 | zypp(zypper)
   108   |  109   | Fri Jan 13 13:01:06 2012 | Fri Jan 13 13:01:10 2012 | zypp(zypper)
```

- 2 使用下列指令取得快照對的已變更檔案清單：`snapper status 前..後`。含有內容變更的檔案以「c」標示，新增的檔案以「+」標示，刪除的檔案以「-」標示。下面的範例顯示了安裝套件 `ncftp` 的快照對。

```
~ # snapper status 108..109
+... /usr/bin/ncftp
+... /usr/bin/ncftpbatch
+... /usr/bin/ncftpget
+... /usr/bin/ncftpls
[...]
```

+...	/usr/share/man/man1/ncftpspooler.1.gz
c...	/var/cache/zypp/solv/@System/cookie
c...	/var/cache/zypp/solv/@System/solv
c...	/var/lib/rpm/Basenames
c...	/var/lib/rpm/Dirnames
c...	/var/lib/rpm/Filemd5s
c...	/var/lib/rpm/Group
c...	/var/lib/rpm/Installtid
c...	/var/lib/rpm/Name
c...	/var/lib/rpm/Packages
c...	/var/lib/rpm/Providename
c...	/var/lib/rpm/Provideversion
c...	/var/lib/rpm/Requirename
c...	/var/lib/rpm/Requireversion

```
c... /var/lib/rpm/Shalheader
c... /var/lib/rpm/Sigmd5
c... /var/lib/zypp/SoftLocks
```

- 3** 若要顯示特定檔案的差異，請執行 `snapper diff` 前..後 檔案名稱。如果不指定 檔案名稱，將會顯示所有檔案的差異。

```
~ # snapper diff 108..109 /var/lib/zypp/SoftLocks
--- /.snapshots/108/snapshot/var/lib/zypp/SoftLocks 2012-01-12
23:15:22.408009164 +0100
+++ /.snapshots/109/snapshot/var/lib/zypp/SoftLocks 2012-01-13
13:01:08.724009131 +0100
@@ -1,4 +1,2 @@
-# zypp::SoftLocksFile generated Thu Jan 12 23:10:46 2012
-#
-ncftp
-#
+# zypp::SoftLocksFile generated Fri Jan 13 13:01:08 2012
+##
```

- 4** 若要還原一或多個檔案，請執行 `snapper -v undochange` 前..後 檔案名稱。如果不指定 檔案名稱，將會還原所有已變更的檔案。

```
~ # snapper -v undochange 108..109
create:0 modify:16 delete:21
undoing change...
deleting /usr/share/man/man1/ncftpspooler.1.gz
deleting /usr/share/man/man1/ncftpput.1.gz
[...]
deleting /usr/bin/ncftpls
deleting /usr/bin/ncftpget
deleting /usr/bin/ncftpbatch
deleting /usr/bin/ncftp
modifying /var/cache/zypp/solv/@System/cookie
modifying /var/cache/zypp/solv/@System/solv
modifying /var/lib/rpm/Basenames
modifying /var/lib/rpm/Dirnames
modifying /var/lib/rpm/Filemd5s
modifying /var/lib/rpm/Group
modifying /var/lib/rpm/Installtid
modifying /var/lib/rpm/Name
modifying /var/lib/rpm/Packages
modifying /var/lib/rpm/Providename
modifying /var/lib/rpm/Provideversion
modifying /var/lib/rpm/Requirename
modifying /var/lib/rpm/Requireversion
modifying /var/lib/rpm/Shalheader
modifying /var/lib/rpm/Sigmd5
modifying /var/lib/zypp/SoftLocks
undoing change done
```

4.2.2 使用 Snapper 從每小時備份還原檔案

除了 YaST 和 zypper 快照之外，Snapper 還會建立系統分割區 (/) 的每小時備份。您可以使用這些備份快照來還原遭意外刪除或修改但無法復原的檔案。利用 Snapper 的差異比對功能，您還可以瞭解在特定時間點執行了哪些修改。

每小時備份快照屬於單一類型，並以描述時間軸標示。若要從這些快照還原檔案，請依過程 4.1, “使用 YaST 「*Snapper*」 模組復原變更” [25 頁] 或過程 4.2, “使用 snapper 指令復原變更” [28 頁] 中所述繼續操作。

注意：快照的儲存時間

依預設，系統會保留過去十天、十個月或十年的第一個快照。如需詳細資料，請參閱範例 4.1 「時間軸組態範例」 [32 頁]。

4.2.3 建立和修改 Snapper 組態

Snapper 的行為方式在組態檔案中加以定義；每個分割區或 Btrfs 子磁碟區的行為都是特定的。這些組態檔案位於 /etc/snapper/configs/ 下。隨 Snapper 一起安裝之 / 目錄的預設組態名為根。它會建立並管理 YaST 和 zypper 快照，以及 / 的每小時備份快照。

您可以為其他格式為 Btrfs 的分割區或 Btrfs 分割區上的現有子磁碟區建立您自己的組態。在下面的範例中，我們將設定 Snapper 組態以用於備份掛接於 /srv/www 且採用 Btrfs 格式之獨立分割區上的 Web 伺服器資料。

您可以使用 snapper 本身或 YaST 「*Snapper*」 模組來從這些快照還原檔案。在 YaST 中，您需要選取「*目前組態*」，同時還需要使用全域參數 -c 指定 snapper 的組態 (例如 snapper -c myconfig list)。

若要建立新的 Snapper 組態，請執行 snapper create-config:

```
snapper -c www-data❶ create-config  
/srv/www❷
```

- ❶ 組態檔案的名稱。
- ❷ 要建立快照之分割區或 Btrfs 子磁碟區的掛裝點。

此指令將會使用 `/etc/snapper/config-templates/default` 中的適當預設值建立一個新的組態檔案 `/etc/snapper/config-templates/www-data`。

提示：組態預設值

新組態的預設值取自 `/etc/snapper/config-templates/default`。若要使用您自己的一組預設值，請在同一目錄中建立此檔案的副本，然後根據您的需求進行調整。若要使用該副本，請使用 **create-config** 指令指定 `-t` 選項：

```
snapper -c www-data create-config -t my_defaults /srv/www
```

4.2.3.1 調整組態檔案

若要調整組態檔案，您需要使用編輯器對它進行修改。它包含格式為 `鍵=值` 的鍵/值組。您只能變更 *值*。

SUBVOLUME

要建立快照之分割區或子磁碟區的掛裝點。請勿進行變更。

FSTYPE

分割區的檔案系統類型。請勿進行變更。

NUMBER_CLEANUP

定義當快照總計數超出使用 `NUMBER_LIMIT` 指定的數目以及使用 `NUMBER_MIN_AGE` 指定的期限時，是否自動刪除舊快照。有效值：`yes` 和 `no`

注意：限制和期限

系統始終會同時評估 `NUMBER_LIMIT` 和 `NUMBER_MIN_AGE`。只有在同時滿足這兩個條件時，才會刪除快照。如果您希望總是保留特定數目的快照而不考慮其期限，請將 `NUMBER_MIN_AGE` 設為 0。不過，如果您不想保留超過特定期限的快照，請將 `NUMBER_LIMIT` 設為 0。

NUMBER_LIMIT

定義在 `NUMBER_CLEANUP` 設為 `yes` 時要保留的快照數量。

NUMBER_MIN_AGE

定義快照在可供自動刪除之前的最短保留期限 (秒)。

TIMELINE_CREATE

如果設為 yes，將會建立每小時快照。這是目前唯一一種自動建立快照的方法，因此強烈建議您將它設為 yes。有效值：yes 和 no

TIMELINE_CLEANUP

定義當快照計數超出使用時間軸限制 * 選項指定的數目以及使用 TIMELINE_MIN_AGE 指定的期限時，是否自動刪除舊快照。有效值：yes 和 no

TIMELINE_MIN_AGE

定義快照在可供自動刪除之前的最短保留期限 (秒)。

TIMELINE_LIMIT_HOURLY、TIMELINE_LIMIT_DAILY、
TIMELINE_LIMIT_MONTHLY 和 TIMELINE_LIMIT_YEARLY
要以小時、天、月和年保留的快照數目。

範例 4.1 時間軸組態範例

```
TIMELINE_CREATE="yes"  
TIMELINE_CLEANUP="yes"  
TIMELINE_MIN_AGE="1800"  
TIMELINE_LIMIT_HOURLY="10"  
TIMELINE_LIMIT_DAILY="10"  
TIMELINE_LIMIT_MONTHLY="10"  
TIMELINE_LIMIT_YEARLY="10"
```

此組態範例啟用了會自動清理的每小時快照。系統始終會同時評估 TIMELINE_MIN_AGE 和 TIMELINE_LIMIT_*。在此範例中，快照在可供刪除之前的最短期限設為 30 分鐘 (1800 秒)。因為我們建立了每小時快照，所以這可確保僅保留最新的快照。如果將 TIMELINE_LIMIT_DAILY 設為非零值，這表示同時會保留當天的第一個快照。

要保留的快照

- 每小時：已建立的最後十個快照。
- 每日：保留最近十天內建立的第一個每日快照。
- 每月：保留最近十個月內當月最後一天建立的第一個快照。

- 每年：保留最近十年內當年最後一天建立的第一個快照。

4.2.3.2 以一般使用者身分使用 Snapper

依預設，Snapper 只能由 root 使用。但是，在下列情況中，某些群組或使用者需要能夠建立快照或透過回復至快照來復原變更：

- 網站管理員希望建立 /srv/www 的快照。
- 資料庫管理員希望建立資料庫的快照。
- 使用者希望建立其主目錄的快照。

為了以上這些目的，您可以建立用於授予使用者或/和群組權限的 Snapper 組態。除了此組態變更之外，對應的 .snapshots 目錄還必須可供指定的使用者讀取和存取。

過程 4.3 讓一般使用者可以使用 Snapper

請注意，此程序中的所有步驟都必須由 root 執行。

- 1 若不存在，請為使用者應該能夠在其上使用 Snapper 的分割區或子磁碟區建立 Snapper 組態。如需指示，請參閱第 4.2.3 節「建立和修改 Snapper 組態」[30頁]。範例：

```
snapper --config web_data create /srv/www
```

- 2 組態檔案將在 /etc/snapper/configs/ 名稱下建立，其中「名稱」是您在上一步中使用 -c/--config 指定的值(例如 /etc/snapper/configs/web_data)。根據您的需求調整該值；如需詳細資料，請參閱第 4.2.3.1 節「調整組態檔案」[31頁]。

- 3 設定 ALLOW_USERS 和/或 ALLOW_GROUPS 的值，以分別向使用者和/或群組授予權限。多個項目需要用 Space 加以分隔。例如，若要向使用者 www_admin 授予權限，請輸入：

```
ALLOW_USERS="www_admin"
```

- 4 對快照目錄路徑/.snapshots 授予讀取與存取權限。路徑將由您在此程序的第一步中所指定的子磁碟區取代。範例：

```
chmod a+rx /srv/www/.snapshots
```

現在，指定的使用者和/或群組便可以使用給定的 Snapper 組態。您可以使用 `list` 指令進行測試，例如：

```
www_admin:~ > snapper -c web_data list
```

4.2.4 停用自動快照

如果您在安裝期間使用 `Btrfs` 設定了根分割區，`Snapper` 將會自動建立系統的每小時快照，以及 `YaST` 和 `zypper` 交易的前快照與後快照。上述每個任務都可以按如下所示停用：

停用每小時快照

編輯 `/etc/snapper/configs/root` 並將 `TIMELINE_CREATE` 設為 `no`：

```
TIMELINE_CREATE="no"
```

停用 `zypper` 快照

解除安裝套件 `snapper-zypp-plugin`

停用 `YaST` 快照

編輯 `/etc/sysconfig/yast2` 並將 `USE_SNAPPER` 設為 `no`：

```
USE_SNAPPER="no"
```

4.3 手動建立和管理快照

`Snapper` 並不限於依照組態自動建立和管理快照；您還可以使用指令行工具或 `YaST` 模組手動建立快照對（「前與後」）或單一快照。

所有 `Snapper` 操作都會對現有組態進行（如需詳細資料，請參閱第 4.2.3 節「建立和修改 `Snapper` 組態」[30頁]）。您只能為存在組態的分割區或子磁碟區建立快照。預設會使用系統組態（根）。如果您要為您自己的組態建立或管理快照，則必須明確選擇它。您可以使用 `YaST` 中的「目前組態」下拉式功能表，或在指令行上指定 `-c` (`snapper -c 我的組態 指令`)。

4.3.1 快照中繼資料

每個快照都包含快照本身和一些中繼資料。建立快照時，您還需要指定中繼資料。修改快照表示變更其中繼資料—無法修改其內容。下列中繼資料適用於每個快照：

- **類型**：快照類型，請參閱第 4.3.1.1 節「快照類型」[35頁] 以取得詳細資料。此資料無法變更。
- **編號**：快照的唯一編號。此資料無法變更。
- **前快照編號**：指定相應前快照的編號。僅適用於類型為後的快照。此資料無法變更。
- **描述**：快照的描述。
- **使用者資料**：延伸描述，您可在其中以逗號分隔之鍵=值清單的形式指定自定資料：`reason=testing_stuff, user=tux`
- **清理演算法**：快照的清理演算法，請參閱第 4.3.1.2 節「清理演算法」[36頁] 以取得詳細資料。

4.3.1.1 快照類型

Snapper 知道三種不同類型的快照：前、後與單一。實際上，它們並無差異，但是 Snapper 會以不同的方式處理它們。

前

修改前檔案系統的快照。每個前快照都對應一個後快照。例如用於自動建立 YaST/zypper 快照。

POST

修改後檔案系統的快照。每個後快照都對應一個前快照。例如用於自動建立 YaST/zypper 快照。

single

獨立快照。例如用於自動建立每小時快照。這是建立快照時的預設類型。

4.3.1.2 清理演算法

Snapper 提供了三種用於清理舊快照的演算法。每日 cron 工作中會執行這些演算法。清理頻率本身是在分割區或子磁碟區的 Snapper 組態中加以定義 (如需詳細資料，請參閱第 4.2.3.1 節「調整組態檔案」[31頁])。

數目

當達到特定的快照計數時刪除舊快照。

時間軸

刪除經過特定期限的舊快照，但會保留大量每小時、每日、每月和每年快照。

空-前-後

刪除無差異的前/後快照對。

4.3.2 建立快照

建立快照的方式是執行 `snapper create` 或在 YaST 模組「*Snapper*」中按一下「建立」。下列範例說明如何從指令行建立快照。使用 YaST 介面時，採用它們應該不難。

提示：快照描述

您應始終指定有意義的描述，以便日後能夠識別其用途。透過使用者資料選項可以指定更多資訊。

```
snappercreate --description "2013 年第 2 週的快照"
```

為預設 (根) 組態建立獨立快照 (類型為單一) 並提供描述。因為未指定清理演算法，所以一律不自動刪除快照。

```
snapper --config home create --description "在 ~tux 中清理"
```

為名為 home 的自定組態建立獨立快照 (類型為單一) 並提供描述。因為未指定清理演算法，所以一律不自動刪除快照。

```
snapper --config home create --description "每日資料備份"  
--cleanup-algorithm timeline
```

為名為home的自定組態建立獨立快照(類型為單一)並提供描述。當檔案符合特定於組態中時間軸清理演算法的準則時，將會自動刪除該檔案。

```
snapper create --type pre--pre-number--description "在  
Apache 組態清理之前"
```

建立類型為前的快照並列印快照編號。需要第一個指令才能建立用於儲存「前」和「後」狀態的快照對。

```
snapper create --type post--pre-number 30--description "在  
Apache 組態清理之後"
```

建立類型為後並與前快照編號 30 配對的快照。需要第二個指令才能建立用於儲存「前」和「後」狀態的快照對。

```
snapper create --command COMMAND--description "在指令前後"  
在執行指令前後自動建立快照對。僅當在指令行上使用 snapper 時，此選項才可用。
```

4.3.3 修改快照中繼資料

Snapper可讓您修改快照的描述、清理演算法和使用者資料，所有其他中繼資料則無法變更。下列範例說明如何從指令行修改快照。使用 **YaST** 介面時，採用它們應該不難。

若要透過指令行修改快照，您需要知道其編號。請使用 **snapper list** 來顯示所有快照及其編號。

YaST「*Snapper*」模組已列出所有快照。從清單中選擇一個快照，然後按一下「修改」。

```
snapper modify --cleanup-algorithm "時間軸" 10  
修改預設(根)組態之快照 10 的中繼資料。清理演算法設為時間軸。
```

```
snapper --config home modify --description "每日備份"  
--cleanup-algorithm "時間軸"120  
修改名為home的自定組態之快照 120 的中繼資料。將會設定新的描述並取消設定清理演算法。
```

4.3.4 刪除快照

若要使用 YaST 「*Snapper*」 模組刪除快照，請從清單中選擇快照，然後按一下「刪除」。

若要使用指令行工具刪除快照，您需要知道其編號。請透過執行 `snapper list` 來取得該編號。若要刪除快照，請執行 `snapper delete 編號`。

提示：刪除快照對

刪除前快照時，您應一律刪除其對應的後快照 (反之亦然)。

```
snapper delete 65
```

刪除預設 (根) 組態的快照 65。

```
snapper -c home delete 89 90
```

刪除名為 `home` 之自定組態的快照 89 和 90。

提示：舊快照佔用較多磁碟空間

如果您要刪除快照以釋放硬碟上的空間 (如需詳細資料，請參閱第 4.1.1 節「快照與磁碟空間」[23頁])，請確定先刪除舊快照。快照越舊，它佔用的磁碟空間就越多。

快照也可由每日 `cron` 工作自動刪除。如需詳細資訊，請參閱第 4.3.1.2 節「清理演算法」[36頁]。

4.4 限制

雖然 `Btrfs` 及 `Snapper` 已備妥可用於線上，但是它們仍在持續不斷地進行進一步開發。目前存在下列限制。計劃在後續版本中解決這些問題。

4.4.1 資料一致性

在建立快照時，沒有任何一種機制可確保資料的一致性。在建立快照的同時寫入檔案 (例如資料庫)，都將導致檔案損毀或部分寫入。還原此類檔案將會導致

問題。因此，強烈建議您始終仔細檢閱已變更檔案及其差異的清單。僅還原確實需要歸屬於要復原之動作的檔案。

4.4.2 回復使用者新增

`/home` 通常位於獨立的分割區上。此類獨立分割區不屬於用於執行 YaST 復原的預設組態。因此，在使用 Snapper 復原使用者新增時，不會刪除使用者的主分割區。強烈建議您使用 YaST「*使用者和群組管理*」工具來移除使用者。

4.4.3 不對 `/boot` 和開機載入程式的變更執行任何復原

目前，SUSE Linux Enterprise Server 無法從 Btrfs 分割區開機。因此，當對系統分割區使用 Btrfs 時，會在安裝過程中為 `/boot` 建立獨立分割區。因為 `/boot` 不支援快照，所以下列限制適用於 YaST/zypper 復原：

不對開機載入程式上的任何組態變更進行復原

唯一可供復原的檔案是 `/etc` 中的開機載入程式組態檔案。主要組態檔案位於 `/boot` 下，無法進行復原。

不對核心安裝進行完整復原

核心本身及其 `initrd` 均安裝在 `/boot` 分割區中，而核心模組或來源則分別安裝在 `/var/lib` 和 `/usr/src` 中。此外，每個核心安裝還會變更 `/boot` 中的開機載入程式組態檔案。因此，每當您執行涉及復原核心安裝的復原時，都需要從 `/boot` 手動移除核心及其 `initrd`，並透過移除核心的開機項目來調整開機載入程式組態。

4.5 常見問題解答

為何 Snapper 從不顯示 `/var/log`、`/tmp` 及其他目錄中的變更？

對於某些目錄，我們決定停用「建立快照」（例如 `/var/log`），因為回復記錄會加大搜尋問題的難度。為了排除某路徑進行「快照建立」，我們為該路徑建立了子磁碟區。排除對 SUSE Linux Enterprise Server 上的下列掛接點進行「快照建立」：

- /opt
- /srv
- /tmp
- /var/crash
- /var/log
- /var/run
- /var/spool
- /var/tmp

能否從開機載入程式將快照開機？

目前不行。SUSE Linux Enterprise Server 上的開機載入程式目前不支援從 Btrfs 分割區進行開機。

4.6 對簡易佈建的 LVM 磁碟區使用 Snapper

除了針對 Btrfs 檔案系統建立快照之外，snapper 還支援針對格式為 ext3 或 XFS 之簡易佈建的 LVM 磁碟區「建立快照」(但不支援對一般 LVM 磁碟區建立快照)。如需詳細資訊及設定指示，請參閱第 15.2 節「LVM 組態」(第 15 章「進階磁碟設定」, ↑部署指南)。

若要對簡易佈建的 LVM 磁碟區使用 Snapper，您需要為它建立一個 Snapper 組態。在 LVM 上，需要使用 `--fstype=lvm`(檔案系統) 指定檔案系統。目前支援 ext3 和 XFS，因此 ext3 或 xfs 是檔案系統的有效值。範例：

```
snapper -c lvm create-config --fstype="lvm(xfs)" /thin_lvm
```

您可以依第 4.2.3.1 節「調整組態檔案」[31 頁] 中所述根據需求調整此組態。現在，您可以使用 Snapper 來建立和管理快照、還原檔案以及復原變更(如上所述)。

透過 VNC 進行遠端存取

虛擬網路計算 (VNC) 可讓您透過圖形桌面環境控制遠端電腦 (與遠端外圍程序存取相對)。VNC 獨立於平台，可讓您從任何作業系統存取遠端機器。

SUSE Linux Enterprise Server 支援兩種不同類型的 VNC 工作階段：一次性工作階段，只要用戶端 VNC 連線不中斷，該工作階段將一直處於「作用中」；永久工作階段，此工作階段將一直處於「作用中」，除非明確將其終止。

注意：工作階段類型

機器可以在不同的連接埠上同時提供這兩種工作階段，但是開啟的工作階段無法從一種類型轉換為另一種類型。

5.1 一次性 VNC 工作階段

一次性工作階段由遠端用戶端啟動。它會在伺服器上啟動圖形登入畫面。這樣，您就可以選擇啟動工作階段的使用者，如果登入管理員支援，還可以選擇桌面環境。一旦您終止此類 VNC 工作階段的用戶端連線，在該工作階段內啟動的所有應用程式也會隨之終止。一次性 VNC 工作階段無法共用，不過在同一台主機上可以同時啟動多個工作階段。

過程 5.1 啟用一次性 VNC 工作階段

- 1 啟動「YaST」>「網路服務」>「遠端管理 (VNC)」。
- 2 選取「允許遠端管理」。

- 3 若需要，還可核取「在防火牆中開啟埠」(例如，當網路介面設定為位於外部區域中時)。如果您有多個網路介面，請透過「*防火牆細節*」設定在特定介面開啟防火牆埠的限制。
- 4 按一下「*完成*」確認您的設定。
- 5 如果有些需要的套件尚未提供，您需要批准安裝缺失套件。

注意：可用的組態

SUSE Linux Enterprise Server 上的預設組態以 16 位元色彩深度、1024x768 像素解析度顯示工作階段。使用「一般」的 VNC 檢視器 (相當於 VNC 顯示埠 1) 時，可在連接埠 5901 上檢視工作階段，而使用網頁瀏覽器時，則可在連接埠 5801 上檢視工作階段。

其他組態可在不同的連接埠上使用，請參閱第 5.1.2 節「設定一次性 VNC 工作階段」[43頁]。

在一次性工作階段中，VNC 顯示埠號碼和 X 顯示埠號碼是獨立的。VNC 顯示埠號碼需要手動指定給伺服器支援的每個組態 (在上例中為 :1)。每次以其中一種組態啟動 VNC 工作階段時，工作階段會自動獲得可用的 X 顯示埠號碼。

5.1.1 啟動一次性 VNC 工作階段

若要啟動一次性 VNC 工作階段，用戶端機器上必須安裝 VNC 檢視器。SUSE Linux 產品上的標準檢視器是 `vncviewer`，由套件 `tightvnc` 提供。也可以使用網頁瀏覽器和 Java Applet 來檢視 VNC 工作階段。

若要以伺服器的預設組態啟動 VNC 檢視器與工作階段，請使用以下指令：

```
vncviewer jupiter.example.com:1
```

您也可以指定含兩個冒號的連接埠號碼，而不指定 VNC 顯示埠號碼：

```
vncviewer jupiter.example.com::5901
```

或者，可以在支援 Java 的網頁瀏覽器中，輸入 URL `http://jupiter.example.com:5801` 來檢視 VNC 工作階段

5.1.2 設定一次性 VNC 工作階段

如果您不需要或不想修改預設組態，可以跳過本小節。

一次性 VNC 工作階段透過 `xinetd` 精靈啟動。`/etc/xinetd.d/vnc` 中有一個組態檔。其中預設會提供六個組態區塊：三個用於 VNC 檢視器 (`vnc1` 到 `vnc3`)，另外三個提供 Java Applet (`vnchttpd1` 到 `vnchttpd3`)。預設只有 `vnc1` 及 `vnchttpd1` 處於作用中狀態。

若要啟用某個組態，請在第一欄中以 `#` 字元將 `disable = yes` 這一行設定成註解，或者乾脆移除該行。若要取消啟用某個組態，請取消註解或新增該行。

Xvnc 伺服器可透過 `server_args` 選項設定。相關選項清單，請參閱 `Xnvc --help`。

新增自定組態時，請確定它們沒有使用同一台主機上的其他組態、服務或現有的永久 VNC 工作階段已在使用的連接埠。

輸入以下指令啟用組態變更：

```
rcxinetd reload
```

重要：防火牆與 VNC 埠

依照過程 5.1, “啟用一次性 VNC 工作階段” [41 頁] 中所述啟用遠端管理時，會在防火牆中開啟連接埠 5801 及 5901。如果提供 VNC 工作階段的網路介面受防火牆保護，則您在為 VNC 工作階段啟用其他連接埠時，需要手動開啟相應的連接埠。如需指示，請參閱第 15 章「*Masquerading and Firewalls*」(↑*Security Guide*)。

5.2 永久 VNC 工作階段

永久 VNC 工作階段在伺服器上啟動。不論用戶端的連線狀態為何，此工作階段以及在此工作階段中啟動的所有應用程式會一直執行，直至工作階段被終止。

從多個用戶端可以同時存取一個永久工作階段。此特性非常適合用於在一個用戶端具有完整存取權，而所有其他用戶端具有僅檢視存取權的場合進行演示操

作。在訓練中，訓練員可能需要存取學員桌面的情況則是另一個使用案例。不過，大多數情況下您可能並不想共用 VNC 工作階段。

與會啟動顯示管理員的一次性工作階段不同，永久工作階段會啟動準備就緒的作業桌面，該桌面以啟動 VNC 工作階段之使用者的身分執行。

對永久工作階段的存取受到密碼保護，密碼可能為以下兩種類型：

- 授予完全存取權的一般密碼，或
- 授予非互動式 (僅檢視) 存取權限的選擇性僅檢視密碼。

一個工作階段可以同時擁有這兩種類型的多個用戶端連線。

過程 5.2 啟動永久 VNC 工作階段

- 1 開啟外圍程序，並確定您以應當擁有 VNC 工作階段的使用者身分登入。
- 2 如果提供 VNC 工作階段的網路介面受防火牆保護，則您需要在防火牆中手動開啟工作階段使用的連接埠。如果要啟動多個工作階段，可以開啟一系列連接埠。如需如何設定防火牆的詳細資料，請參閱第 15 章「*Masquerading and Firewalls*」(↑*Security Guide*)。

`vncserver` 對顯示埠 :1 使用連接埠 5901，對顯示埠 :2 使用連接埠 5902，依此類推。對於永久工作階段，VNC 顯示埠和 X 顯示埠的號碼通常都是相同的。

- 3 若要以 1024x769 像素的解析度及 16 位元的色彩深度啟動工作階段，請輸入以下指令：

```
vncserver -geometry 1024x768 -depth 16
```

`vncserver` 指令在未指定顯示埠號碼的情況下，會挑選未使用的號碼，並列印出它的選擇。有關更多選項的資訊，請參閱 `man 1 vncserver`。

首次執行 `vncviewer` 時，它會要求您輸入擁有工作階段完整存取權限的密碼。如果需要，您也可以提供對工作階段具有僅檢視存取權限的密碼。

此處提供的密碼還可供同一個使用者用來啟動以後的工作階段。使用 `vncpasswd` 指令可以變更這些密碼。

重要：安全性考量

請務必使用足夠長 (8 個或更多字元) 的嚴密密碼。請不要共用這些密碼。

VNC 連線未經過加密，因此能夠偵測兩部機器間網路傳輸的人員，可以在工作階段開始時的密碼傳送過程中讀取密碼。

若要終止工作階段，請從 VNC 檢視器關閉在 VNC 工作階段內部執行的桌面環境，就如同關閉一般本地 X 工作階段一樣。

如果您想要手動終止工作階段，請在 VNC 伺服器上開啟一個外圍程序，並務必以擁有您要終止之 VNC 工作階段的使用者身分登入。執行以下指令以終止在顯示埠 :1 上執行的工作階段：`vncserver -kill :1`

5.2.1 連接至永久 VNC 工作階段

若要連接至永久 VNC 工作階段，必須安裝 VNC 檢視器。SUSE Linux 產品上的標準檢視器是 `vncviewer`，由套件 `tightvnc` 提供。也可以使用網頁瀏覽器和 Java Applet 來檢視 VNC 工作階段。

若要啟動 VNC 檢視器並連接至 VNC 伺服器的顯示埠 :1，請使用以下指令

```
vncviewer jupiter.example.com:1
```

您也可以指定含兩個冒號的連接埠號碼，而不指定 VNC 顯示埠號碼：

```
vncviewer jupiter.example.com::5901
```

或者，可以在支援 Java 的網頁瀏覽器中，輸入 URL

`http://jupiter.example.com:5801` 來檢視 VNC 工作階段

5.2.2 設定永久 VNC 工作階段

永久 VNC 工作階段可透過編輯 `$HOME/.vnc/xstartup` 來設定。此外圍程序程序檔預設會啟動 `xterm` 及 `twm` 視窗管理員。若要改為啟動 GNOME 或 KDE，請用下列其中一項取代以 `twm` 開頭的行：

```
/usr/bin/gnome      # GNOME  
/usr/bin/startkde   # KDE
```

注意：每個使用者對應一個組態

永久 VNC 工作階段透過單個基於使用者的組態設定。由一個使用者啟動的多個工作階段皆使用相同的啟動檔案和密碼檔案。

使用指令行工具管理軟體

本章介紹了兩個用於管理軟體的指令行工具：Zypper 與 RPM。有關在此內容中所使用辭彙的定義(例如，儲存庫、修補程序或更新)，請參閱第 9.1 節「術語定義」(第 9 章「安裝或移除軟體」, ↑部署指南)。

6.1 使用 Zypper

Zypper 是用於安裝、更新和移除套件以及管理儲存庫的指令行套件管理員。Zypper 的語法與 `rug` 的語法類似。不同的是，Zypper 不需要視情境執行 `zmd` 精靈。如需有關 `rug` 相容性的詳細資訊，請參閱 `man zypper` 中的「與 RUG 的相容性」部分。這部分內容對於執行遠端軟體管理任務或透過外圍程序程序檔管理軟體非常有用。

6.1.1 一般使用情形

Zypper 的一般語法為：

```
zypper [global-options] command [command-options] [arguments] ...
```

括號中的部分為非必需。執行 Zypper 最簡單的方法就是輸入其名稱，後面跟著指令。例如，若要將所有需要的修補程式套用至系統類型：

```
zypper patch
```

此外，您還可以在指令之前輸入全域選項來從一或多個全域選項中進行選擇。例如，`--non-interactive` 表示直接執行指令，不詢問任何問題 (自動套用預設回答)：

```
zypper --non-interactive patch
```

若要使用特定於特殊指令的選項，請在指令之後輸入這些選項。例如，`--auto-agree-with-licenses` 表示將所有需要的修補程式套用至系統，而不要求確認任何授權 (系統會自動接受所有授權)。

```
zypper patch --auto-agree-with-licenses
```

某些指令需要一或多個引數：例如，使用安裝指令時，您需要指定要安裝的套件：

```
zypper install mplayer
```

某些選項也需要引數。以下指令會列出所有已知模式：

```
zypper search -t pattern
```

您可以將上述所有指令組合使用。例如，以下指令將從 `factory` 儲存庫安裝 `mplayer` 和 `amarok` 套件，並顯示詳細資訊：

```
zypper -v install --from factory mplayer amarok
```

`--from` 選項可確保所有儲存庫均處於啟用狀態 (以解決相依性問題)，並且始終從指定的儲存庫要求套件。

大部分 Zypper 指令都有一個 `dry-run` 選項，對指定的指令進行模擬。它可以用於測試。

```
zypper remove --dry-run MozillaFirefox
```

Zypper 支援全域 `--userdata` 字串選項，用於識別交易之用途。使用者定義的字串會傳遞至位於 `/var/log/zypp/history` 中的 `zypper` 歷程記錄及 `Snapper`。

```
zypper --userdata string patch
```

6.1.2 使用 Zypper 安裝和移除軟體

若要安裝或移除套件，請使用以下指令：

```
zypper install package_name
zypper remove package_name
```

Zypper 可以使用多種方式來指定安裝和移除指令中所使用的套件：

用確切的套件名稱 (與版本號碼)

```
zypper install MozillaFirefox
```

或

```
zypper install MozillaFirefox-3.5.3
```

用儲存庫別名和套件名稱

```
zypper install mozilla:MozillaFirefox
```

`mozilla` 是要安裝套件所在之儲存庫的別名。

用含萬用字元的套件名稱

以下指令將安裝名稱以「**Moz**」開頭的所有套件。使用萬用字元時請務必小心，特別是在移除套件時。

```
zypper install 'Moz*'
```

用功能

例如，您要安裝 **Perl** 模組，但不知道套件的名稱，用功能指定便會幫上忙：

```
zypper install 'perl(Time::ParseDate)'
```

用功能和/結構和/或版本

除功能外，還可以同時指定結構 (如 `i586` 或 `x86_64`) 和/或版本。版本的前面必須使用運算子：`<` (小於)、`<=` (小於等於)、`=` (等於)、`>=` (大於等於)、`>` (大於)。

```
zypper install 'firefox.x86_64'
zypper install 'firefox>=3.5.3'
zypper install 'firefox.x86_64>=3.5.3'
```

用 **RPM** 檔案的路徑

您也可以指定套件的本地或遠端路徑：

```
zypper install /tmp/install/MozillaFirefox.rpm
zypper install
http://download.opensuse.org/repositories/mozilla/SUSE_Factory/x86_64/MozillaFirefox-3.5.3-1.3.x86_64.rpm
```

若要同時安裝並移除套件，請使用 `+/-` 輔助按鍵。若要安裝 `emacs` 並移除 `vim`，請使用：

```
zypper install emacs -vim
```

若要移除 `emacs` 並安裝 `vim`，請使用：

```
zypper remove emacs +vim
```

為了防止將名稱以 `-` 開頭的套件解譯為指令選項，請一律將此類名稱用做第二個引數。如果行不通，則在前面加上 `--`：

```
zypper install -emacs +vim      # Wrong
zypper install vim -emacs       # Correct
zypper install -- -emacs +vim   # same as above
zypper remove emacs +vim       # same as above
```

如果想讓系統在移除某套件後自動移除由於此操作而導致不再需要的所有套件，請使用 `--clean-deps` 選項：

```
rm package_name --clean-deps
```

依預設，`Zypper` 會在安裝或移除所選套件前或出現問題時要求您確認。使用 `--non-interactive` 選項可覆寫此行為。此選項必須放在實際指令 (`install`、`remove` 和 `patch`) 的前面，如下所示：

```
zypper --non-interactive install package_name
```

此選項允許在程序檔與 `cron` 工作中使用 `Zypper`。

警告：不要移除必要的系統套件

不要移除 `glibc`、`zypper`、`kernel` 或類似套件。這些套件都是系統的必要套件，若是移除，可能會導致系統不穩定甚至停止工作。

6.1.2.1 安裝或下載來源套件

若要安裝某套件對應的來源套件，請使用：

```
zypper source-install package_name
```

使用此指令還會安裝指定套件的建構相依套件。如果不想如此，請新增參數 `-D`。若想單獨安裝建構相依套件，請使用 `-d`。

```
zypper source-install -D package_name # source package only
zypper source-install -d package_name # build dependencies only
```

當然，您必須在儲存庫清單中啟用含來源套件的儲存庫(預設會新增，但不會啟用)，此指令才有效。如需有關儲存庫管理的詳細資料，請參閱第 6.1.5 節「使用 Zypper 管理儲存庫」[57頁]。

儲存庫中所有可用來源套件的清單可透過以下指令獲得：

```
zypper search -t srcpackage
```

您還可以將所有已安裝套件的來源套件下載到本地目錄。若要下載來源套件，請使用：

```
zypper source-download
```

預設下載目錄為 `/var/cache/zypper/source-download`。您可以使用 `--directory` 選項變更該目錄。若只想顯示遺失或多餘的套件而不進行任何下載或刪除操作，請使用 `--status` 選項。若要刪除多餘的來源套件，請使用 `--delete` 選項。若要停用刪除操作，請使用 `--no-delete` 選項。

6.1.2.2 公用程式

若要驗證是否仍滿足所有相依條件並執行未滿足的相依條件，請使用：

```
zypper verify
```

除了必須滿足的相依條件之外，一些套件還會「推薦」其他套件。這些推薦的套件只有在確實可用並可安裝時才會進行安裝。如果所推薦的套件在推薦方套件安裝之後 (透過新增其他套件或硬體) 才可用，請使用以下指令：

```
zypper install-new-recommends
```

此指令在接入網路攝影機或 WLAN 設備後非常有用。它將安裝設備的驅動程式及相關軟體 (如果有)。驅動程式及相關軟體只有在符合了某些硬體相依性條件後才可安裝。

6.1.3 使用 Zypper 更新軟體

Zypper 有三種方法更新軟體：安裝修補程式、安裝新版本的套件或更新整個套裝作業系統。最後一種方法透過 `zypper dist-upgrade` 指令來實現，可參閱第 6.1.4 節「使用 zypper 進行套裝作業系統升級」[54頁]。

6.1.3.1 安裝修補程式

若要安裝所有正式發佈的適用於您系統的修補程式，只需執行：

```
zypper patch
```

在此情況下，系統會檢查儲存庫中所有可用修補程式的關聯性，並視需要進行安裝。為 SUSE Linux Enterprise Server 安裝進行註冊後，包含此類修補程式的正式更新儲存庫將新增至您的系統。需要套用這些修補程式時，只需輸入上述指令即可。

Zypper 有三種指令可以查詢修補程式的可用性：

```
zypper patch-check
```

列出所需修補程式 (已套用至系統但尚未安裝的修補程式) 的數量。

```
~ # zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

```
zypper list-patches
```

列出所需的所有修補程式 (已套用至系統但尚未安裝的修補程式)。

```
~ # zypper list-patches
Loading repository data...
Reading installed packages...

Repository | Name | Version | Category | Status
-----+-----+-----+-----+-----
Updates for openSUSE 11.3 11.3-1.82 | lxsession | 2776 | security | needed
```

```
zypper patches
```

列出為 SUSE Linux Enterprise Server 提供的所有修補程式，不論是否已安裝或適用於您的安裝。

還會列出與特定問題相關的修補程式並加以安裝。若要列出特定的修補程式，請使用 `zypper list-patches` 指令及以下選項：

```
--bugzilla[=數字]
```

列出 **Bugzilla** 問題所需的所有修補程式。如果您只想列出針對此特定錯誤的修補程式，還可以指定錯誤編號。

`--cve [= 編號]`

列出各種 CVE (Common Vulnerabilities and Exposures, 通用弱點與揭露) 問題所需的所有修補程式, 或僅符合特定 CVE 編號的修補程式 (如果指定編號)。

若要安裝針對特定 Bugzilla 或 CVE 問題的修補程式, 請使用以下指令：

```
zypper patch --bugzilla=number
```

或

```
zypper patch --cve=number
```

例外, 若要安裝 CVE 編號為 CVE-2010-2713 的安全性修補程式, 請執行：

```
zypper patch --cve=CVE-2010-2713
```

6.1.3.2 安裝更新

如果儲存庫中只含有新套件, 但未提供修補程式, 則 `zypper patch` 不起任何作用。若要使用可用的較新版本更新所有安裝的套件, 請使用：

```
zypper update
```

若要更新個別套件, 請在更新或安裝指令中指定套件：

```
zypper update package_name  
zypper install package_name
```

所有可安裝的新套件的清單可透過以下指令獲得：

```
zypper list-updates
```

請注意, 此指令只會列出符合以下準則的套件：

- 與已安裝套件具有相同的廠商,
- 提供套件的儲存庫相較於已安裝套件, 擁有更高或相同的優先程度,
- 可安裝 (符合所有相依性條件)。

所有新可用套件 (無論是否可安裝) 的清單可透過以下指令獲得：

```
zypper list-updates --all
```

若要找出新套件無法安裝的原因，只需如上文所述使用 `zypper install` 或 `zypper update` 指令即可。

6.1.3.3 升級到新的產品版本

若要將安裝的產品輕鬆升級到新版本 (例如，從 SUSE Linux Enterprise Server 11 升級到 SUSE Linux Enterprise Server 11 SP1)，請先調整您的儲存庫以符合目前的 SUSE Linux Enterprise Server 儲存庫。如需詳細資訊，請參閱第 6.1.5 節「使用 Zypper 管理儲存庫」[57頁]。然後使用 `zypper dist-upgrade` 指令並指定所需的儲存庫。此指令可確保所有套件都從目前啟用的儲存庫安裝。如需詳細說明，請參閱第 6.1.4 節「使用 zypper 進行套裝作業系統升級」[54頁]。

若將要套裝作業系統升級限制為特定儲存庫中的套件，並在滿足相依性條件時考量其他儲存庫，請使用 `--from` 選項並指定儲存庫 (使用別名、編號或 URI)。

注意: `zypper update` 與 `zypper dist-upgrade` 的不同之處

選擇 `zypper update` 會將套件更新至您的產品所適用的較新版本，並保持系統的完整性。`zypper update` 遵從以下規則：

- 不變更廠商
- 不變更結構
- 不降級
- 保留安裝的套件

執行 `zypper dist-upgrade` 時，目前啟用的儲存庫中的所有套件都會安裝。此規則會強制執行，因此套件可能會變更廠商或結構，甚至降級。不滿足相依條件的所有套件在升級後都會被解除安裝。

6.1.4 使用 zypper 進行套裝作業系統升級

使用 `zypper` 指令行公用程式可以升級至新版套裝作業系統。最重要的是，您可以從執行中的系統啟動系統升級程序。

對於要執行遠端升級或在許多具有類似設定的系統上升級的進階使用者來說，此項功能很有吸引力。

6.1.4.1 在使用 zypper 開始升級之前

為了避免在使用 zypper 進行升級的過程中出現未預期的錯誤，請將導致風險的因素減至最低：

- 儘可能多地關閉應用程式和不需要的服務，並將所有的一般使用者登出。
- 在開始升級之前停用協力廠商儲存庫，或降低這些儲存庫的優先程度，以便讓預設系統儲存庫之套件的優先程度優先。完成升級後，再啟用這些儲存庫，並編輯其版本字串，使之與升級後正在執行之系統套裝作業系統的版本號碼相符。

6.1.4.2 升級程序

警告：檢查系統備份

在真正開始執行升級程序前進行檢查，確定您的系統備份最新並可還原。這一點很重要，因為您之後必須執行許多手動步驟。

程式 zypper 指令可以使用完整形式，也可以使用縮寫形式。例如，您可以將 `zypper install` 縮寫為 `zypper in`。在以下段落中，使用的是簡短形式。

- 1 執行線上更新，以確定軟體管理堆疊保持最新。如需詳細資訊，請參閱第 1 章「YaST 線上更新」[3頁]。
- 2 設定要用做更新來源的儲存庫。請務必正確設定。使用 YaST (請參閱第 9.3 節「管理軟體儲存庫與服務」(第 9 章「安裝或移除軟體」, ↑部署指南)) 或 zypper (請參閱第 6.1 節「使用 Zypper」[47頁])。根據您的自定設定，以下步驟中使用的儲存庫名稱會稍有不同。

考慮準備或更新自己的安裝伺服器。如需背景詳細資訊，請參閱第 14.2.1 節「使用 YaST 設定安裝伺服器」(第 14 章「遠端安裝」, ↑部署指南)。

若要檢視您目前的儲存庫，請輸入：

```
zypper lr -u
```

- 2a 使用以下指令將系統儲存庫的版本號碼從 11-SP2 提升為 11-SP3，以及新增儲存庫：

```
server=http://download.example.org
zypper ar $server/distribution/11-SP3/repo/oss/ SLE-11-SP3
zypper ar $server/update/11-SP3/ SLE-11-SP3-Update
```

移除舊的儲存庫：

```
zypper rr SLE-11-SP2
zypper rr SLE-11-Update
```

- 2b** 停用協力廠商儲存庫或其他 Open Build Service 儲存庫，因為 `zypper dup` 只能用於預設的儲存庫 (以要停用的儲存庫名稱取代 `repo-alias`)：

```
zypper mr -d repo-alias
```

或者，也可以降低這些儲存庫的優先程度。

注意：處理未解決的相依性

`zypper dup` 會移除所有存在相依性未解決的問題的套件，但會保留滿足相依性之已停用儲存庫的套件。

`zypper dup` 可確保所有安裝的套件都來自同一個可用的儲存庫。它不會考慮所安裝套件的版本、架構或廠商，因此會模擬執行全新安裝。儲存庫中不再可用的套件會視為孤立套件。如果此類套件無法滿足相依性，即會被解除安裝。若滿足相依性，將不會被解除安裝。

- 2c** 此作業結束後，使用以下指令檢查儲存庫組態：

```
zypper lr -d
```

- 3 使用 `zypper ref` 重新整理本地中繼資料和儲存庫內容。
- 4 使用 `zypper up zypper` 從 11 SP1 儲存庫拉入 `zypper` 和套件管理堆疊。
- 5 使用 `zypper dup` 執行實際的套裝作業系統升級。系統會要求您確認 SUSE Linux Enterprise 和某些套件的授權，具體視安裝的套件集而定。
- 6 使用 `SuSEconfig` 執行基本的系統組態。
- 7 使用 `shutdown -r now` 將系統重新開機。

6.1.5 使用 Zypper 管理儲存庫

Zypper 的所有安裝或修補指令均依賴於一系列已知的儲存庫。若要列出系統可識別的所有儲存庫，請使用指令：

```
zypper repos
```

結果類似於以下輸出：

範例 6.1 Zypper—已知儲存庫的清單

#	Alias	Enabled	Refresh	Name
1	SUSE-Linux-Enterprise-Server 11-0	Yes	No	SUSE-Linux-Enterprise-Server 11-0
2	SLES-11-Updates	Yes	Yes	SLES 11 Online Updates
3	broadcomdrv	Yes	No	Broadcom Drivers

在各種指令中指定儲存庫時，可以使用 `zypper repos` 指令輸出的別名、URI 或儲存庫編號。儲存庫別名是儲存庫名稱的縮寫形式，用於儲存庫處理指令。請注意，修改儲存庫清單後，儲存庫的編號可能會發生變更。但別名永遠不會自行變更。

依預設，不會顯示儲存庫的詳細資料 (如 URI 或優先程度)。若要列出所有詳細資料，可以使用以下指令：

```
zypper repos -d
```

6.1.5.1 新增儲存庫

若要新增儲存庫，請執行

```
zypper addrepo URIalias
```

URI 可以是網際網路儲存庫、網路資源、目錄，也可以是 CD 或 DVD (如需詳細資料，請造訪 http://en.opensuse.org/openSUSE:Libzypp_URIs)。別名是儲存庫的縮寫與唯一識別碼。您可以隨意選擇，前提是它必須是唯一的。如果指定了已使用的別名，Zypper 會發出警告。

6.1.5.2 移除儲存庫

若要從清單中移除儲存庫，請使用 `zypper removerepo` 指令，加上要刪除的儲存庫別名或編號。例如，若要移除範例 6.1 「Zypper—已知儲存庫的清單」 [57頁] 中所列的第三個儲存庫，請使用以下指令：

```
zypper removerepo 3
```

6.1.5.3 修改儲存庫

`zypper modifyrepo` 可以啟用或停用儲存庫。您也可以使用此指令變更儲存庫的內容 (如重新整理行為、名稱或優先程度)。以下指令將啟用名為 `updates` 的儲存庫，開啟自動重新整理功能，並將優先程度設為 20：

```
zypper modifyrepo -er -p 20 'updates'
```

修改儲存庫不只是局限於一個儲存庫，您也可以對群組執行該操作：

- a：所有儲存庫
- l：本地儲存庫
- t：遠端儲存庫
- m 類型：某種類型的儲存庫 (其中類型可以是以下其中一種：http、https、ftp、cd、dvd、dir、file、cifs、smb、nfs、hd、iso)

若要重新命名儲存庫別名，請使用 `renamerepo` 指令。以下範例會將別名「Mozilla Firefox」變更為「firefox」：

```
zypper renamerepo 'Mozilla Firefox' firefox
```

6.1.6 使用 Zypper 查詢儲存庫和套件

Zypper 提供多種方法來查詢儲存庫或套件。若要獲得所有可用產品、模式、套件或修補程式的清單，請使用以下指令：

```
zypper products  
zypper patterns  
zypper packages  
zypper patches
```

若要在所有儲存庫中查詢某些套件，請使用 `search`。它可以對套件名稱、或(視情況)對套件摘要及描述進行搜尋。搜尋詞彙中可以使用萬用字元 `*` 和 `?`。依預設，搜尋不區分大小寫。

```
zypper search firefox          # simple search for "firefox"
zypper search "**fire*"        # using wildcards
zypper search -d fire          # also search in package descriptions and summaries
zypper search -u firefox       # only display packages not already installed
```

若要搜尋提供特殊功能的套件，請使用指令 `what-provides`。例如，如果您想瞭解哪個套件提供 `Perl` 模組 `SVN::Core`，請使用以下指令：

```
zypper what-provides 'perl(SVN::Core)'
```

若要查詢單個套件，請在 `info` 指令中使用準確的套件名稱做為引數。它會顯示套件的詳細資訊。如果還想顯示套件所需/推薦的項目，請使用選項 `--requires` 和 `--recommends`：

```
zypper info --requires MozillaFirefox
```

`what-provides` 套件類似於 `rpm -q --whatprovides` 套件，但是 `rpm` 只能查詢 **RPM** 資料庫(即所有已安裝套件的資料庫)。另外，`Zypper` 會告知您任何儲存庫功能的提供者，而不是只有已安裝的儲存庫。

6.1.7 設定 Zypper

`Zypper` 現隨附一個組態檔案，透過該檔案可永久變更 `Zypper` 的行為(整個系統範圍或僅針對特定使用者)。對於系統範圍的變更，請編輯 `/etc/zypp/zypper.conf`。對於特定使用者的變更，請編輯 `~/.zypper.conf`。如果 `~/.zypper.conf` 尚不存在，您可以使用 `/etc/zypp/zypper.conf` 做為範本：將其複製到 `~/.zypper.conf` 並根據喜好進行調整。如需有關可用選項的說明，請參閱檔案中的備註。

6.1.8 疑難排解

如果您在存取設定之儲存庫中的套件時遇到問題(例如，`zypper` 找不到特定套件，儘管您知道它存在於某個儲存庫中)，則可使用以下指令重新整理儲存庫：

```
zypper refresh
```

如果不起作用，請嘗試

```
zypper refresh -fdb
```

此指令會強制執行全面的重新整理和資料庫重建，包括強制下載原始中繼資料。

6.1.9 btrfs 檔案系統上的 Zypper 復原功能

如果在根分割區上使用 btrfs 檔案系統並且已安裝 snapper，則在提交檔案系統的變更以建立相應的檔案系統快照時，zypper 會自動呼叫 snapper (透過 snapper 所安裝的程序檔)。這些快照可用於回復 zypper 所做的所有變更。如需有關 snapper 的詳細資訊，請參閱 `man snapper`。

Zypper (和 YaST) 目前僅建立根檔案系統的快照，無法設定其他子磁碟區。此功能在預設檔案系統上無法使用。

6.2 RPM — 套件管理員

RPM (RPM 套件管理員) 用於管理軟體套件。主要指令為 `rpm` 及 `rpmbuild`。使用者、系統管理員和套件建立者可以在功能強大的 RPM 資料庫中查詢已安裝軟體的詳細資訊。

`rpm` 主要包括五種模式：安裝/解除安裝(或更新)軟體套件、重建 RPM 資料庫、查詢 RPM 基礎或個別的 RPM 歸檔、套件完整性檢查以及簽署套件。`rpmbuild` 可用於建立初始來源的可安裝套件。

可安裝的 RPM 歸檔以特殊二進位格式包裝封裝。這些歸檔由要安裝的程式檔和 `rpm` 在安裝期間用來設定軟體套件或儲存在 RPM 資料庫中供記錄之用的特定中繼資訊所組成。RPM 歸檔的副檔名通常為 `.rpm`。

提示：軟體開發套件

對於許多套件，軟體開發所需的元件(程式庫、標頭、Include 檔案等)分別封裝在單獨的套件中。只有在您想要自行編譯軟體(例如，最新的 GNOME 套件)時，才需要這些開發套件。根據副檔名 `-devel` 即可識別出這些套件，例如 `alsa-devel`、`gimp-devel` 和 `libkde4-devel` 套件。

6.2.1 確認套件驗證性

RPM 套件具有 GPG 簽名。若要驗證 RPM 套件的簽名，請使用指令 `rpm --checksig 套件-1.2.3.rpm` 來判斷套件是來自 Novell/SUSE，還是來自另一個可信任機構。特別建議在從網際網路更新套件時使用此指令。

6.2.2 管理套件：安裝、更新和解除安裝

一般而言，安裝 RPM 歸檔很簡單：`rpm -i package.rpm`。使用此指令可安裝套件，但是必須滿足其相依性條件，而且不能與其他套件衝突。如果 rpm 要求要安裝的套件必須符合相依性要求，會顯示錯誤訊息。RPM 資料庫會在背景中確認沒有產生衝突——特定的檔案僅可屬於一個套件。藉由選擇不同選項，您可以強迫 rpm 忽略這些預設，但只有進階使用者才可以這樣做。否則，會危及系統完整性，還可能危害更新系統的能力。

`-U` 或 `--upgrade` 以及 `-F` 或 `--freshen` 選項可用來更新套件 (例如，`rpm -F 套件.rpm`)。此指令會移除舊版的檔案，並立刻安裝新檔案。兩個版本之間的不同在於 `-U` 會安裝先前系統中沒有的套件，而 `-F` 僅更新先前安裝的套件。在更新時，rpm 會使用下列策略小心地更新組態檔：

- 如果系統管理員未變更組態檔，rpm 會安裝新版本的相應檔案。系統管理員不需要做任何動作。
- 如果系統管理員在更新之前變更了組態檔案，rpm 會將變更的檔案以副檔名 `.rpmorig` 或 `.rpmsave` (備份檔案) 儲存，並安裝新套件的版本，但此操作僅在最初安裝的檔案與新版本不同時才會執行。在這種情況下，請比較備份檔案 (`.rpmorig` 或 `.rpmsave`) 與新安裝的檔案，然後再對新檔案做一次變更。之後，請確定刪除所有 `.rpmorig` 和 `.rpmsave` 檔案以避免未來更新的問題。
- 如果組態檔已存在，*且*如果在 `.spec` 檔案中指定了 `noreplace` 標籤，便會出現 `.rpmnew` 檔案。

在更新之後，應該在比較完 `.rpmsave` 和 `.rpmnew` 之後將它們移除，才不會妨礙未來的更新。如果 RPM 資料庫之前無法辨識檔案，會指定 `.rpmorig` 副檔名。

否則，會使用 `.rpmsave`。換言之，`.rpmorig` 是在將外來格式更新為 **RPM** 後產生的。`.rpmsave` 是在將舊版 **RPM** 更新為新版 **RPM** 後產生的。`.rpmnew` 不會透露任何關於系統管理員是否曾對組態檔做過任何變更的資訊。可在 `/var/adm/rpmconfigcheck` 找到這些檔案的清單。部分組態檔 (如 `/etc/httpd/httpd.conf`) 不會覆寫以允許後續操作。

`-U` 切換參數的功能不不完全等同於使用 `-e` 選項進行解除安裝以及使用 `-i` 選項進行安裝。如果可能，請使用 `-U`。

若要移除套件，請輸入 `rpm -e 套件.rpm`，在不出現相依性問題的情況下刪除套件。只要其他應用程式還需要它，理論上無法刪除 `Tcl/Tk`，。即使是這種情況下，**RPM** 還是可從資料庫呼叫以得到協助。如果由於某種原因無法進行這樣的刪除操作 (即使不存在其他相依性問題)，或許可以使用選項 `--rebuilddb` 來重建 **RPM** 資料庫。

6.2.3 RPM 與修補程式

為了確保系統的操作安全性，必須經常在系統上安裝更新套件。以前，要除去套件中的錯誤，只能夠更換整個套件。在大型套件中，如果某些小檔案包含錯誤，就很容易出現這種情況。但是，**SUSE RPM** 提供在套件中安裝修補程式的功能。

最重要的考量可用 `pine` 當作範例：

修補程式 **RPM** 是否適用於我的系統？

若要進行檢查，首先請查詢安裝的套件版本。以 `pine` 為例，可使用指令

```
rpm -q pine
pine-4.44-188
```

然後檢查修補程式 **RPM** 是否適用於此版本的 `pine`：

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

此修補程式適用於三種不同版本的 **Pine**。範例中也列出安裝的版本，因此可安裝此修補程式。

修補程式會更換哪些檔案？

受到修補程式影響的檔案可在修補程式 **RPM** 中輕易地看出。rpm 參數 **-P** 可讓您選擇特殊的修補程式功能。可使用以下指令顯示檔案清單：

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

或者，如果已經安裝修補程式，可使用以下指令：

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

修補程式 **RPM** 如何安裝於系統中？

修補程式 **RPM** 可做為一般 **RPM** 使用。唯一的不同是必須已經安裝適合的 **RPM**。

系統中已經安裝哪個修補程式，是用於哪個套件版本？

使用指令 `rpm -qPa` 可顯示系統中已經安裝的所有修補程式清單。如果新系統中僅安裝一個修補程式 (如本範例)，則清單顯示如下：

```
rpm -qPa
pine-4.44-224
```

如果在日後，您想要知道原始安裝的套件版本，可在 **RPM** 資料庫中找到此資訊。以 `pine` 為例，可使用以下指令顯示此資訊：

```
rpm -q --basedon pine
pine = 4.44-188
```

可在 `rpm` 以及 `rpmbuild` 的 `man` 頁面中找到包括 **RPM** 修補程式功能的相關資訊。

注意：SUSE Linux Enterprise Server 的正式更新

為了儘可能減小更新的下載大小，SUSE Linux Enterprise Server 的正式更新以 **Delta RPM** 套件的形式提供，而不是以修補程式 **RPM** 的形式提供。如需詳細資料，請參閱第 6.2.4 節「Delta RPM 套件」[64頁]。

6.2.4 Delta RPM 套件

Delta RPM 套件包含舊版與新版 RPM 套件之間的差異。將 delta RPM 套用到舊版 RPM 上會產生一個全新的 RPM。但是您不需要取得舊版的 RPM，因為 delta RPM 也可以和安裝的 RPM 搭配使用。delta RPM 套件的大小比修補程式 RPM 還小，這一特點有利於透過網際網路傳送更新套件。缺點是使用 delta RPM 的更新作業會比一般或修補程式 RPM 消耗更多的 CPU 週期。

prepdeltarpm、writedeltarpm 以及 applydeltarpm 二進位檔屬於 delta RPM 套裝軟體 (deltarpm 套件) 的一部分，可協助您建立並套用 delta RPM 套件。使用下列指令可建立名為 new.delta.rpm 的 delta RPM。下列指令假設 old.rpm 和 new.rpm 都已存在：

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

最後，移除暫存工作檔案 old.cpio、new.cpio 以及 delta。

如果已經安裝舊套件，使用 applydeltarpm 即可從檔案系統重新建構新 RPM：

```
applydeltarpm new.delta.rpm new.rpm
```

若不要存取檔案系統，而要從舊 RPM 產生新 RPM，請使用 -r 選項：

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

如需技術詳細資訊，請參閱 /usr/share/doc/packages/deltarpm/README。

6.2.5 RPM 查詢

rpm 指令在使用 -q 選項時會啟動查詢，以便檢查 RPM 歸檔 (藉由新增選項 -p 的方式)，並查詢所安裝套件的 RPM 資料庫。有多個切換參數可用於指定所需的資訊類型。請參閱表格 6.1 「最重要的 RPM 查詢選項」 [64頁]。

表格 6.1 最重要的 RPM 查詢選項

-i	套件資訊
----	------

-l	檔案清單
-f FILE	查詢包含 <i>FILE</i> 檔案的套件 (完整的路徑必須以 <i>FILE</i> 指定)
-s	含有狀態資訊的檔案清單 (隱含 -l)
-d	只列出文件檔案 (隱含 -l)
-c	只列出組態檔案 (隱含 -l)
--dump	含有完整詳細資訊的檔案清單 (與 -l、-c 或 -d 一起搭配使用)
--provides	列出另一個套件可以使用 --requires 要求的套件功能
--requires、-R	套件所需的功能
--scripts	安裝程序檔 (預先安裝、後續安裝、解除安裝)

例如, `rpm -q -i wget` 指令可顯示如 範例 6.2 「`rpm -q -i wget`」[65頁] 中所顯示的資訊。

範例 6.2 `rpm -q -i wget`

```

Name       : wget                               Relocations: (not relocatable)
Version    : 1.11.4                             Vendor: openSUSE
Release    : 1.70                               Build Date: Sat 01 Aug 2009
09:49:48 CEST
Install Date: Thu 06 Aug 2009 14:53:24 CEST      Build Host: build18
Group      : Productivity/Networking/Web/Utilities Source RPM:
wget-1.11.4-1.70.src.rpm
Size       : 1525431                             License: GPL v3 or later
Signature  : RSA/8, Sat 01 Aug 2009 09:50:04 CEST, Key ID b88b2fd43dbdc284
Packager   : http://bugs.opensuse.org
URL        : http://www.gnu.org/software/wget/
Summary    : A Tool for Mirroring FTP and HTTP Servers
Description:
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

只有在您指定完整檔案名稱及完整路徑時，選項 `-f` 才會有作用。提供盡可能多的檔案名稱。例如，以下指令

```
rpm -q -f /bin/rpm /usr/bin/wget
```

會產生：

```
rpm-4.8.0-4.3.x86_64
wget-1.11.4-11.18.x86_64
```

如果只知道檔案名稱的一部分，可使用範例 6.3「搜尋套件的程序檔」[66頁] 中所示的外圍程序程序檔。執行時，可將部份檔案名稱當作參數傳給程序檔。

範例 6.3 搜尋套件的程序檔

```
#!/bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

`rpm -q --changelog rpm` 指令會顯示有關特定套件 (在此範例中為 `rpm` 套件) 變更資訊的詳細清單，並按日期排序。

藉由安裝的 **RPM** 資料庫協助，可執行驗證檢查。這些檢查可以使用 `-v`、`-y` 或 `--verify` 來啟動。使用此選項，`rpm` 可顯示從安裝開始，套件中所有變更過的檔案。`rpm` 使用八個字元的符號來提供下列變更的提示：

表格 6.2 RPM 驗證選項

S	MD5 檢查總數
s	檔案大小
L	符號連結
T	修改時間
D	主要和次要的設備編號
U	擁有者
G	群組

如果是組態檔，會印出字母 `c`。例如，若 `/etc/wgetrc` (`wget` 套件) 有變更：

```
rpm -V wget
S.5....T c /etc/wgetrc
```

RPM 資料庫的檔案放在 `/var/lib/rpm`。如果分割區 `/usr` 的大小為 1 GB，此資料庫將佔用 30 MB 左右的空間，尤其是在完整更新之後。如果資料庫遠大於預期，使用選項 `--rebuilddb` 來重建資料庫很有用。在執行之前，請備份舊的資料庫。`cron` 程序檔 `cron.daily` 會對資料庫做每日備份 (以 `gzip` 封裝)，並將備份儲存在 `/var/adm/backup/rpmdb` 中。副本數量由 `/etc/sysconfig/backup` 中的變數 `MAX_RPMDDB_BACKUPS` (預設值：5) 控制。單一備份的大小大約是 1 GB 的 `/usr` 備份成 1 MB。

6.2.6 安裝與編譯來源套件

所有來源套件均帶有副檔名 `.src.rpm` (來源 RPM)。

注意：安裝的來源套件

來源套件可從安裝媒體複製到硬碟，並用 **YaST** 解壓縮。但是，在套件管理員中，它們不會被標示為已安裝 (`[i]`)。這是因為來源套件沒有輸入 **RPM** 資料庫中。只有已安裝的作業系統軟體會列在 **RPM** 資料庫中。您在「安裝」來源套件時，僅會將原始程式碼新增到系統中。

在 `/usr/src/packages` 中必須可以找到 `rpm` 和 `rpmbuild` 的下列目錄 (除非您在如 `/etc/rpmrc` 的檔案中指定自定設定)：

SOURCES

用於原始來源 (`.tar.bz2` 或 `.tar.gz` 檔案等) 和配送特定調整 (大部份是 `.diff` 或 `.patch` 檔案)

SPECS

用於 `.spec` 檔案，和中繼 `Makefile` 相似，可控制 `build` 程序

BUILD

所有來源均在此目錄中解壓縮、修補和編譯

RPMS

儲存完整二進位套件的地方

SRPMS

此處為來源 RPM

當您使用 YaST 安裝來源套件時，所有需要的元件都會安裝在 `/usr/src/packages` 中：SOURCES 中的來源和調整以及 SPECS 中的相關 `.spec`。

警告

請不要對系統元件 (glibc、rpm、sysvinit 等) 進行試驗，因為這樣會危害系統的穩定性。

以下範例使用 `wget.src.rpm` 套件。安裝來源套件之後，會獲得類似下列清單中所列的檔案：

```
/usr/src/packages/SOURCES/wget-1.11.4.tar.bz2
/usr/src/packages/SOURCES/wgetrc.patch
/usr/src/packages/SPECS/wget.spec
```

`rpmbuild -b X /usr/src/packages/SPECS/wget.spec` 可開始編譯。
`X` 代表建立程序各種階段的萬用字元 (請參閱 `--help` 的輸出或 RPM 文件以取得詳細資訊)。以下僅為簡略的說明：

`-bp`

在 `/usr/src/packages/BUILD` 中準備來源：解壓縮和修補。

`-bc`

執行與 `-bp` 相同動作，但是會額外編譯。

`-bi`

執行與 `-bp` 相同的動作，但是會額外安裝建立的軟體。警告：如果套件不支援 **BuildRoot** 功能，您可能會覆寫組態檔。

`-bb`

執行與 `-bi` 相同的動作，但是會額外建立二進位套件。如果編譯成功，二進位應該在 `/usr/src/packages/RPMS`。

-ba

執行與 -bb 相同的動作，但是會額外建立來源 RPM。如果編譯成功，二進位應該在 /usr/src/packages/SRPMS。

--short-circuit

略過部分步驟。

現在可使用 rpm -i (最好使用 rpm -U) 來安裝所建立的二進位 RPM。使用 rpm 來安裝會讓它出現在 RPM 資料庫中。

6.2.7 以 build 編譯 RPM 套件

許多套件中都包含不想要的檔案，它們會在 build 程序中增到執行系統中，因為導致危險產生。若要避免此狀況，可以使用 build，它會建立要在其中建置套件的定義環境。若要建立此 chroot 環境，必須提供 build 程序檔與完整的套件樹狀結構。此樹狀結構可在硬碟上、透過 NFS 或從 DVD 取得。用 build --rpms directory 設定位置。與 rpm 不同，build 指令在來源目錄中尋找 .spec 檔。若要以掛接在系統的 /media/dvd 之下的 DVD 建立 wget (如上面的範例)，請以 root 身分執行下列指令：

```
cd /usr/src/packages/SOURCES/  
mv ../SPECS/wget.spec .  
build --rpms /media/dvd/suse/ wget.spec
```

之後，系統便會在 /var/tmp/build-root 中建立一個最小的環境。套件將於此環境中建立。完成時，結果套件位於 /var/tmp/build-root/usr/src/packages/RPMS 中。

build 程序檔可提供數個額外選項。例如，讓程序檔偏好使用您自己的 RPM、省略建置環境的啟始化，或將 rpm 指令限制在上述某個階段。可使用 build --help 以及參閱 build man 頁面來存取其他資訊。

6.2.8 RPM 歸檔和 RPM 資料庫工具

Midnight Commander (mc) 可顯示 RPM 歸檔的內容，並複製部分內容。它將歸檔以虛擬檔案系統呈現，提供 Midnight Commander 的所有常見功能表選項。使用 F3 可顯示 HEADER。使用游標和 Enter 可檢視歸檔結構。使用 F5 可複製歸檔元件。

具有完整功能的套件管理員是以 YaST 模組的方式提供。如需詳細資料，請參閱第 9 章「安裝或移除軟體」(↑部署指南)。

Bash 和 Bash 程序檔

如今，有許多人使用具有圖形使用者介面 (GUI) 的電腦，例如 KDE 或 GNOME 介面。儘管這些介面提供了很多功能，但使用它們執行自動任務時，還是會有限制。外圍程序是 GUI 的有效補充，本章概述了外圍程序 (以 Bash 為例) 的一些方面。

7.1 什麼是「外圍程序」？

一般而言，*外圍程序*就是 Bash (Bourne again Shell)。本章中提及的「外圍程序」指的是 Bash。實際上，可用的外圍程序不止 Bash (還有 ash、csh、ksh、zsh、...)，每個外圍程序都包含不同的功能和特性。如需有關其他外圍程序的詳細資訊，請在 YaST 中搜尋*外圍程序*。

7.1.1 瞭解 Bash 組態檔案

外圍程序可啟用為：

1. **互動式登入外圍程序** 使用 `--login` 選項啟用 Bash 以登入機器，或使用 SSH 登入遠端機器時會採用這種方式。
2. **「一般」互動式外圍程序** 啟動 xterm、konsole、gnome-terminal 或類似工具時通常會採用這種方式。
3. **非互動式外圍程序** 在指令行中呼叫外圍程序程序檔時會採用這種方式。

系統會讀取不同的組態檔案，視所使用的外圍程序類型而定。下面的表格顯示了登入與非登入外圍程序組態檔案。

表格 7.1 登入外圍程序的 *Bash* 組態檔案

檔案	描述
<code>/etc/profile</code>	請勿修改此檔案，否則您的修改在下次更新時可能會被破壞！
<code>/etc/profile.local</code>	擴充 <code>/etc/profile</code> 時使用此檔案
<code>/etc/profile.d/</code>	包含特定程式的系統級組態檔案
<code>~/.profile</code>	在此處插入登入外圍程序的使用者特定組態

表格 7.2 非登入外圍程序的 *Bash* 組態檔案

<code>/etc/bash.bashrc</code>	請勿修改此檔案，否則您的修改在下次更新時可能會被破壞！
<code>/etc/bash.bashrc.local</code>	使用此檔案只能插入 Bash 的系統級修改
<code>~/.bashrc</code>	在此處插入使用者特定的組態

此外，*Bash* 還使用其他檔案：

表格 7.3 *Bash* 的特殊檔案

檔案	描述
<code>~/.bash_history</code>	包含您鍵入的所有指令清單
<code>~/.bash_logout</code>	登出時執行

7.1.2 目錄結構

下表概述了 Linux 系統中最重要的高層級目錄。下列清單中提供了關於目錄與重要子目錄的更多詳細資訊。

表格 7.4 標準目錄網路樹的綜覽

目錄	內容
/	根目錄 — 目錄樹的起點。
/bin	基本的二進位檔案，例如系統管理員與一般使用者都需要使用的指令。通常還包含 Bash 等外圍程序。
/boot	開機載入程式的靜態檔案。
/dev	存取主機特定設備所需的檔案。
/etc	主機特定系統的組態檔案。
/home	存放系統中所有擁有帳戶之使用者的主目錄。但是，root 的主目錄不在 /home 中，而是位於 /root 內。
/lib	基本的共享程式庫與核心模組。
/media	抽取式媒體的定點。
/mnt	用於暫時掛接檔案系統的定點。
/opt	附加應用程式軟體套件。
/root	超級使用者 root 的主目錄。
/sbin	基本的系統二進位檔案。

目錄	內容
/srv	系統所提供之服務的資料。
/tmp	暫存檔案。
/usr	包含唯讀資料的次要階層。
/var	可變資料，例如記錄檔案。
/windows	僅當系統中同時安裝了 Microsoft Windows* 與 Linux 才可以使用。包含 Windows 資料。

以下清單提供了更多詳細資訊，以及目錄中包含的檔案與子目錄的一些範例：

/bin

包含 root 及其他使用者可能會使用的基本外圍程序指令。這些指令包括 ls、mkdir、cp、mv、rm 以及 rmdir。/bin 還包含 SUSE Linux Enterprise Server 中的預設外圍程序 Bash。

/boot

包含開機所需的資料，例如開機載入程式、核心及核心開始執行使用者模式程式之前所使用的其他資料。

/dev

存放代表硬體元件的設備檔案。

/etc

包含控制 X Window System 等程式的操作的本地組態檔案。/etc/init.d 子目錄包含開機期間執行的程序檔。

/home/使用者名稱

存放系統中每個擁有帳戶之使用者的個人資料。只有檔案擁有者或系統管理員才能修改位於此處的檔案。依預設，電子郵件目錄與個人桌面組態以隱藏檔案與目錄的形式存放於此。KDE 使用者可在 .kde4 中找到其桌面系統的個人組態資料，而 GNOME 使用者可在 .gconf 中找到該資料。

注意：網路環境中的主目錄

如果您是在網路環境中工作，您的主目錄可能會對應至檔案系統中 `/home` 以外的目錄。

`/lib`

包含啟動系統及執行根檔案系統中指令所需的基本共享程式庫。在 Windows 中，對應的共享程式庫為 DLL 檔案。

`/media`

包含 CD-ROM、USB 晶片組及數位相機 (若使用 USB) 等抽取式媒體的掛接點。`/media` 通常存放系統硬碟之外的任何類型磁碟機或光碟機。抽取式媒體插入或連接到系統並進行掛接後，您就可以從此處存取該媒體。

`/mnt`

此目錄提供了暫時掛接之檔案系統的定點。`root` 可在此處掛接檔案系統。

`/opt`

為安裝協力廠商軟體而保留。這裡有選擇性軟體與大型附加程式套件。

`/root`

`root` 使用者的主目錄。這裡有 `root` 的個人資料。

`/sbin`

如 `s` 所指示，此目錄存放適用於超級使用者的公用程式。`/sbin` 不僅包含 `/bin` 中的二進位檔案，還包含啟動、還原及復原系統所必需的二進位檔案。

`/srv`

存放系統所提供之服務的資料，例如 FTP 與 HTTP。

`/tmp`

需要檔案暫時儲存區的程式會使用此目錄。

重要：開機時清理 `/tmp`

系統重新開機後，先前儲存於 `/tmp` 中的資料無法保證仍然存在。這視情況而定，例如，取決於 `/etc/sysconfig/cron` 中的設定。

`/usr`

`/usr` 與使用者無關，而是 UNIX 系統資源 (UNIX system resource) 的縮寫。`/usr` 中的資料是靜態的唯讀資料，可依照檔案系統階層標準 (Filesystem Hierarchy Standard, FHS) 在不同的主機之間共享。此目錄包含所有應用程式，並且會在檔案系統中建立次要階層。KDE4 與 GNOME 也位於此處。`/usr` 存放了許多子目錄，例如 `/usr/bin`、`/usr/sbin`、`/usr/local` 以及 `/usr/share/doc`。

`/usr/bin`

包含一般情況下可存取的程式。

`/usr/sbin`

包含為系統管理員保留的程式，例如修復功能。

`/usr/local`

在此目錄中，系統管理員可安裝獨立於套裝作業系統的本地延伸。

`/usr/share/doc`

存放系統的各種文件檔案與版本說明。在 `manual` 子目錄中，可找到此手冊的線上版本。如果安裝了多種語言，此目錄可能會包含不同語言的手冊版本。

在 `packages` 內，可找到系統上安裝之軟體套件所包含的文件。每個套件都有一個子目錄 `/usr/share/doc/packages/套件名稱`，該目錄通常用於存放套件的讀我檔案，有時也會存放範例、組態檔案或其他程序檔。

如果系統中安裝了 HOWTO，`/usr/share/doc` 還會包含 `howto` 子目錄，其中有許多與 Linux 軟體設定及操作相關之任務的其他文件。

`/var`

`/usr` 存放的是靜態唯讀資料，而 `/var` 存放的是系統操作時寫入的資料，因此為可變資料，例如記錄檔案或多工緩衝處理資料。如需 `/var/log/` 中包含之最重要記錄檔的綜覽，請參閱表格 35.1 「記錄檔案」 [513頁]。

7.2 寫入外圍程序程序檔

使用外圍程序程序檔可以方便地完成各種任務：收集資料、搜尋文字中的單字或片語，以及執行很多其他有用的操作。以下範例顯示了一個列印文字的小型外圍程序程序檔：

範例 7.1 列印文字的外圍程序程序檔

```
#!/bin/sh ❶  
# Output the following line: ❷  
echo "Hello World" ❸
```

- ❶ 第一行以 *Shebang* 字元(#!)開頭，指出此檔案為程序檔。程序檔透過 *Shebang* 後面指定的解譯器執行，在此例中為 `/bin/sh`。
- ❷ 第二行為備註，以 `#` 開頭。建議將較為複雜的行設為備註，以便記住其作用。
- ❸ 第三行使用內建指令 `echo` 列印相應的文字。

您需要符合一些先決條件才能執行此程序檔：

1. 每個程序檔都應包含一行 *Shebang* 行 (上面的範例即是如此。)如果程序檔未包含此行，您需要手動呼叫直譯器。
2. 您可以將程序檔儲存於任何位置。但是，最好將其儲存於外圍程序可以找到的目錄中。外圍程序中的搜尋路徑由環境變數 `PATH` 決定。一般使用者通常沒有寫入 `/usr/bin` 的權限。因此，建議將程序檔儲存在使用者目錄 `~/bin/` 中。以上範例名為 `hello.sh`。
3. 程序檔需要執行權限。使用下列指令設定權限：

```
chmod +x ~/bin/hello.sh
```

如果滿足了上述所有先決條件，便可以按以下方式執行程序檔：

1. **絕對路徑** 執行程序檔時可以使用絕對路徑。在此例中為 `~/bin/hello.sh`。
2. **任何位置** 如果 `PATH` 環境變數包含程序檔所在的目錄，則只需使用 `hello.sh` 便可執行程序檔。

7.3 重新指向指令事件

每條指令可以使用三個通道用於輸入或輸出：

- **標準輸出** 這是預設的輸出通道。指令進行列印時會使用標準輸出通道。
- **標準輸入** 如果指令需要使用者或其他指令的輸入，將會使用此通道。
- **標準錯誤** 指令使用此通道報告錯誤。

要重新指向這些通道，可以使用以下幾種方式：

指令 > 檔案

將指令輸出儲存為檔案，現有的檔案將會刪除。例如，ls 指令將輸出寫入到檔案 listing.txt 中：

```
ls > listing.txt
```

指令 >> 檔案

將指令輸出附加至檔案。例如，ls 指令將輸出附加至檔案 listing.txt 中：

```
ls >> listing.txt
```

指令 < 檔案

讀取檔案，將其做為指定指令的輸入。例如，read 指令會將檔案內容讀取至變數中：

```
read a < foo
```

指令1 | 指令2

將左邊指令的輸出重新指向為右邊指令的輸入。例如，cat 指令會輸出 /proc/cpuinfo 檔案的內容。再由 grep 使用此輸出內容單獨過濾出包含 cpu 的行：

```
cat /proc/cpuinfo | grep cpu
```

每個通道都有一個**檔案描述子**：0 (零) 代表標準輸入，1 代表標準輸出，2 代表標準錯誤。您可以將此檔案描述子插入到 < 或 > 字元的前面。例如，下行將搜尋以 foo 開始的檔案，但透過將檔案重新指向至 /dev/null 隱藏了錯誤：

```
find / -name "foo*" 2>/dev/null
```


7.4 使用別名

別名為一或多條指令的簡短定義。別名的語法為：

```
alias NAME=DEFINITION
```

例如，下面這一行定義了別名 `lt`，它會輸出一份較長的清單 (選項 `-l`)，按修改時間排序 (`-t`)，並按相反順序進行列印 (`-r`)：

```
alias lt='ls -ltr'
```

要檢視所有的別名定義，請使用 `alias`。若要移除別名，請使用 `unalias` 和對應的別名名稱。

7.5 使用 Bash 中的變數

外圍程序變數可以是全域變數或本地變數。您可以在所有外圍程序中存取全域變數或環境變數。與此相反，本地變數僅顯示於目前的外圍程序中。

要檢視所有環境變數，請使用 `printenv` 指令。如需瞭解變數的值，則將變數名稱做為引數插入：

```
printenv PATH
```

無論是全域變數還是本地變數，都可以使用 `echo` 進行檢視：

```
echo $PATH
```

要設定本地變數，請使用變數名稱，後面跟上等號，再跟上值：

```
PROJECT="SLED"
```

請不要在等號兩邊插入空格，否則將會出錯。要設定環境變數，請使用 `export`：

```
export NAME="tux"
```

若要移除變數，請使用 `unset`：

```
unset NAME
```

下表包含了部分可在外圍程序程序檔中使用的常用環境變數：

表格 7.5 有用的環境變數

HOME	目前使用者的主目錄
HOST	目前的主機名稱
LANG	工具當地化以後，會使用此環境變數指定的語言。也可將英語設定為 C
PATH	外圍程序的搜尋路徑，即以冒號分隔的目錄清單
PS1	指定在每條指令前列印的一般提示
PS2	指定執行多行指令時列印的輔助提示
PWD	目前的工作目錄
USER	目前的使用者

7.5.1 使用引數變數

例如，如果您有程序檔 `foo.sh`，可以按以下格式執行該程序檔：

```
foo.sh "Tux Penguin" 2000
```

若要存取傳送至程序檔的所有引數，需要使用位置參數。`$1` 代表第一個引數的位置參數，`$2` 代表第二個引數的位置參數，依此類推。最多可以使用九個參數。要獲取程序檔名稱，請使用 `$0`。

下面的程序檔 `foo.sh` 可列印從 1 到 4 的所有引數：

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

如果您使用以上引數執行此程序檔，所得結果為：

```
"Tux Penguin" "2000" "" ""
```

7.5.2 使用變數替代項

變數替代項會從左側或右側將模式套用至變數內容。以下清單包含了可用的語法格式：

`${VAR#pattern}`

從左側移除最短的相符項：

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##pattern}`

從左側移除最長的相符項：

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

`${VAR%pattern}`

從右側移除最短的相符項：

```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%pattern}`

從右側移除最長的相符項：

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

`${VAR/pattern_1/pattern_2}`

使用 *pattern_2* 替代 *pattern_1* 中 *VAR* 的內容：

```
file=/home/tux/book/book.tar.bz2
echo ${file/tux/wilber}
/home/wilber/book/book.tar.bz2
```

7.6 分組與組合指令

外圍程序允許您組合及分組指令，以便按條件執行。每條指令都會傳回決定操作成功與否的離開碼。如果為0(零)，則說明指令成功，任何其他離開碼都代表特定於指令的錯誤。

以下清單顯示了可對指令分組的方式：

指令1 ; 指令2

以順序執行指令。不檢查離開碼。下行透過 `cat` 顯示檔案內容，然後透過 `ls` 列印其檔案內容，而不管其離開碼為何：

```
cat filelist.txt ; ls -l filelist.txt
```

指令1 && 指令2

如果左邊的指令成功，即會執行右邊的指令(邏輯「與」)。下行顯示檔案內容，並且僅在前面的指令成功時才會列印其檔案內容 (將其與此清單中的上一個項目進行比較)：

```
cat filelist.txt && ls -l filelist.txt
```

指令1 || 指令2

如果左邊的指令失敗，即會執行右邊的指令(邏輯「或」)。下行將只會在於 `/home/tux/foo` 中建立目錄失敗時，才會在 `/home/wilber/bar` 中建立目錄：

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

```
funcname() { ... }
```

建立外圍程序函數。可以使用位置參數存取其引數。下行定義了可列印較短訊息的函數 `hello`：

```
hello() { echo "Hello $1"; }
```

可以按以下格式呼叫此函數：

```
hello Tux
```

將會列印：

```
Hello Tux
```

7.7 使用通用流程建構元

為了控制程序檔的流程，外圍程序包含 `while`、`if`、`for` 及 `case` 建構元。

7.7.1 If 控制指令

`If` 指令用於檢查運算式。例如，以下程式碼將測試目前的使用者是否為 `Tux`：

```
if test $USER = "tux"; then
    echo "Hello Tux."
else
    echo "You are not Tux."
fi
```

測試運算式可以很複雜，也可以很簡單。下面的運算式會檢查檔案 `foo.txt` 是否存在：

```
if test -e /tmp/foo.txt ;
then
    echo "Found foo.txt"
fi
```

測試運算式也可以縮寫到角括弧中：

```
if [ -e /tmp/foo.txt ] ; then
    echo "Found foo.txt"
fi
```

如需更多有用的運算式，請參閱<http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lsst/ch03sec02.html>。

7.7.2 使用 For 指令建立迴路

`for` 迴路可讓您對一組項目執行指令。例如，以下程式碼會列印目前目錄中關於 `PNG` 檔案的部分資訊：

```
for i in *.png; do
    ls -l $i
done
```

7.8 如需更多資訊

`man` 頁面 `man sh` 中提供了關於 `Bash` 的重要資訊。以下清單中提供了更多關於此主題的資訊：

- <http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html> — `Bash` 初級使用者指南
- <http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html> — `BASH` 程式設計 - 方法介紹
- <http://tldp.org/LDP/abs/html/index.html> — `Bash` - 程序檔進階指南
- <http://www.grymoire.com/Unix/Sh.html> — `Sh` - `Bourne` 外圍程序

II. 系統

64 位元系統環境的 32 位元和 64 位元應用程式

8

SUSE® Linux Enterprise Server 可用於多種 64 位元平台。但這並不表示所有包含的應用程式都已移植到 64 位元平台。SUSE Linux Enterprise Server 支援在 64 位元系統環境中使用 32 位元應用程式。本章概述了有關 SUSE Linux Enterprise Server 在 64 位元平台下的支援方式。它說明 32 位元應用程式的執行方式 (執行期間支援) 以及如何編譯 32 位元應用程式，讓它們在 32 位元和 64 位元兩種系統環境都可執行。另外，您可找到關於核心 API 和 32 位元應用程式如何在 64 位元核心下執行的相關資訊。

適用於 ia64、ppc64、System z 及 x86_64 等 64 位元平台的 SUSE Linux Enterprise Server，可讓現有的 32 位元應用程式「不需額外的設定即可在 64 位元環境中執行。」對應的 32 位元平台為 x86 (對應 ia64)、ppc (對應 ppc64)、x86 (對應 x86_64)。這項支援意謂您可以繼續使用偏好的 32 位元應用程式，無需等到對應的 64 位元連接埠上市。目前的 ppc64 系統是以 32 位元模式執行大部分應用程式，不過您可以執行 64 位元應用程式。

8.1 執行期間支援

重要：不同應用程式版本之間的衝突

如果應用程式有 32 位元和 64 位元兩種版本，同時安裝二種版本，一定會發生問題。在這種狀況下，可在兩種版本中選定一種來安裝並使用。

此規則的一個例外是 PAM (可插入驗證模組)。SUSE Linux Enterprise Server 在驗證程序中將 PAM 當做使用者與應用程式之間的溝通層。在另外還可執行 32 位元應用程式的 64 位元作業系統上，一律要安裝兩個版本的 PAM 模組。

要正確執行，每一個應用程式都需要一些程式庫。不幸的是，這些程式庫的 32 位元和 64 位元版本，名稱都一樣。它們必須透過其他方法來區分彼此。

要保留與 32 位元版本的相容性，程式庫儲存在系統中的位置，與在 32 位元環境中的位置相同。在 32 位元和 64 位元環境中，`libc.so.6` 的 32 位元版本都位於 `/lib/libc.so.6`。

所有 64 位元程式庫和物件檔案都位於名為 `lib64` 的目錄。以往儲存在 `/lib` 和 `/usr/lib` 下的 64 位元物件檔案，現在放在 `/lib64` 和 `/usr/lib64` 目錄下。這表示在 `/lib` 和 `/usr/lib` 之下，有預留空間給 32 位元程式庫使用，因而兩種版本的檔案名稱能夠保持不變。

32 位元 `/lib` 目錄的子目錄，如果包含不取決於字數的資料內容，則不會移動。此配置與 LSB (Linux Standards Base) 以及 FHS (File System Hierarchy Standard) 相容。

► **ipf:** ia64 的 64 位元程式庫位於標準 `lib` 目錄中，系統沒有 `lib64` 目錄，也沒有 `lib32` 目錄。ia64 會以模擬方式執行 32 位元 x86 程式碼。一組基本程式庫會安裝在 `/emul/ia32-linux/lib` 和 `/emul/ia32-linux/usr/lib` 中。◀

8.2 軟體開發

所有 64 位元架構都支援 64 位元物件的開發。對 32 位元編譯的支援層級需視結構而定。以下為 GCC (GNU Compiler Collection) 和 Binutil 的工具鏈的各種執行實作選項，包括組合器 `as` 以及連結器 `ld`：

Biarch 編譯器

Biarch 開發工具鏈可以產生 32 位元和 64 位元二種物件。Biarch 開發工具鏈可以產生 32 位元和 64 位元物件。幾乎所有平台都預設支援 64 位元物件的編譯。如果使用特殊旗標，就可以產生 32 位元物件。此特殊旗標是適用於 GCC 的 `-m32`。Binutil 的旗標視結構而定，但是 GCC 會將正確的旗標傳送至連結器和組合器。Biarch 開發工具鏈目前可用於 amd64 (支援 x86 和 amd64 說明的開發)、System z 及 ppc64。32 位元物件一般是建立在 ppc64 平台上。要產生 64 位元物件，必須使用 `-m64` 旗標。

不支援

SUSE Linux Enterprise Server 並不支援在所有平台上直接開發 32 位元軟體。若要在 ia64 底下開發 x86 應用程式，請使用與 SUSE Linux Enterprise Server 對應的 32 位元版本。

所有標題檔案必須使用與結構無關的形式來編寫。安裝的 32 位元和 64 位元程式庫，必須有一個與已安裝標頭檔案相符的 API (應用程式設計介面)。一般的 SUSE Linux Enterprise Server 環境是根據此原則而設計。對於手動更新的程式庫，請自行解決這些問題。

8.3 Biarch 平台的軟體編譯

若要在 biarch 結構上，為其他結構開發二進位程式，必須為第二個結構額外安裝相關程式庫。如果第二個結構是 32 位元結構，這些套件稱為 `rpmname-32bit` 或 `rpmname-x86` (針對 ia64)；如果第二個結構是 64 位元結構，則套件稱為 `rpmname-64bit`。您還需要 `rpmname-devel` 套件的各個標頭和程式庫，以及 `rpmname-devel-32bit` 或 `rpmname-devel-64bit` 之第二個結構的開發程式庫。

例如，若要編譯一個使用 `libaio` 的程式，而所在系統的第二個結構是 32 位元結構 (`x86_64` 或 `System z`)，您需要以下 RPM：

`libaio-32bit`

32 位元執行期間套件

`libaio-devel-32bit`

32 位元開發的標題和程式庫

`libaio`

64 位元執行期間套件

`libaio-devel`

64 位元開發標題和程式庫

大部份開放原始碼程式使用的程式組態是以 `autoconf` 為基礎。若要使用 `autoconf` 為第二個結構設定程式，請覆寫 `autoconf` 的一般編譯器和連結器設定，方法是執行包含其他環境變數的 `configure` 程序檔。

以下範例參考第二個結構為 x86 的 x86_64 系統：以 ppc 為第二個結構的 ppc64，其範例都與此類似。此範例不適用於無法在其中建立 32 位元套件的 ia64。

1 使用 32 位元編譯器：

```
CC="gcc -m32"
```

2 指示連結器處理 32 位元物件 (務必使用 gcc 做為連結器前端)：

```
LD="gcc -m32"
```

3 設定組合器來產生 32 位元物件：

```
AS="gcc -c -m32"
```

4 指定連結器旗標，例如 32 位元程式庫的位置：

```
LDFLAGS="-L/usr/lib"
```

5 指定 32 位元目標代碼程式庫的位置：

```
--libdir=/usr/lib
```

6 指定 32 位元 X 程式庫的位置：

```
--x-libraries=/usr/lib
```

並非每一個程式都需要所有這些變數。將它們配合各程式使用。

以下是在 x86_64、ppc64 或 System z 上編譯原生 32 位元應用程式的 configure 呼叫範例：

```
CC="gcc -m32"  
LDFLAGS="-L/usr/lib;"  
./configure --prefix=/usr --libdir=/usr/lib --x-libraries=/usr/lib  
make  
make install
```

8.4 核心規格

x86_64、ppc_64 和 System z 適用的 64 位元核心，可提供 64 位元和 32 位元兩種核心 ABI (應用程式二進位介面)。後者與相對應 32 位元核心的 ABI 是相同

的。這表示 32 位元應用程式可以用與 32 位元核心溝通相同的方式，來與 64 位元核心溝通。

32 位元系統模擬的 64 位元核心呼叫，不支援系統程式使用的所有 API。這要視平台而定。基於這個原因，少數應用程式 (例如 `lspci`) 必須進行編譯編譯為 64 位元程式，才能在非 `ppc64` 平台上正確運作。在 IBM System z 上，並非所有 `ioctl`s 都可用於 32 位元核心 ABI 中。

64 位元核心只可以載入為此核心特別編譯的 64 位元核心模組。它無法使用 32 位元核心模組。

提示：核心可載入模組

部份應用程式需要個別的核心可載入式模組。如果您想在 64 位元系統環境使用這種 32 位元應用程式，請洽詢此應用程式的提供者以及 SUSE，確定是否可以取得此模組的核心可載入式模組的 64 位元版本以及核心 API 的 32 位元編譯版本。

啟動及設定 Linux 系統

啟動 Linux 系統涉及多個元件。硬體自身是由 BIOS 啟動的。BIOS 會藉由開機載入程式啟動核心。此後，關於 `init` 和執行層級的開機程序完全由作業系統控制。憑藉執行層級的概念，您可以保持日常使用的設定，以及對系統執行維護任務。

9.1 Linux 開機程序

Linux 開機程序由數個階段所組成，每個階段分別由不同的元件所代表。以下清單簡短概述開機程序，以及所有相關主要元件的功能。

1. **BIOS** 開啟電腦之後，BIOS 會啟動初始化螢幕和鍵盤並測試主記憶體。在此階段中，機器不會存取大量儲存媒體。接著，會從 CMOS 值載入目前日期、時間和最重要的周邊。識別第一個硬碟及其規格之後，系統控制將會從 BIOS 轉到開機載入程式。如果 BIOS 支援網路開機，則也可以設定提供開機載入程式的開機伺服器。在 x86 系統上，需要 PXE 開機。其他架構通常使用 BOOTP 通訊協定來取得開機載入程式。
2. **開機載入程式** 第一顆硬碟的第一個實體 512 位元組資料磁區，會載入主要記憶體。接著，在此磁區開頭的開機載入程式會接管開機程序。開機載入程式執行的指令，決定其他部份的開機程序。因此，第一個硬碟的前 512 位元組是主開機紀錄(MBR)。然後，開機載入程式會將控制權交給實際的作業系統，在這裡是指 Linux 核心。如需 Linux 開機載入程式 GRUB 的詳細資訊，請參閱第 10 章「開機載入程式 GRUB」[109頁]。進行網路開機時，BIOS 會充當開機載入程式。它會從開機伺服器取得要啟動的影像，然後啟動系統。這與本地硬碟完全無關。

3. **核心和 `initramfs`** 為了送出系統控制權，開機載入程式會將核心和初始 RAM 式檔案系統 (`initramfs`) 兩者都載入記憶體。核心可以直接使用 `initramfs` 的內容。`initramfs` 包含一個名為 `init` 的小執行檔，該執行檔可以處理實際根目錄檔案系統的掛接。若需要特殊的硬體驅動程式才能存取大量儲存，那一定就是 `initramfs` 了。如需 `initramfs` 的詳細資訊，請參閱第 9.1.1 節「`initramfs`」[94頁]。如果系統沒有本地硬碟，`initramfs` 必須向核心提供根目錄檔案系統。這可以藉由 iSCSI 或 SAN 這類網路區塊設備來完成，但也可以使用 NFS 做為根設備。
4. **`initramfs` 上的 `init`** 本程式將執行掛接適當根目錄檔案系統所需執行的全部動作，例如提供所需檔案系統的核心功能，以及為 `udev` 提供適用於大量儲存控制器的設備驅動程式。找到根目錄檔案系統後，將會檢查是否有錯誤並進行掛接。若掛接成功，系統會清理 `initramfs` 並執行根目錄檔案系統上的 `init` 程式。如需有關 `init` 的詳細資訊，請參閱第 9.1.2 節「`initramfs` 上的 `init`」[95頁]。如需有關 `udev` 的詳細資訊，請參閱第 14 章「使用 `udev` 進行動態核心設備管理」[167頁]。
5. **`init`** `init` 會透過幾個提供不同功能的不同層級來處理實際的系統開機作業。第 9.2 節「`init` 程序」[97頁] 中對 `init` 做了介紹。

9.1.1 `initramfs`

`initramfs` 是一個小型 `cpio` 歸檔，可由核心載入 RAM 磁碟。在實際根目錄檔案系統掛接之前，它提供可讓程式執行的最小 Linux 環境。BIOS 常式會將這個精簡的 Linux 環境載入記憶體，該環境只要求記憶體空間足夠大，此外沒有特定的硬體要求。`initramfs` 在任何情況下都必須提供一個名為 `init` 的可執行檔，由它來在根目錄檔案系統上執行實際的 `init` 程式，如此開機程序才可繼續進行。

在根目錄檔案系統能夠掛接以及作業系統可以啟動之前，核心需要相應的驅動程式才能存取根目錄檔案系統所在的設備。這些驅動程式可能包含特定類型硬碟的特殊驅動程式，或者甚至包含存取網路檔案系統的網路驅動程式。

`initramfs` 上的 `init` 可以載入根目錄檔案系統所需的模組。當模組載入之後，`udev` 便會為 `initramfs` 提供所需的設備。在後來的開機程序中，變更根目錄檔案系統後，必須重新產生這些設備。結合使用 `boot.udev` 和指令 `udevtrigger` 可以實現此目的。

如果您要變更已安裝系統上的硬體 (例如硬碟)，而開機時此硬體需要核心中存在與原先不同的驅動程式，那麼您就必須更新 `initramfs`。此過程與更新其前任 (`init`) 一樣，需要透過呼叫 `mkinitrd` 來完成。如果不使用任何引數呼叫 `mkinitrd`，將會建立一個 `initramfs`。呼叫 `mkinitrd -R` 則會建立一個 `init`。在 SUSE® Linux Enterprise Server 中，`/etc/sysconfig/kernel` 中的變數 `INITRD_MODULES` 會指定要載入的模組。安裝之後，此變數會自動設定為正確值。模組會確實依據它們在 `INITRD_MODULES` 中出現的順序來載入。如果您不依賴於 `/dev/sd?` 設備檔案的正確設定，這一點將無關緊要。不過，在目前系統中，您也可以使用 `/dev/disk/` 下以幾個不同子目錄分類的設備檔案，這些子目錄的名稱為 `by-id`、`by-path` 和 `by-uuid`，這些目錄總是代表相同磁碟。在安裝時也可以透過指定相應的掛接選項來實現此目的。

重要：更新 `initramfs` 或 `init`

開機載入程式將採用與核心相同的方式載入 `initramfs` 或 `init`。更新 `initramfs` 或 `init` 之後不需要重新安裝 `GRUB`，因為開機時 `GRUB` 會在目錄中搜尋適當的檔案。

9.1.2 `initramfs` 上的 `init`

`initramfs` 上的 `init` 主要用途是為掛接以及存取實際根目錄檔案系統做好準備。根據您的系統組態，`init` 負責下列任務。

載入核心模組

存取您電腦的硬體元件可能需要特殊的驅動程式 (最重要的元件是硬碟)，具體取決於您的硬體組態。若要存取最終的根目錄檔案系統，核心需載入適當的檔案系統驅動程式。

提供區塊特殊檔案

對於每個載入的模組，核心均會產生設備事件。udev 會處理這些事件，並在 /dev 內的 **RAM** 檔案系統中產生所需的特殊區塊檔案。如果沒有這些專用檔案，便無法存取檔案系統和其他設備。

管理 RAID 和 LVM 設定

如果您之前將系統設定為在 **RAID** 或 **LVM** 下存放根目錄檔案系統，init 此時會設定 **LVM** 或 **RAID**，以便之後能夠存取根目錄檔案系統。如需有關 **RAID** 與 **LVM** 的資訊，請參閱第 15 章「進階磁碟設定」(↑部署指南)。

管理網路組態

如果您之前將系統設定為使用網路掛接的根目錄檔案系統(透過 **NFS** 掛接)，那麼 init 此時必須確定是否已載入適當的網路驅動程式，並且這些驅動程式是否設定為允許存取根目錄檔案系統。

如果檔案系統位於 **iSCSI** 或 **SAN** 這樣的網路區塊設備上，initramfs 還會設定與儲存伺服器間的連線。

若於安裝過程的啟始開機階段呼叫 init，它執行的任務會與上述任務有所不同：

尋找安裝媒體

當您啟動安裝程序時，您的機器會透過安裝媒體上的 **YaST** 安裝程式載入一個安裝核心以及一個特殊的 init。在 **RAM** 檔案系統中執行的 **YaST** 安裝程式，必需具備安裝媒體的實際位置相關資訊，以便存取該程式和安裝作業系統。

啟始硬體辨識並載入適當核心模組

如第 9.1.1 節「initramfs」[94頁] 中所述，開機程序會以最少量的驅動程式啟動，供大部分的硬體組態使用。init 會啟動一個啟始硬體掃描程序，以確定這組驅動程式是否適合您的硬體組態。開機程序所需的模組名稱會寫入 /etc/sysconfig/kernel 的 INITRD_MODULES 中。這些名稱用來產生系統開機所需的自定 initramfs。如果模組不是開機所需，而是供 **coldplug** 使用，則模組會寫入 /etc/sysconfig/hardware/hwconfig-*。用此目錄中的組態檔案描述的所有設備都會在開機程序中啟始化。

載入安裝系統或救援系統

正確識別硬體後，系統會立即載入適當的驅動程式，udev 會建立特殊的設備檔案，而 init 會透過實際的 YaST 安裝程式啟動安裝系統或者啟動救援系統。

啟動 YaST

最後，init 會啟動 YaST，後者會啟動套件安裝和系統組態程序。

9.2 init 程序

init 程式是第一個程序，它負責以所需的方式來啟始化系統。init 由核心直接啟動，它拒絕訊號 9，因為這個訊號通常會結束程序。所有其他程式不是由 init 直接啟動，就是由它的子程序啟動。

init 是在 `/etc/inittab` 檔案中集中設定，執行層級也是在該檔案中定義(請參閱第 9.2.1 節「執行層級」[97頁])。該檔案還會指定每個執行層級可以使用的服務和精靈。按照 `/etc/inittab` 的項目，init 會執行多個程序檔。依預設，開機後啟動的第一個程序檔是 `/etc/init.d/boot`。系統啟始化階段一旦完成，系統就會使用 `/etc/init.d/rc` 程序檔將執行層級變更為其預設執行層級。為避免混淆，這些稱做 *init 程序檔* 的程序檔都位於目錄 `/etc/init.d` 中(請參閱第 9.2.2 節「Init 程序檔」[100頁])。

系統啟動和關閉的程序，是由 init 維護。從這個角度看，核心可以視為一個背景程序，負責維護所有其他的程序，以及根據其他程式的要求來調整 CPU 時間和硬體存取。

9.2.1 執行層級

在 Linux 中是由執行層級定義啟動系統的方式，以及在所執行的系統可以使用哪些服務。開機之後，系統會按照 `/etc/inittab` 中的 `initdefault` 這一行文字的定義而啟動。一般是 3 或 5。請參閱表格 9.1 「可用的 Runlevel」[98頁]。還有一種方法是，執行層級可以在開機期間指定(例如，在開機提示時新增執行層級編號)。所有不是由核心自身直接計算的參數，都會傳送給 init。要開機進入 runlevel 3，只需在開機提示處新增數字 3。

表格 9.1 可用的 *Runlevel*

執行層級	描述
0	系統終止
S 或 1	單一使用者模式
2	本地多重使用者模式，不包含遠端網路 (NFS 等)
3	完整的多重使用者模式，包含網路
4	「使用者定義」，除非管理員設定了此執行層級，否則此項將不可用
5	完整多重使用者模式，包含網路、X 顯示管理員—KDM、GDM 或 XDM
6	系統重新開機

重要：避免透過 NFS 掛接分割區的執行層級 2

如果系統會透過 NFS 掛接 `/usr` 一類分割區，您就不應該使用執行層級 2。如果程式檔案或是程式庫因執行層級 2 (本地多重使用者模式，無遠端網路) 無法提供 NFS 服務而發生遺失，系統可能無法正常運作。

若要在系統執行時變更執行層級，請輸入 `telinit` 以及當成引數的對應數字。只有系統管理員可以執行此動作。以下清單列出執行層級區域中最重要指令摘要。

`telinit 1` 或 `shutdown now`

系統變更為單一使用者模式。此模式是用於系統維護和管理任務。

`telinit 3`

可以啟動所有主要的程式和服務 (包括網路)，且可讓一般使用者登入並在非圖形環境下使用該系統。

```
telinit 5
```

啟用圖形式環境。此時通常會啟動顯示管理員，如 XDM、GDM 或 KDM。
如果已啟用自動登入，本地使用者就可以登入事先選定的視窗管理員
(GNOME、KDE 或任何其他視窗管理員)。

```
telinit 0 或 shutdown -h now
```

系統終止。

```
telinit 6 或 shutdown -r now
```

系統終止後重新開機

所有 SUSE Linux Enterprise Server 標準安裝中，預設都使用執行層級 5。使用者會在提示之下使用圖形介面登入或預設的使用者會自動登入。

警告：/etc/inittab 中有錯誤可能會造成系統開機發生錯誤

如果 /etc/inittab 損毀，系統可能無法正常開機。因此，在編輯 /etc/inittab 時要格外小心。將機器重新開機前，請務必使用 `telinit q` 指令讓 `init` 重新讀取 /etc/inittab。

通常，當您變更執行層級時會發生兩件事。首先，啟動目前執行層級中的停止程序檔，關閉對目前執行層級很重要的一些程式。然後啟動新執行層級的啟動程序檔。在大部份的情況下，此時也會啟動一些程式。例如，從執行層級 3 變更成 5 時，會發生以下事件：

1. 管理員 (root) 可以透過輸入 `telinit 5`，要求 `init` 變更為不同的執行層級。
2. `init` 會檢查目前的執行層級 (runlevel) 並決定是否要以新執行層級作為啟動 /etc/init.d/rc 的參數。
3. 現在，如果新執行層級沒有啟動程序檔，`rc` 會呼叫目前執行層級的停止程序檔。在此範例中，所有程序檔都位於 /etc/init.d/rc3.d (舊的執行層級是 3)，並以 `K` 開頭。`K` 後面的數字表示以 `stop` 參數執行程序檔的順序，因為還有其他的因素要考慮。
4. 新的執行層級啟動程序檔，會最後才啟動。在此範例中的所有程序檔，都位於 /etc/init.d/rc5.d，而且開頭是 `S`。同時，`S` 後面的數字決定要啟動程序檔的序列。

變更成與目前 `runlevel` 相同的 `runlevel` 時，`init` 只會檢查 `/etc/inittab` 是否變更，並啟動適當的步驟，例如，在另一個介面啟動 `getty`。使用指令 `telinit q` 也可以完成相同功能。

9.2.2 Init 程序檔

`/etc/init.d` 中的程序檔有兩種類型：

由 `init` 直接執行的程序檔

這種狀況僅出現於開機程序或立即關閉系統 (電源中斷或使用者按下 **Ctrl + Alt + Del**) 時。對 IBM System z 系統而言，僅出現於開機程序期間或立即關閉系統時 (電源斷開或透過「訊號靜止」)。此程序檔定義於 `/etc/inittab`。

由 `init` 間接執行的程序檔

這些程序檔在變更執行層級時就會執行，而且永遠會呼叫主要程序檔 `/etc/init.d/rc`，以保證相關程序檔的順序正確。

所有程序檔都位於 `/etc/init.d`。在開機時執行的程序檔會透過 `/etc/init.d/boot.d` 的符號連結來呼叫。用於變更執行層級的程序也可以透過其中一個子目錄 (`/etc/init.d/rc0.d` 到 `/etc/init.d/rc6.d`) 的符號連結來呼叫。這樣的安排是為了更加明確，避免程序檔用於多個執行層級時，造成重複情況。因為每一個程序檔都可當成啟動程序檔和停止程序檔來執行，所以這些程序檔必須瞭解參數 `start` 和 `stop`。程序檔也瞭解 `restart`、`reload`、`force-reload` 和 `status` 選項。這些不同選項在 表格 9.2 「可用的 `init` 程序檔選項」 [100頁] 都有說明。直接由 `init` 執行的程序檔沒有這些連結。他們可以根據需要從執行層級獨立執行。

表格 9.2 可用的 `init` 程序檔選項

選項	描述
<code>start</code>	啟動服務。
<code>stop</code>	停止服務。

選項	描述
<code>restart</code>	如果服務在執行中，先停止，再重新啟動。如果服務沒有執行，請啟動它。
<code>reload</code>	不需停止和重新啟動服務，就可以重新載入組態。
<code>force-reload</code>	如果服務支援，請重新載入組態。否則，執行與 <code>restart</code> 相同的動作。
<code>status</code>	顯示目前狀態。

每一個特定執行層級子目錄中的連結，可以將程序檔與不同執行層級產生關聯。安裝或解除安裝套件時，可以透過程式 `insserv` 的協助，新增和移除這些連結 (或透過 `/usr/lib/lsb/install_initd`，它是一個會呼叫該程式的程序檔)。請參閱 `man 8 insserv` 以取得詳細資料。

這些設定也都可以利用 `YaST` 模組來變更。如果您需要透過指令行檢查狀態，請使用 `chkconfig` 工具。`man 8 chkconfig` **man** 頁面中提供了說明。

簡介最先啟動的開機及最後啟動的停止程序檔，並說明維護程序檔。

boot

使用 `init` 直接啟系統時會執行。它與所選的執行層級無關，而且只會執行一次。此時會掛接 `/proc` 和 `/dev/pts` 檔案系統，並啟動 `blogd` (開機記錄精靈)。如果系統是更新或安裝之後第一次開機，會啟動啟始系統組態。

`blogd` 精靈是透過 `boot` 和 `rc` 啟動的服務，先於其他任何服務。它在這些程序檔 (會執行多個子程序檔，如使特殊區塊檔案能夠使用) 觸發的動作完成之後就會停止。`blogd` 會將螢幕輸出的所有內容寫入記錄檔案 `/var/log/boot.msg`，但唯有當 `/var` 掛接為可讀寫，才會發生。否則，`blogd` 會緩衝處理所有螢幕資料，直到 `/var` 可以使用為止。使用 `man 8 blogd` 可取得關於 `blogd` 的其他資訊。

boot 程序檔還負責啟動 `/etc/init.d/boot.d` 中名稱以 `s` 開頭的所有程序檔。在該處，會檢查檔案系統，並在需要時設定迴圈設備。也會設定系統時間。如果自動檢查和修復檔案系統時發生錯誤，系統管理員輸入管理員密碼後即可介入。最後執行的程序檔是 `boot.local`。

`boot.local`

此處輸入開機時進入執行層級之前要執行的其他指令。它就像是 DOS 系統的 `AUTOEXEC.BAT`。

`halt`

僅在進入執行層級 0 或 6 時才會執行此程序檔。此時，它做為 `init` 或 `init` 來執行。系統是否關閉還是重新開機，取決於呼叫 `halt` 的方式。如果在關機期間需要執行特殊指令，請將這些指令新增至 `init` 程序檔。

`rc`

此程序檔會呼叫目前執行層級的適當停止程序檔，以及新選取執行層級的啟動程序檔。與 `/etc/init.d/boot` 程序檔相似，系統從 `/etc/inittab` 中呼叫此程序檔，並使用所需的執行層級做為參數。

您可以建立自己的程序檔，並輕鬆將它們整合至上述配置。如需有關格式化、命名以及組織自定程序檔的指示，請參閱 LSB 的規格和 `init`、`init.d`、`chkconfig` 及 `insserv` 的 `man` 頁面。另請參閱 `startproc` 和 `killproc` 的 `man` 頁面。

警告：錯誤的 `init` 程序檔可能會終止系統

錯誤的 `init` 程序檔可能會讓您的機器當機。編輯類似程序檔要格外小心，可能的話，讓它們在多重使用者環境下密集測試。第 9.2.1 節「執行層級」[97頁] 中提供了關於 `init` 程序檔的有用資訊。

若要為指定的程式或服務建立自定 `init` 程序檔，請使用 `/etc/init.d/skeleton` 檔案做為樣板。使用新名稱儲存此檔案的副本，並根據需要編輯相關程式和檔案名稱、路徑以及其他詳細資料。您也可能因個人的特別需求而要增強程序檔的功能，以便 `init` 程序觸發適當的動作。

上方的 `INIT INFO` 區塊是程序檔的必要組件，因此必須進行編輯。請參閱範例 9.1 「迷你 `INIT INFO` 區塊」[103頁]。

範例 9.1 迷你 *INIT INFO* 區塊

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

請在 *INFO* 區塊的第一行中、*Provides:* 後面，為此 *init* 程序檔所控制的程式或服務指定名稱。在 *Required-Start:* 與 *Required-Stop:* 這兩行中，指定服務本身停止後仍必須處於執行狀態的所有服務。此資訊以後會用來產生程序檔名稱的編號，這些就是在執行層級目錄可以找到的編號。*Default-Start:* 和 *Default-Stop:* 之後，指定應該自動啟動或停止服務的執行層級。最後，會在 *Description:* 簡要說明討論中的服務。

若要從執行層級目錄 (*/etc/init.d/rc?.d/*) 建立對應到 */etc/init.d/* 中的程序檔，請輸入 *insserv new-script-name* 指令。*insserv* 會根據 *INIT INFO* 標頭進行計算，在執行層級目錄 (*/etc/init.d/rc?.d/*) 中建立啟動和停止程序檔的必要連結。該程式也會為這些連結的名稱加上必要的編號，即可依正確順序啟動和停止每一個執行層級。如果您偏好以圖形工具來建立類似連結，請使用 *YaST* 提供的執行層級編輯器，請見第 9.2.3 節「使用 *YaST* 設定 *System Services (Runlevel)*」[103頁]。

如果 */etc/init.d/* 裡已經有程序檔，應該整合至現有的執行層級配置，使用 *insserv* 在執行層級目錄中立即建立連結，或者在 *YaST* 的執行層級編輯器中啟用對應的服務。下次重新啟動時，將會套用您所做的變更——新服務會自動啟動。

請勿手動設定這些連結。如果 *INFO* 區塊發生錯誤，稍後執行某些其他服務的 *insserv* 將會發生問題。手動新增的服務將會在下次為此程序檔執行 *insserv* 時予以移除。

9.2.3 使用 *YaST* 設定 *System Services (Runlevel)*

使用「*YaST*」>「系統」>「*System Services (Runlevel)*」啟動此 *YaST* 模組後，會出現一個綜覽清單，其中會列出所有可用的服務和每項服務目前的狀態(停用或啟用)。決定要以「簡單模式」或「進階模式」使用模組。大部份情況下，預

設的「簡單模式」應該都已夠用。左欄顯示服務的名稱，中間欄顯示其目前狀態，而右欄提供簡短說明。視窗下方為選取的服務提供更詳細的說明。若要啟用服務，在表格中選取它，然後選取「啟用」。停用服務的步驟也一樣。

要更仔細控制啟動或停止服務的執行層級，或者變更預設的執行層級，請先選取「進階模式」。目前預設的執行層級或「initdefault」(系統開機時預設掛接的執行層級)會出現在視窗上方。一般情況下，SUSE Linux Enterprise Server 系統的預設執行層級是執行層級 5 (含網路和 X 的完整多重使用者模式)。合適的替代方法可能是執行層級 3 (含網路的完整多重使用者模式)。

此 YaST 對話方塊允許其中一個執行層級選項 (如表格 9.1 「可用的 Runlevel」 [98 頁] 所列) 做為新預設。此外，還可使用此視窗中的表格，啟用或停用個別服務和精靈。表格會列示可用的服務和精靈，顯示它們在您的系統上目前是否啟用，如果啟用，是哪一個執行層級。使用滑鼠選取其中一列後，按一下代表執行層級的核取方塊 (「B」、「0」、「1」、「2」、「3」、「5」、「6」和「S」) 來定義執行層級，以便在該處執行選取的服務或精靈。執行層級 4 並未定義，以便建立自定執行層級。表格概觀的正下方，提供目前所選服務或精靈的簡要說明。

警告：錯誤的執行層級設定可能會造成系統損害

錯誤的執行層級設定可能會導致系統無法使用。在您套用變更之前，請務必確定您知道它們的後果。

圖形 9.1 System Services (Runlevel)



使用「啟動、停止或重新整理」，決定是否啟動服務。「重新整理狀態」檢查目前狀態。您可以使用「設定或重設」來做選擇，將您的變更套用至系統，或復原啟動執行層級編輯器之前的設定。選取「確定」即可將變更的設定儲存至磁碟。

9.3 透過 /etc/sysconfig 設定系統組態

SUSE Linux Enterprise Server 的主要組態是由 /etc/sysconfig 中的組態檔案來控制。/etc/sysconfig 中個別的檔案只由相關的程式檔讀取。這可以確保例如網路設定，只由網路相關的程序檔來剖析。

有兩種方式可以編輯系統組態：使用 YaST Sysconfig 編輯器或手動編輯組態檔。

9.3.1 使用 YaST Sysconfig 編輯器變更系統組態

YaST sysconfig 編輯器會提供一個易於使用的前端工具，用於設定系統。無須瞭解要變更之組態變數的實際位置，只要使用此模組內建的搜尋功能，根據需要變更組態變數的值，接著 YaST 會套用這些變更、根據 sysconfig 中設定的值更新組態，然後重新啟動服務。

警告：修改 `/etc/sysconfig/*` 檔案可能會損壞您的安裝檔案

如果您先前並無經驗和相關知識，請勿修改 `/etc/sysconfig` 檔案。它可能會嚴重損毀您的系統。`/etc/sysconfig` 中的檔案包含每一個變數的簡短註解，說明它們的實際作用。

圖形 9.2 使用 sysconfig 編輯器的系統組態



YaST sysconfig 對話方塊分割成三個部份。對話方塊的左側顯示所有可設定變數的樹狀結構檢視。當您選取變數時，右側會顯示目前的選擇，以及此變數的目前設定。下方的第三個視窗對變數的用途、可能值、預設值以及產生此變數的實際組態檔提供了簡短說明。對話方塊也提供關於變更變數後要執行的組態程序檔，以及變更結果會啟動什麼新服務等等的相關資訊。YaST 會要求您確認變更，並告訴您在選取「完成」並離開對話方塊後會執行的程序檔。請選取目前要略過的服務和程序檔，它們會在稍後啟動。為了讓變更生效，YaST 會自動套用所有變更並重新啟動已變更組態的服務。

9.3.2 手動變更系統組態

若要手動變更系統組態，請執行下列步驟：

- 1 切換為 `root` 身分。
- 2 使用 `telinit 1`，將系統置於單一使用者模式 (執行層級 1)。
- 3 使用選擇的編輯器對組態檔進行所需變更。

如果未使用 `YaST` 來變更 `/etc/sysconfig` 中的組態檔，請確定空的變數值是由兩個引號所表示 (`KEYTABLE=""`)，而且該值與其中的空格包夾在引號中。由一個文字組成的值不需要包夾在引號中。

- 4 執行 `SUSEconfig` 來確定變更生效。
- 5 使用 `telinit 預設 執行層級 指令`，將系統還原成先前的執行層級。採用系統預設的執行層級來取代 `default_runlevel`。若要返回有網路和 `X` 的完整多重使用者模式，請選擇 5；若要在有網路的完整多重使用者模式下工作，請選擇 3。

變更整個系統設定，例如網路組態時，才會用到此程序。小幅度變更不必進入單一使用者模式，不過您也可以進入單一使用者模式，即可百分之百確定所有相關程式都正確重新啟動。

提示：設定自動系統組態

若要停用由 `SUSEconfig` 自動設定的系統組態，請將 `/etc/sysconfig/suseconfig` 中的 `ENABLE_SUSECONFIG` 變數設為 `no`。如果您想使用 `SUSE` 安裝支援，請勿停用 `SUSEconfig`，也可以停用部分自動組態。

開機載入程式 GRUB

本章介紹如何設定 SUSE® Linux Enterprise Server 中使用的開機載入程式 GRUB (Grand Unified Bootloader)。一種特殊的 YaST 模組，可用於設定所有設定。如果您不熟悉 Linux 開機的要點，請閱讀以下章節，取得部份背景資訊。本章節也敘述使用 GRUB 開機時，經常遇到的部份問題以及它們的解決方案。

注意：使用 UEFI 的機器上未安裝 GRUB

依照慣例，GRUB 將會安裝在配有傳統 BIOS 的機器上與使用相容支援模組 (CSM) 的 UEFI (統一可擴充韌體介面) 機器上。未啟用 CSM 的 UEFI 機器會自動安裝 eLILO (如果 DVD1 開機成功)。如需詳細資訊，請參閱系統上 `/usr/share/doc/packages/elilo/` 中的 **eLILO** 文件。

本章節著重於開機管理以及開機載入程式 GRUB 的組態。整個開機程序簡述於第 9 章「啟動及設定 Linux 系統」[93頁]。開機載入程式是機器 (BIOS) 與作業系統 (SUSE Linux Enterprise Server) 之間的介面。開機載入程式的組態會直接影響作業系統的開機。

下列詞彙將在本章節中經常出現，而且可能需要說明：

MBR (主開機記錄)

MBR 的結構是由作業系統 (獨立會議) 所定義。前 446 位元組是保留給程式碼。它們通常包含一部分開機載入程式或作業系統選取器。接下來的 64 位元組為最多包含四項的分割區表提供空間。分割區表包含磁碟分割以及檔案系統類型相關資訊。作業系統需要此表格來處理硬碟。在 MBR 中使用傳統標準程式碼的情況下，只有一個分割區必須標示為作用中。MBR 的

最後兩個位元組必須包含靜態的「魔術編號」(AA55)。包含不同值的 MBR 會被一些 BIOS 視為無效，所以開機時不列入考慮。

開機磁區

開機磁區是除了擴充分割區以外，硬碟分割區的第一個磁區，它只會當成其他分割區的「容器」。這些開機磁區有 512 位元組的空間供程式碼使用，而這些程式碼是用來啟動各自分割區中安裝的作業系統。這適用於 DOS、Windows 和 OS/2 分割區格式的開機磁區，它們也包含檔案系統的部分重要基本資料。相反的，Linux 分割區的開機磁區一開始是空白，直到設定不同於 XFS 的檔案系統之後，才會寫入記錄。因此，Linux 分割區無法自行啟動，即使它包含核心以及有效的根檔案系統。開機磁區如果包含可以啟動系統的有效程式碼，則它的魔術編號與 MBR 的最後兩個位元組相同(AA55)。

10.1 使用 GRUB 開機

GRUB 包含兩個階段。第一個階段包含 512 個位元組，其唯一的任務就是載入開機載入程式的第二個階段。接下來，會載入第二個階段。這個階段會包含開機載入程式的主要部分。

某些組態會使用中繼階段 1.5，用來配置和載入適當檔案系統的階段 2。在適當情況下，這種方法在安裝或使用 YaST 初始設定 GRUB 時會是預設選項。

第二個階段可以存取許多檔案系統。目前支援 ext2、ext3、ReiserFS、Minix 及 Windows 使用的 DOS FAT 檔案系統。對於 XFS、UFS 以及 BSD 使用的 FFS，也支援到一定的程度。自 0.95 版開始，GRUB 也可以從包含 ISO 9660 標準檔案系統(符合「El Torito」規格)的 CD 或 DVD 啟動。即使是在系統開機之前，GRUB 也可以存取支援之 BIOS 磁碟機(BIOS 偵測到的磁片或硬碟、CD 光碟機和 DVD 磁碟機)的檔案系統。因此，對 GRUB 組態檔案(menu.lst)所做的變更，將不需要重新安裝開機管理程式。啟動系統後，GRUB 會重新載入功能表檔案以及核心或起始 RAM 磁碟(initrd)的有效路徑和分割區資料，然後找這些檔案。

GRUB 的實際組態以下方描述的四個檔案為基礎：

```
/boot/grub/menu.lst
```

此檔案包含可以使用 GRUB 啟動的分割區或作業系統，所有的相關資訊。如果沒有這段資訊，GRUB 指令行就會提示使用者提供如何繼續執行(如需詳細資訊，請參閱第 10.1.1.3 節「在開機程序期間編輯功能表項目」[115頁])。

`/boot/grub/device.map`

此檔案會從 GRUB 和 BIOS 表示法，將設備名稱轉譯成 Linux 設備名稱。

`/etc/grub.conf`

此檔案包含 GRUB 外圍程序正確安裝開機載入程式所需的指令、參數和選項。

`/etc/sysconfig/bootloader`

此檔案由 perl-bootloader 程式庫 (在借助 YaST 設定開機載入程式時及每次安裝新的核心時使用) 讀取。它包含預設會新增到開機載入程式組態檔案的組態選項 (如核心參數)。

有多種方法可以控制 GRUB。現有組態啟動項目，可以從圖形功能表選取 (開頭顯示畫面)。組態會從檔案 `menu.lst` 載入。

在 GRUB，啟動前可以變更所有啟動參數。例如，編輯功能表檔案發生的錯誤，可以用此方法更正。在出現某類輸入提示時也可以透過互動方式輸入開機指令。如需詳細資料，請參閱第 10.1.1.3 節「在開機程序期間編輯功能表項目」[115頁]。GRUB 提供開機前，判斷核心和 `initrd` 二者位置的可能性。以此方法，您還可以為開機載入程式組態中不存在的項目，啟動安裝的作業系統。

GRUB 事實上有兩個版本：一個是開機載入程式，一個是位於 `/usr/sbin/grub` 的一般 Linux 程式。後者稱為 *GRUB 外圍程序*。它可以在安裝系統中提供 GRUB 模擬功能，並可用來安裝 GRUB 或是在套用之前測試設定。這種將 GRUB 安裝成硬碟或磁片上的開機載入程式的功能，以指令 `setup` 的形式整合於 GRUB。Linux 載入時，可以在 GRUB 外圍程序使用此指令。

10.1.1 檔案 `/boot/grub/menu.lst`

圖形開頭顯示畫面以及開機功能表是以 GRUB 組態檔 `/boot/grub/menu.lst` 為基礎的，它包含可以透過功能表啟動的所有分割區或作業系統，全部的相關資訊。

每次啟動系統時，GRUB 會從檔案系統載入功能表檔案。基於此因素，GRUB 不需要在每次變更檔案後，重新安裝。使用 YaST 開機載入程式來修改 GRUB 組態，如第 10.2 節「使用 YaST 設定開機載入程式」[119頁] 所述一般。

功能表檔案包含指令。語法相當簡單。每一行包含一個指令，後面是由像外圍程序中的空格所分開的選用參數。基於歷史因素，部份指令可以允許 = 放在第一個參數前面。註解是以井字號 (#) 開頭。

若要識別功能表綜覽中的功能表項目，請為每一個項目設定 `title`。關鍵字 `title` 後面的文字 (包括任何空格) 將在功能表中顯示成可選取的選項。當這個功能表項目被選取時，就會執行下一個 `title` 指示的所有指令。

最簡單的案例是重新導向至其他作業系統的開機載入程式。指令是 `chainloader` 及引數通常是 **GRUB** 區塊表示法中，其他分割區的啟動區塊。例如：

```
chainloader (hd0,3)+1
```

GRUB 中的設備名稱會在第 10.1.1.1 節「硬碟和分割區的命名慣例」[113頁] 說明。這個範例會指定第一個硬碟中，第四個分割區的第一個區塊。

使用指令 `kernel` 來指定核心影像。第一個引數是分割區中，核心影像的路徑。其他引數會傳送到指令行上的核心。

如果核心沒有內建驅動程式來存取根分割區、或是這時是使用包含進階 **HotPlug** 功能的最新 **Linux** 系統，`initrd` 就必須以個別的 **GRUB** 指令來指定，它唯一的引數是 `initrd` 檔案路徑。因為 `initrd` 的載入位址是記錄於載入的核心影像，所以指令 `initrd` 必須立即接在 `kernel` 指令的後面。

指令 `root` 會簡化核心和 `initrd` 檔案的指定。`root` 的唯一引數是設備或分割區。這個設備會用於所有一直到下一個 `root` 指令指定時才會出現明確指定設備的所有核心、`initrd` 或其他檔案路徑。

`boot` 指令會在每一個功能表項目最後暗示，所以它不需要寫入功能表檔案。不過，如果您使用互動式 **GRUB** 來啟動，必須在最後輸入 `boot` 指令。指令本身沒有引數。它只是啟動載入的核心影像或指定的鏈結載入器。

撰寫所有功能表項目之後，將其中一個定義為 `default` 項目。否則，會使用第一個 (項目 0) 做為預設項目。您也可以指定預設項目要在幾秒後啟動。`timeout` 和 `default` 通常在功能表項目前面。如需參考範例，請參閱第 10.1.1.2 節「功能表檔案範例」[113頁]。

10.1.1.1 硬碟和分割區的命名慣例

GRUB 用於硬碟和分割區的命名慣例與用於一般 Linux 設備的命名慣例不同。它比較類似 BIOS 的簡易磁碟列舉方式，而且語法類似一些 BSD 衍生版本中所用的語法。在 GRUB 中，分割區的編號從 0 開始。這表示 (hd0, 0) 是第一個硬碟的第一個分割區。與一般桌上型機器的 primary master 硬碟對應的 Linux 設備名稱是 /dev/sda1。

四個可能的主分割區會指定分割區編號 0 到 3。邏輯分割區是從 4 開始編號：

```
(hd0,0)   first primary partition of the first hard disk
(hd0,1)   second primary partition
(hd0,2)   third primary partition
(hd0,3)   fourth primary partition (usually an extended partition)
(hd0,4)   first logical partition
(hd0,5)   second logical partition
```

由於獨立於 BIOS 設備，GRUB 不會區分 PATA (IDE)、SATA、SCSI 和硬體 RAID 設備。BIOS 或其他控制器識別的所有硬碟，會按照 BIOS 的開機順序編號。

可惜的是，它通常無法將 Linux 設備名稱正確對應至 BIOS 設備名稱。它會透過演算法的協助來產生此對應，然後儲存至檔案 device.map，需要時可以編輯它。如需關於檔案 device.map 的資訊，請參閱第 10.1.2 節「檔案 device.map」[116頁]。

完整 GRUB 路徑包含放在括號中的設備名稱，以及指定分割區中檔案系統的檔案路徑。路徑開頭是一個斜線。例如，如果系統有一個 PATA (IDE) 硬碟，它的第一個分割區包含 Linux，則可以使用如下方式指定可開機核心：

```
(hd0,0)/boot/vmlinuz
```

10.1.1.2 功能表檔案範例

以下範例顯示 GRUB 功能表檔案的結構。這個範例安裝會在 /dev/sda5 下建立 Linux 開機分割區，在 /dev/sda7 下建立根分割區，在 /dev/sda1 下進行 Windows 安裝。

```
gfxmenu (hd0,4)/boot/message❶
color white/blue black/light-gray❷
default 0❸
timeout 8❹
```

```

title linux⑤
    root (hd0,4)
    kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
    initrd /boot/initrd

title windows⑥
    rootnoverify (hd0,0)
    chainloader +l

title floppy⑦
    rootnoverify (hd0,0)
    chainloader (fd0)+l

title failsafe⑧
    root (hd0,4)
    kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma \
    apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
    initrd /boot/initrd.shipped

```

第一個區塊定義開頭顯示畫面的組態：

- ❶ 背景影像 message 位於 /dev/sda5 分割區的 /boot 目錄中。
- ❷ 顏色配置：白色(前景)、藍色(背景)，黑色(選中項目)，以及淺灰色(選中項目的背景)。色彩配置對於開頭顯示畫面沒有作用，只對您可以存取而且可以自定的 GRUB 功能表有作用(您可以使用 Esc，結束開頭顯示畫面)。
- ❸ 依預設，啟動的是第一個 (0) 功能表項目 title linux。
- ❹ 沒有任何用者輸入，經過 8 秒後，GRUB 會自動啟動預設項目。若要停用自動開機，請刪除 timeout。如果設定為 timeout 0，GRUB 會馬上啟動預設項目。

第二個(最大的)區塊會列示各種可開機的作業系統。個別作業系統的區段會從 title 開始。

- ❺ 第一個項目(title linux)負責將 SUSE Linux Enterprise Server 開機。核心(vmlinuz)是位在第一個硬碟的第一個邏輯分割區(開機分割區)。核心參數，例如根分割區和 VGA 模式，會在此添加。根分割區是根據 Linux 命名慣例(/dev/sda7/)指定的，因為此資訊由核心讀取，與 GRUB 無關。initrd 也是位在第一個硬碟的第一個邏輯分割區。
- ❻ 第二個項目負責載入 Windows。Windows 是從第一個硬碟的第一個分割區啟動(hd0,0)。指令 chainloader +l 會造成 GRUB 載入並執行指定分割區的第一個磁區。
- ❼ 下一個項目允許從磁片開機，無需修改 BIOS 設定。
- ❽ 開機選項 failsafe 會以選擇的核心參數來啟動 Linux，可以啟動發生問題的 Linux 系統。

功能表檔案可以在需要時變更。GRUB 會在下次啟動時使用修改的設定。使用 YaST 或選擇的編輯器，永久地編輯檔案。另一種方法是，使用 GRUB 的編輯功能，以互動方式暫時變更 (請參閱第 10.1.1.3 節「在開機程序期間編輯功能表項目」 [115頁])。

10.1.1.3 在開機程序期間編輯功能表項目

在圖形化開機功能表中，可以使用方向鍵選取要啟動的作業系統。如果選取 Linux 系統，可以在開機提示時輸入其他啟動參數。若要直接編輯個別功能表項目，請按 Esc 結束開頭顯示畫面，然後跳到 GRUB 文字功能表，再按 E。用此方式所做的變更，只會套用到目前開機，因此不會永久變更。

重要：開機程序期間的鍵盤配置

US 鍵盤配置是啟動時唯一可以使用的鍵盤配置。請參閱圖形 35.3 「美國鍵盤配置」 [521頁]。

編輯功能表項目有利於修復無法再啟動的缺陷系統，因為開機載入程式錯誤的組態檔，可以手動輸入參數，便得以解決。在開機程序期間手動輸入參數，對於測試新設定但可避免損壞原始系統，有很大的幫助。

啟用編輯模式之後，使用方向鍵選取功能表項目來編輯組態。若要讓組態變成可編輯狀態，請再按 E 一次。使用此方法，在對於開機程序產生負面影響之前編輯錯誤的分割區或路徑指定。按 Enter，結束編輯模式並返回功能表。然後按 B 來啟動此項目。底下的說明文字會顯示進一步可行的動作。

若要永久地輸入變更的開機選項，然後傳送至核心，以 root 身分開啟檔案 menu.lst，然後將各自的核心參數加入到現有的指令行，並以空格分隔：

```
title linux
    root(hd0,0)
    kernel /vmlinuz root=/dev/sda3 additional parameter
    initrd /initrd
```

GRUB 會在下次啟動系統時，使用新參數。另一種方法是，使用 YaST 開機載入程式模組做此變更。將新參數加入至現有的行，並用空格分開。

10.1.2 檔案 device.map

檔案 `device.map` 會將 GRUB 和 BIOS 設備名稱對應至 Linux 設備名稱。在包含 PATA (IDE) 和 SCSI 硬碟的混合系統中，GRUB 必須透過特定程序來確定開機順序，因為 GRUB 可能無法存取 BIOS 的開機順序資訊。GRUB 儲存分析的結果至檔案 `/boot/grub/device.map`。對於 BIOS 中的開機順序設定為 PATA 先於 SCSI 的系統，其範例 `device.map` 檔案如下所示：

```
(fd0)  /dev/fd0
(hd0)  /dev/sda
(hd1)  /dev/sdb
```

或

```
(fd0)  /dev/fd0
(hd0)  /dev/disk-by-id/DISK1 ID
(hd1)  /dev/disk-by-id/DISK2 ID
```

因為 PATA (IDE)、SCSI 和其他硬碟的順序取決於多種因素，並且 Linux 無法識別映射，所以檔案 `device.map` 中的順序可透過手動方式設定。如果您在開機時遇到問題，可檢查此檔案中的序列是否與 BIOS 中的序列相對應，然後在需要時使用 GRUB 提示暫時進行修改。啟動 Linux 系統之後，檔案 `device.map` 可以透過 YaST 開機載入程式或其他選擇的編輯器，永久性編輯。

注意：最大硬碟數

為了定址硬碟，GRUB 會使用 BIOS 服務。此作業是透過軟體岔斷 `Int13h` 來完成的。由於 `Int13h` 最多只能處理八個磁碟，因此，即使存在更多磁碟，GRUB 也只能從那些經由 `Int13h` 處理的磁碟開機 (多重路徑系統中常常會出現這種情況)。因此，安裝時建立的 `device.map` 檔案最多只能包含八個 `Int13h` 處理的磁碟。

在手動變更檔案 `device.map` 之後，執行以下指令來重新安裝 GRUB。此指令會造成檔案 `device.map` 重新載入，並以 `grub.conf` 列示的指令執行：

```
grub --batch < /etc/grub.conf
```

10.1.3 檔案 /etc/grub.conf

除了 `menu.lst` 和 `device.map` 之外，第三重要的 GRUB 組態檔案是 `/etc/grub.conf`。此檔案包含 GRUB 外圍程序正確安裝開機載入程式所需的指令、參數和選項：

```
setup --stage2=/boot/grub/stage2 --force-lba (hd0,1) (hd0,1)
quit
```

此指令會告知 GRUB 自動將開機載入程式安裝到第一個硬碟上的第二個分割區 (`hd0,1`)，安裝時使用位於同一個分割區上的開機影像。從已掛接的檔案系統安裝 `stage2` 影像時必須使用 `--stage2=/boot/grub/stage2` 參數。部分 BIOS 的 LBA 支援實作錯誤，`--force-lba` 提供了忽略這些錯誤的解決方案。

10.1.4 檔案 /etc/sysconfig/language

此組態檔案只在借助 YaST 設定開機載入程式時以及每次安裝新的核心時才使用。它可以由修改開機載入程式組態檔案 (例如 GRUB 中的 `/boot/grub/menu.lst`) 的 `perl-bootloader` 程式庫進行相應的評估。`/etc/sysconfig/bootloader` 不是 GRUB 特定的組態檔案，其值適用於 SUSE Linux Enterprise Server 上安裝的任何開機載入程式。

注意：核心更新之後的開機載入程式組態

每次安裝新的核心後，`perl-bootloader` 便會使用 `/etc/sysconfig/bootloader` 中指定的預設值寫入新的開機載入程式組態檔案 (例如針對 GRUB 寫入 `/boot/grub/menu.lst`)。如果要使用一組自定的核心參數，請務必根據需要調整 `/etc/sysconfig/bootloader` 中相關的預設值。

LOADER_TYPE

指定要在系統 (如 GRUB 或 LILO) 上安裝的開機載入程式。請勿直接修改—請依過程 10.6, “變更開機載入程式類型” [124頁] 中所述使用 YaST 變更開機載入程式。

DEFAULT_VGA / FAILSAFE_VGA / XEN_VGA

開機時使用之 `framebuffer` 的螢幕解析度和色彩深度使用核心參數 `vga` 進行設定。這些值定義要用於預設開機項目、`Failsafe` 和 `XEN` 項目的解析度和色彩深度。有效值包括：

表格 10.1 螢幕解析度與色彩深度參照表

	640x480	800x600	1024x768	1280x1024	1600x1200
8bit	0x301	0x303	0x305	0x307	0x31C
15bit	0x310	0x313	0x316	0x319	0x31D
16bit	0x311	0x314	0x317	0x31A	0x31E
24bit	0x312	0x315	0x318	0x31B	0x31F

DEFAULT_APPEND / FAILSAFE_APPEND / XEN_KERNEL_APPEND

核心參數(除 vga 之外) 會自動附加到開機載入程式組態檔案中的預設、Failsafe 和 XEN 開機項目。

CYCLE_DETECTION / CYCLE_NEXT_ENTRY

設定是否使用開機循環偵測，以及若使用則應在重新開機循環(如Failsafe)時將 /boot/grub/menu.lst 中的哪個替代項開機。如需詳細資訊，請參閱 /usr/share/doc/packages/bootcycle/README。

10.1.5 設定啟動密碼

即使作業系統啟動之前，GRUB 也可以存取檔案系統。沒有 root 許可權的使用者，在此時可以存取 Linux 系統中的檔案(這些檔案在系統啟動後，他們並無法存取)。若要封鎖此類型的存取，或防止使用者啟動特定的作業系統，請設定開機密碼。

重要：開機密碼和開頭顯示畫面

如果您在 GRUB 使用啟動密碼，將不會顯示一般的開頭顯示畫面。

按照以下方式，以使用者 root 的身分設定開機密碼：

- 1 在 root 提示下，使用 grub-md5-crypt 將密碼加密：

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```


2 將加密字串貼到檔案 menu.lst 的全域區段：

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

現在 GRUB 指令只可以在按 **P** 並輸入密碼後的啟動提示時執行。不過，使用者仍然可以從開機功能表，啟動所有作業系統。

3 要防止一或多個作業系統從開機功能表啟動，將項目 lock 新增至沒有密碼便不可以啟動的 menu.lst 每一個段落。例如：

```
title linux
    kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
    initrd (hd0,4)/initrd
    lock
```

重新啟動系統並從開機功能表選取 Linux 之後，將會顯示以下錯誤訊息：

```
Error 32: Must be authenticated
```

按 **Enter** 進入功能表。然後按 **P**，進入密碼提示要求。輸入密碼並按 **Enter** 之後，應該就可啟動選取的作業系統 (本範例為 Linux)。

10.2 使用 YaST 設定開機載入程式

在 SUSE Linux Enterprise Server 系統中設定開機載入程式最簡單的方法是使用 YaST 模組。在「YaST 控制中心」選取「系統」>「開機載入程式組態」。正如圖形 10.1「開機載入程式設定」[120頁]所示，這時會顯示系統目前的開機載入程式組態，並允許您進行變更。

圖形 10.1 開機載入程式設定



使用「區段管理」索引標籤可以編輯、變更以及刪除個別作業系統的開機載入程式區段。要加入選項，請按一下「新增」。若要變更現有選項的值，請先用滑鼠選取，接著按一下「編輯」。如果要移除現有項目，請選取它並按一下「刪除」。如果不熟悉開機載入程式選項，請先閱讀第 10.1 節「使用 GRUB 開機」[110頁]。

使用「開機載入程式安裝」索引標籤可以檢視和變更關於類型、位置和進階載入程式設定的設定。

按一下「其他」可存取進階組態選項。內建的編輯器可讓您變更 GRUB 組態檔案。如需詳細資料，請參閱第 10.1 節「使用 GRUB 開機」[110頁]。還可以刪除現有的組態然後「從頭開始」，或者讓 YaST 「建議新的組態」。也可以將組態寫入磁碟，或者從磁碟中重新讀取組態。要還原安裝期間儲存的原始主開機記錄 (MBR)，請選擇「還原硬碟的 MBR」。

10.2.1 調整預設開機項目

若要變更預設開機的系統，請依照下列步驟執行：

過程 10.1 設定預設系統

- 1 開啟「磁區管理」索引標籤。
- 2 從清單中選取所需項目。
- 3 按一下「設定為預設值」。
- 4 按一下「確定」，啟動這些變更。

10.2.2 修改開機載入程式位置

若要修改開機載入程式的位置，請執行下列步驟：

過程 10.2 變更開機載入程式位置

- 1 選取「開機載入程式安裝」索引標籤，然後為「開機載入程式位置」選擇以下其中一個選項：

「從主開機記錄開機」

這樣會在第一個磁碟的 MBR 中安裝開機載入程式 (根據 BIOS 中預設的開機順序)。

「從根分割區開機」

這會在 / 分割區的開機磁區中安裝開機載入程式。

「從開機分割區開機」

這會在 /boot 分割區的開機磁區中安裝開機載入程式。

「從延伸分割區開機」

這會在延伸分割區容器中安裝開機載入程式。

「自定開機分割區」

這個選項可讓您手動指定開機載入程式的位置。

- 2 按一下「確定」套用您的變更。

10.2.3 變更開機載入程式逾時

開機載入程式不會立即啟動預設系統。在逾時期間，您可以選取系統開機，或是寫入一些核心參數。若要設定開機載入程式逾時時間，請依照下列步驟執行：

過程 10.3 變更開機載入程式逾時

- 1 開啟「開機載入程式安裝」索引標籤。
- 2 按一下「開機載入程式選項」。
- 3 輸入新值、用滑鼠按住適當的方向鍵或使用鍵盤上的方向鍵，變更「逾時秒數」的設定值。
- 4 按兩次「確定」儲存變更。

警告：0 秒逾時

若將逾時設定為 0 秒，您將無法在開機時存取 GRUB。如果另外還將預設開機選項設定為非 Linux 作業系統，實際結果則是您將無法存取 Linux 系統。

10.2.4 設定啟動密碼

使用 YaST 模組，您也可以設定密碼來保護開機。這可以提供您另一層安全保護。

過程 10.4 設定開機載入程式密碼

- 1 開啟「開機載入程式安裝」索引標籤。
- 2 按一下「開機載入程式選項」。
- 3 按一下滑鼠啟動「使用密碼保護開機載入程式」選項，並輸入兩次「密碼」。
- 4 按兩次「確定」儲存變更。

10.2.5 調整磁碟順序

如果您的電腦有多個硬碟，您可以指定磁碟開機順序採用機器 BIOS 的設定 (請參閱第 10.1.2 節「檔案 device.map」[116頁])。若要執行這個動作，請依照下列步驟執行：

過程 10.5 設定磁碟順序

- 1 開啟「開機載入程式安裝」索引標籤。
- 2 按一下「開機載入程式詳細資訊」。
- 3 如果列出超過一個磁碟，請選擇一個磁碟，然後按一下「向上」或「向下」重新排列顯示磁碟的順序。
- 4 按兩次「確定」儲存變更。

10.2.6 設定進階選項

可透過「開機載入程式安裝」>「開機載入程式選項」設定進階開機選項。一般情況下，不需要變更預設設定。

「在分割區表中為開機分割區設定使用中旗標」

啟動包含開機載入程式的分割區。部分舊版的作業系統 (例如 Windows 98) 只能從使用中的分割區開機。

「將一般開機碼寫入 MBR」

以與作業系統無關的一般代碼取代目前的 MBR。

「除錯旗標」

將 GRUB 設定為除錯模式，以顯示描述磁碟活動的訊息。

「隱藏開機功能表」

隱藏開機功能表並使用預設項目開機。

警告

如果隱藏開機功能表，您將無法在開機時存取 **GRUB**。如果另外還將預設開機選項設定為非 **Linux** 作業系統，實際結果則是您將無法存取 **Linux** 系統。

「使用信任的 *GRUB*」

啟動信任的 **GRUB**，以支援信任的計算功能。

「圖形功能表檔案」

顯示開機畫面時所使用的圖形檔案路徑。

「序列連接參數」

如果您的機器是透過序列主控台控制的，您可以指定以何種速度來使用哪一個 **COM** 埠。同時請將「終端機定義」設定為「**serial**」。如需詳細資料，請參閱 `info grub` 或 <http://www.gnu.org/software/grub/manual/grub.html>。

「使用序列控制台」

如果您的機器是透過序列控制台控制的，請啟用此選項並指定以何速度來使用哪一個 **COM** 埠。請參閱 `info grub` 或 <http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal>

10.2.7 變更開機載入程式類型

在「開機載入程式安裝」中設定開機載入程式類型。**SUSE Linux Enterprise Server** 中的預設開機載入程式為 **GRUB**。若要使用 **LILO** 或 **ELILO**，請繼續執行下列步驟：

警告：LILO 不受支援

不建議使用 **LILO**，因為它在 **SUSE Linux Enterprise Server** 上不受支援。請只在特殊情況下使用。

過程 10.6 變更開機載入程式類型

- 1 開啟「開機載入程式安裝」索引標籤。
- 2 為「開機載入程式」選取「*LILO*」。

3 在這時開啟的對話方塊中，選取下面其中一個動作：

「建議新組態」

指定 YaST 建議新的組態。

「轉換目前的組態」

指定 YaST 轉換目前的組態。轉換組態時，可能會遺失某些設定。

「從頭開始設定新的組態」

寫入自定的組態。安裝 SUSE Linux Enterprise Server 時不能使用此動作。

「讀取儲存在硬碟的組態」

載入您個人的 `/etc/lilo.conf`。安裝 SUSE Linux Enterprise Server 時不能使用此動作。

4 按兩次「確定」儲存變更。

轉換過程中，舊的 GRUB 組態會儲存在磁碟中。若要使用它，只要將開機載入程式類型變更回 GRUB，然後從快顯示功能表選擇「還原轉換前儲存的組態」。這個動作只能在已安裝系統上使用。

注意：自定開機載入程式

如果要使用 GRUB 或 LILO 以外的開機載入程式，請選取「不要安裝任何開機載入程式」。請先詳細閱讀開機載入程式的說明文件，再選取這個選項。

10.3 解除安裝 Linux 開機載入程式

YaST 可以用來解除安裝 Linux 開機載入程式，並將 MBR 還原回安裝 Linux 前的狀態。安裝時，YaST 會自動建立原始 MBR 的備份，並在需要時還原。

若要解除安裝 GRUB，請啟動 YaST，然後按一下「系統」>「開機載入程式」以啟動開機載入程式模組。選取「其他」>「還原硬碟的 MBR」，並以「是，重新寫入」進行確認。

10.4 建立開機 CD

如果使用開機管理員來啟動系統時發生問題，或者無法在硬碟上安裝開機管理員，也可以建立一張包含所有 Linux 必要啟動檔案的開機 CD。此時，要求您的系統安裝有 CD 燒錄器。

使用 GRUB 建立可開機的 CD-ROM 只需要一個特殊形式的 *stage2* (稱為 *stage2_eltorito*)，並可以選用自定的 *menu.lst*。不需要典型的檔案 *stage1* 和 *stage2*。

過程 10.7 建立開機 CD

- 1 變更至要在其中建立 ISO 影像的目錄，例如：`cd /tmp`

- 2 為 GRUB 建立子目錄，然後變更至新建立的 *iso* 目錄：

```
mkdir -p iso/boot/grub && cd iso
```

- 3 將核心以及 *stage2_eltorito*、*initrd*、*menu.lst* 和 *message* 檔案複製到 *iso/boot/*：

```
cp /boot/vmlinuz boot/  
cp /boot/initrd boot/  
cp /boot/message boot/  
cp /usr/lib/grub/stage2_eltorito boot/grub  
cp /boot/grub/menu.lst boot/grub
```

- 4 以 *root (cd)* 取代 *root (hdx, y)* 項目，以指向 CD-ROM 設備。您可能還需要調整訊息檔案、核心和 *initrd* 的路徑 — 它們須分別指向 */boot/message*、*/boot/vmlinuz* 和 */boot/initrd*。調整之後，*menu.lst* 的內容應類似於下面的範例：

```
timeout 8  
default 0  
gfxmenu (cd)/boot/message  
  
title Linux  
root (cd)  
kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \  
splash=verbose showopts  
initrd /boot/initrd
```

使用 *splash=silent* (而非使用 *splash=verbose*) 讓開機訊息不要出現在開機程序中。

5 使用以下指令建立 ISO 影像：

```
genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot \  
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 \  
-o grub.iso /tmp/iso
```

6 使用您偏好的公用程式，將產生的檔案 `grub.iso` 燒錄至光碟。請勿將 ISO 影像燒錄為資料檔案，而是在您的燒錄公用程式中使用燒錄 CD 影像的選項。

10.5 圖形化 SUSE 畫面

如果使用 `vga=值` 選項做為核心參數，則圖形 SUSE 螢幕會顯示在第一個主控台上。如果您使用 YaST 來安裝，則會依照選取的解析度與圖形卡來自動啟用此選項。視需要，有三種方式可以停用 SUSE 畫面：

必要時停用 SUSE 畫面。

可以在指令行中輸入指令 `echo 0 >/proc/splash` 以停用圖形式畫面。

若要再次啟用它，請輸入 `echo 1 >/proc/splash`。

預設停用 SUSE 畫面。

您可以新增核心參數 `splash=0` 到開機載入程式的組態。如需更多詳細資訊，請參閱第 10 章「開機載入程式 *GRUB*」[109頁]。但是，如果您想使用文字模式（較早版本的預設值），請設定 `vga=normal`。

完全停用 SUSE 畫面

編譯新的核心且關閉「框架緩衝區支援」中的「使用開機顯示畫面而非開機標幟」選項。在核心中停用框架緩衝區支援，還會自動停用啟動畫面。

警告：不支援

如果您使用自定核心執行系統，SUSE 將無法為您的系統提供任何支援。

10.6 疑難排解

此章節列示使用 GRUB 啟動時，經常遇到的問題以及可能解決方案的簡要說明。部分問題已經在知識庫（網址為 <http://www.suse.com/support>）的文章中做了說明。使用搜尋對話方塊尋找 *GRUB*、開機和開機載入程式這類的關鍵字。

GRUB 和 XFS

XFS 在分割區啟動區塊中，不會保留空間給 `stage1`。因此，不要將 XFS 分割區指定成開機載入程式的位置。您可以建立不是以 XFS 格式化的個別開機分割區來解決這個問題。

GRUB 報告 GRUB 位置錯誤

GRUB 會在系統啟動時檢查連接硬碟的位置。有時候，BIOS 會傳回不一致的資訊，而且 GRUB 會報告 GRUB 位置錯誤。若出現此情況，請更新 BIOS。

如果 Linux 安裝在其他硬碟上，而且未註冊在 BIOS，GRUB 也會傳回此錯誤訊息。開機載入程式的 *stage1* 可以正確找到和載入，不過 *stage2* 則找不到。將新磁碟登錄在 BIOS 就可以解決此問題。

具有多個硬碟的系統無法開機

安裝時，YaST 可能已經判斷硬碟的開機順序錯誤。例如，GRUB 可能會將 PATA (IDE) 磁碟視為 `hd0`，將 SCSI 磁碟視為 `hd1`，即使 BIOS 中的開機順序與此相反，即 SCSI 先於 PATA。

發生此狀況，在啟動程序時，透過 GRUB 指令行的協助來更正硬碟。在系統啟動之後，編輯 `device.map` 來永久套用新的對應。然後檢查檔案 `/boot/grub/menu.lst` 和 `/boot/grub/device.map` 中的 GRUB 設備名稱，然後使用以下指令，重新安裝開機載入程式：

```
grub --batch < /etc/grub.conf
```

從第二顆硬碟啟動 Windows

有些作業系統，例如 Windows，只可以從第一個硬碟啟動。在第一個硬碟以外的硬碟安裝類似作業系統時，會影響個別功能表項目的邏輯變更。

```
...
title windows
    map (hd0) (hd1)
    map (hd1) (hd0)
    chainloader (hd1,0)+1
...
```

在此範例中，Windows 是從第二個硬碟啟動。基於此目的，硬碟的邏輯順序是使用 `map` 變更的。此變更不會影響 GRUB 功能表檔案中的邏輯。因此，第二個硬碟必須指定成 `chainloader`。

10.7 如需更多資訊

如需關於 GRUB 更進一步的資訊，請參閱 <http://www.gnu.org/software/grub/>。另請參閱 grub info 頁面。您也可以在「技術資訊搜尋」搜尋關鍵字「GRUB」，取得關於特殊問題的相關資訊，網址是 <http://www.novell.com/support>。

UEFI (整合可延伸韌體介面)

UEFI (整合可延伸韌體介面) 是系統硬體隨附的韌體、系統的所有硬體元件與作業系統之間的介面。

UEFI 在 PC 系統上的應用越來越廣泛，正逐漸取代傳統的 PC-BIOS。例如，UEFI 可正確支援 64 位元系統並提供安全開機（「安全開機」，需要 2.3.1c 版或更高版本的韌體），這是它最重要的功能之一。最後但同樣重要的是，透過 UEFI，所有 x86 平台上都將可以使用標準韌體。

UEFI 另外還提供下列優勢：

- 從具有 GUID 分割區表 (GPT) 的大型磁碟 (超過 2 TiB) 開機。
- 獨立於 CPU 的結構和驅動程式。
- 具有網路功能的彈性作業系統前環境。
- CSM (相容性支援模組) 可支援透過類似於 PC-BIOS 模擬功能將舊版作業系統開機。

如需詳細資訊，請參閱http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface。下列各節並不是一般性的 UEFI 綜覽，只是有關如何在 SUSE Linux Enterprise 中實作某些功能的提示。

11.1 安全開機

在 UEFI 的領域里，保護開機程序即表示建立一條信任鏈。「平台」是此信任鏈的根；在 SUSE Linux Enterprise 的網路位置中，主機板和板載韌體可視為「平台」。或者換另一種說法，它就是硬體廠商，信任鏈由該硬體廠商流向元件製造商、作業系統廠商等。

信任透過公用金鑰加密來表示。硬體廠商將所謂的「平台金鑰 (PK)」放入韌體中，表示信任的根。與作業系統廠商及其他的信任關係透過使用「平台金鑰」簽署其金鑰加以記錄。

最後，要求任何程式碼必須由其中一個「信任」金鑰簽署後，韌體才將執行程式碼，以此構建安全性——可以是作業系統開始載入程式、位於某些 PCI Express 卡之快閃式記憶體內或磁碟上的一些驅動程式，也可以是韌體本身的更新。

實質上，如果您要使用安全開機，則需要使用韌體信任的金鑰簽署作業系統載入程式，並且需要作業系統載入程式來驗證其載入的核心是否受信任。

金鑰交換金鑰 (KEK) 可新增至 UEFI 金鑰資料庫。這樣一來，您便可以使用其他證書，只要這些證書是以 PK 的私密部分簽署的即可。

11.1.1 在 SUSE Linux Enterprise 上實作

預設會安裝 Microsoft 的金鑰交換金鑰 (KEK)。

注意：需要 GUID 分割區表 (GPT)

安全開機功能要求 GUID 分割區表 (GPT) 以主開機記錄 (MBR) 取代舊分割區。

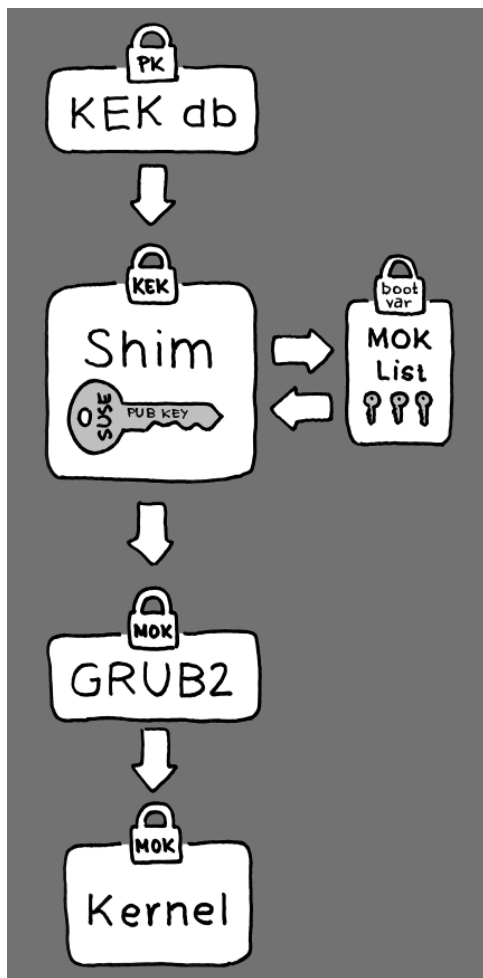
如果 YaST 在安裝期間偵測到 EFI 模式，它將會嘗試建立 GPT 分割區。UEFI 需要在 FAT 格式 EFI 系統分割區 (ESP) 上找到 EFI 程式。

支援 UEFI 安全開機本質上需要具有韌體辨識為信任金鑰之數位簽名的開機載入程式。為了對 SUSE Linux Enterprise 客戶有幫助，韌體先天地信任該金鑰，不需要任何手動介入。

實現此目的方法有兩種。一種方法是與硬體廠商協作，讓他們簽署一個 SUSE 金鑰，隨後 SUSE 會使用它來簽署開機載入程式。另一種方法是執行 Microsoft 的 Windows Logo Certification 程式認證開機載入程式，並讓 Microsoft 辨識 SUSE

簽署金鑰 (即，使用其 KEK 進行簽署)。目前，SUSE 透過 UEFI 簽署服務 (在此範例中為 Microsoft) 來簽署載入程式。

圖形 11.1 UEFI：安全開機程序



在實作層，SUSE 使用 shim 載入程式——這是一個智慧型解決方案，它可避免法律問題並大大簡化了認證和簽署步驟。shim 載入程式的工作是載入開機載入程式 (例如 eLILO 或 GRUB2) 並對它進行驗證；此開機載入程式接著會僅載入 SUSE 金鑰簽署的核心。SUSE 在全新安裝的 SLE11 SP3 上提供此功能，並啟用 UEFI 安全開機。

信任使用者的類型有兩種：

- 第一種是擁有金鑰的使用者。平台金鑰 (PK) 幾乎允許所有作業。金鑰交換金鑰 (KEK) 允許 PK 允許的所有作業，變更 PK 除外。
- 第二種是擁有實際存取機器權限的任何人。擁有實際存取機器權限的使用者可以將機器重新開機並設定 UEFI。

UEFI 提供兩種類型的變數來滿足那些使用者的需求：

- 第一種是所謂的「已驗證變數」，這些變數可透過開機程序 (所謂的「開機服務環境」) 和執行中的作業系統進行更新，但前提是使用簽署變數舊值的金鑰來簽署變數的新值。並且它們只能附加至或變更為序號更高的值。
- 第二種稱為「僅開機服務變數」。開機程序期間執行的所有程式碼都可以存取這些變數。在開機程序結束之後並在作業系統啟動之前，開機載入程式必須呼叫 `ExitBootServices` 呼叫。此後，這些變數無法再存取，且作業系統無法更改它們。

各種 UEFI 金鑰清單屬於第一種類型，因為此類型允許線上更新與新增金鑰、驅動程式和韌體指紋，以及將它們列入黑名單。第二類變數「僅開機服務變數」可協助以安全且開放原始碼友善的方式實作安全開機，因此可與 GPLv3 相容。

SUSE 以 shim 開始，它是一個小而簡單的 EFI 開機載入程式，最初由 Fedora 開發。它由 SUSE KEK 簽署的證書和 Microsoft 發放的證書共同簽署，以系統上 UEFI 金鑰資料庫中可用的 KEK 為基礎。

這允許 shim 載入並執行。

shim 隨後會繼續驗證它要載入的開機載入程式是否受信任。在預設情況下，shim 將會使用內嵌於其主體的獨立 SUSE 證書。此外，shim 將允許「註冊」額外的金鑰，並覆寫預設的 SUSE 金鑰。在下文中，我們稱它們為「機器擁有者金鑰」，或簡稱為 MOK。

接著，開機載入程式會在驗證核心後將其開機，核心繼而將對模組執行同樣的操作。

11.1.2 MOK (機器擁有者金鑰)

如果使用者(「機器擁有者」)要取代開機程序的任何元件，將會使用機器擁有者金鑰(MOK)。mokutils 工具將會協助簽署元件並管理 MOK。

當 shim 載入時，註冊程序便會開始將機器重新開機並中斷開機程序(例如按某個按鈕)。隨後，shim 將進入註冊模式，允許使用者以開機分割區上之檔案中的金鑰取代預設 SUSE 金鑰。如果使用者選擇這麼做，shim 隨後將會計算該檔案的雜湊，並將結果置於「僅開機服務」變數中。這允許 shim 偵測對開機服務以外之檔案所進行的任何變更，從而避免篡改使用者核准的 MOK 清單。

所有這些操作都在開機期間進行—現在僅執行已驗證的程式碼。因此，僅顯示於主控台的使用者可以使用機器擁有者的金鑰組。它不能是可以遠端存取作業系統的惡意軟體或駭客，因為駭客或惡意軟體只能變更檔案，而無法變更儲存在「僅開機服務」變數中的雜湊。

開機載入程式一旦載入並經 shim 驗證，便會在要驗證核心時招呼 shim，以避免驗證碼重複。Shim 將對此使用相同的 MOK 清單，並通知開機載入程式是否可以載入該核心。

如此一來，您便可以安裝您自己的核心或開機載入程式。您只需要安裝一組新的金鑰，隨後真實存在於第一次重新開機期間，由此對它們進行授權。因為 MOK 是一個清單而不僅僅是一個 MOK，所以您可以從多個不同的廠商建立 shim 信任金鑰，從而允許從開機載入程式進行雙重或多重開機。

11.1.3 將自定核心開機

下文以 http://en.opensuse.org/openSUSE:UEFI#Booting_a_custom_kernel 為基礎。

安全開機不會阻止您使用自我編譯的核心。您只須使用您自己的證書簽署該核心，並讓韌體或 MOK 知道該證書。

1 建立用於簽署的自定 X.509 金鑰和證書：

```
openssl req -new -x509 -newkey rsa:2048 -keyout key.asc \
-out cert.pem -nodes -days 666 -subj "/CN=$USER/"
```

如需建立證書的詳細資訊，請參閱http://en.opensuse.org/openSUSE:UEFI_Image_File_Sign_Tools#Create_Your_Own_Certificate。

2 將金鑰和證書封裝成 PKCS#12 結構：

```
openssl pkcs12 -export -inkey key.asc -in cert.pem \
    -name kernel_cert -out cert.p12
```

3 產生 NSS 資料庫以與 pesign 配合使用：

```
certutil -d . -N
```

4 將 PKCS#12 中包含的金鑰和證書輸入到 NSS 資料庫中：

```
pk12util -d . -i cert.p12
```

5 使用 pesign 以新簽名「保護」核心：

```
pesign -n . -c kernel_cert -i arch/x86/boot/bzImage \
    -o vmlinuz.signed -s
```

6 列出核心影像上的簽名：

```
pesign -n . -S -i vmlinuz.signed
```

此時，您可以如一般方式在 `/boot` 中安裝核心。因為核心現在已有自定簽名，所以需要將用於簽署的證書輸入到 UEFI 韌體或 MOK 中。

7 將證書轉換為 DER 格式以便輸入到韌體或 MOK 中：

```
openssl x509 -in cert.pem -outform der -out cert.der
```

8 將證書複製到 ESP 以方便存取：

```
sudo cp cert.der /boot/efi/
```

9 使用 mokutil 自動啟動 MOK 清單。

或者，如果要手動啟動 MOK，請按照下面的程序操作：

9a 重新開機

9b 在 GRUB 功能表中，按「c」鍵。

9c 類型：

```
chainloader $efibootdir/MokManager.efi  
boot
```

9d 選取「從磁碟註冊金鑰」。

9e 導覽到 `cert.der` 檔案並按 **Enter**。

9f 遵循指示註冊金鑰。一般情況下，應按「0」後再按「y」進行確認。

或者，韌體功能表可能提供將新金鑰新增至簽名資料庫的方法。

11.1.4 限制

以安全開機模式開機時，必須遵守下列限制：

- UEFI 系統上無法將混合 ISO 影像辨識為可開機。因此，SP3 不支援從 USB 設備執行 UEFI 開機。
- 為了確保無法輕易規避安全開機，當在安全開機模式下執行時，系統會停用部分核心功能。
- 必須簽署開機載入程式、核心和核心模組。
- 將會停用 `kexec` 和 `kdump`。
- 將會停用休眠 (暫停磁碟上的作業)。
- 無法存取 `/dev/kmem` 和 `/dev/mem`，即使以 `root` 使用者身分也不行。
- 無法存取 I/O 埠，即使以 `root` 使用者身分也不行。所有 X11 圖形驅動程式都必須使用核心驅動程式。
- 不允許透過 `sysfs` 存取 PCI BAR。
- 無法使用 ACPI 中的 `custom_method`。
- 無法使用適用於 `asus-wmi` 模組的 `debugfs`。

- `acpi_rsdp` 參數對核心不起任何影響。

11.2 更多資訊

- <http://www.uefi.org> —UEFI 首頁，您可在其中找到最新的 UEFI 規格。
- Olaf Kirch 和 Vojtěch Pavlík 發佈的部落格文章 (上述章節主要取自這些文章):
 - <http://www.suse.com/blogs/uefi-secure-boot-plan/>
 - <http://www.suse.com/blogs/uefi-secure-boot-overview/>
 - <http://www.suse.com/blogs/uefi-secure-boot-details/>
- <http://en.opensuse.org/openSUSE:UEFI> —UEFI 與 openSUSE。

特殊系統功能

本章會提供各種軟體套件、虛擬主控台及鍵盤配置的相關資訊。還會介紹 `bash`、`cron` 和 `logrotate` 等軟體元件，因為這些元件較之上一版有所變更或加強。這些元件也許不很重要，但與系統的關係密切，使用者可能想變更它們的預設動作。本章最後一節則會介紹語言與國家特定的設定 (I18N 與 L10N)。

12.1 特殊軟體套件的資訊

程式 `bash`、`cron`、`logrotate`、`locate`、`ulimit` 和 `free`，對系統管理員和許多使用者而言十分重要。`man` 頁面和 `info` 頁面是兩個很有用的指令資訊來源，但並非隨時都能使用。`GNU Emacs` 是非常普遍而且很好設定的文字編輯器。

12.1.1 `bash` 套件與 `/etc/profile`

`Bash` 是預設的系統外圍程序。如果以它做為登入外圍程序，可以讀取多種啟始化檔案。`Bash` 會以它們顯示在清單中的順序來處理。

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

在 `~/.profile` 或 `~/.bashrc` 中進行自定設定。為了要確保這些檔案能正確的處理，您必須將基本設定從 `/etc/skel/.profile` 或 `/etc/skel/.bashrc` 中複製至使用者的主目錄。建議您在更新後從 `/etc/skel` 複製設定。請執行下列的外圍程式指令，以避免遺失您調整過的設定。

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

然後個人的調整設定需要從 `*.old` 檔案再複製回去。

12.1.2 cron 套件

如果您需要按預先定義的時間，在背景中定期自動執行指令，則可以使用 `cron` 工具。`cron` 由採用特殊格式的時間表驅動。其中一些表格是由系統提供，使用者也可以視需要撰寫自己的表格。

`cron` 表格現在位於 `/var/cron/tabs`。`/etc/crontab` 做為整個系統的 `cron` 表格。在時間表格之後、指令之前，輸入要直接執行指令的使用者名稱。在 範例 12.1 「`/etc/crontab` 中的項目」[140頁] 中，則是輸入 `root`。位於 `/etc/cron.d` 的套件專用表格有相同的格式。請參閱 `cron man` 頁面 (`man cron`)。

範例 12.1 `/etc/crontab` 中的項目

```
1-59/5 * * * * root    test -x /usr/sbin/atrun && /usr/sbin/atrun
```

您不能呼叫 `crontab -e` 指令來編輯 `/etc/crontab`。這個檔案必須直接載入編輯器中，然後進行修改和儲存。

有些套件會將外圍程式程序檔安裝至 `/etc/cron.hourly`、`/etc/cron.daily`、`/etc/cron.weekly` 及 `/etc/cron.monthly` 目錄中，由 `/usr/lib/cron/run-crons` 控制其執行。`/usr/lib/cron/run-crons` 每隔 15

分鐘會從主表格 (/etc/crontab) 執行一次。這會保證被忽略的程序可以在適當的時間執行。

若要在自定的時間執行 hourly、daily 或其他定期維護程序檔，請定期使用 /etc/crontab 項目移除時戳檔案 (請參閱範例 12.2 「/etc/crontab：移除時戳檔案」 [141頁]，它可以在每個整點前移除 hourly，在每天凌晨的 2:14 移除 daily 等)。

範例 12.2 /etc/crontab：移除時戳檔案

```
59 * * * * root rm -f /var/spool/cron/lastrun/cron.hourly
14 2 * * * root rm -f /var/spool/cron/lastrun/cron.daily
29 2 * * 6 root rm -f /var/spool/cron/lastrun/cron.weekly
44 2 1 * * root rm -f /var/spool/cron/lastrun/cron.monthly
```

或者，可以將 /etc/sysconfig/cron 中的 DAILY_TIME 設定為 cron.daily 啟動的時間。MAX_NOT_RUN 設定確保日常任務能夠觸發並加以執行，即使使用者在長時間內均未於指定的 DAILY_TIME 開啟電腦。MAX_NOT_RUN 的最大值為 14 天。

為明確起見，日常系統維護工作會配送至不同的程序檔。它們包含在 aaa_base 套件中。例如，/etc/cron.daily 中有 suse.de-backup-rpmdb、suse.de-clean-tmp 或 suse.de-cron-local 元件。

12.1.3 記錄檔：套件 logrotate

某些系統服務 (精靈) 以及核心本身，會定期將系統狀態與特定事件記錄到記錄檔中。這樣，管理員可以定期檢查某個時間點的系統狀態、找出錯誤或有問題的功能，並用精確的方式來排除它們。這些記錄檔通常以 FHS 所指定的方式儲存於 /var/log，而且會日益增大。logrotate 套件有助於控制這些檔案增大的方式。

使用檔案 /etc/logrotate.conf 來設定 logrotate。尤其 include 規格主要是設定其他要讀取的檔案。產生記錄檔的程式會在 /etc/logrotate.d 中單獨安裝組態檔。例如，套件 apache2 (/etc/logrotate.d/apache2) 與 syslogd (/etc/logrotate.d/syslog) 隨附的檔案。

範例 12.3 /etc/logrotate.conf 的範例

```
# see "man logrotate" for details
# rotate log files weekly
weekly
```

```
# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#   monthly
#   create 0664 root utmp
#   rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotate 是透過 cron 來控制，並且每日是經由 /etc/cron.daily/logrotate 來呼叫。

重要

create 選項會讀取 /etc/permissions* 中由管理員所做的所有設定。請確定個人的修改不會造成衝突。

12.1.4 locate 指令

可以快速尋找檔案的 locate 指令，未包含在軟體標準安裝的範圍內。若有需要，請安裝 findutils-locate 套件。updatedb 程序會在每晚自行啟動，或啟動系統後的 15 分鐘左右啟動。

12.1.5 ulimit 指令

利用 ulimit (*user limits*) 指令，您可以限制系統資源的使用，並顯示這些限制。ulimit 對於限制應用程式可使用的記憶體特別有用。利用它，可以避免應用程式佔用過多的系統資源，降低作業系統效能，甚至讓系統當機。

ulimit 可以搭配多種選項來使用。若要限制記憶體的使用，請利用 表格 12.1 「ulimit：設定使用者的資源」 [143頁] 中所列的選項。

表格 12.1 *ulimit*：設定使用者的資源

-m	最大的常駐集大小
-v	外圍程序可用的虛擬記憶體最大容量
-s	堆疊的最大大小
-c	所建立的核心檔案的最大大小
-a	將會報告所有目前限制

您可以在 `/etc/profile` 中設定全系統的項目。在此可建立核心檔案 (供程式設計人員除錯之用)。一般使用者無法增加系統管理員在 `/etc/profile` 中所指定的值，但可以在 `~/.bashrc` 中建立特殊的設定項目。

範例 12.4 *ulimit*：`~/.bashrc` 中的設定

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

記憶體配置的單位必須為 **KB**。如需詳細資訊，請參閱 `man bash`。

重要

並非所有的外圍程序都支援 `ulimit` 指示詞。在您根據這些限制的內含設定時，**PAM** (例如 `pam_limits`) 會提供全面的調整設定。

12.1.6 free 指令

`free` 指令顯示系統中總的可用與已用實體記憶體及交換空間，以及核心耗用的緩衝區和快取。*可用的RAM*的概念要回溯到聯合記憶體管理的年代之前。記憶

體要物盡其用的口號非常適用於 Linux。所以，Linux 一直致力於平衡快取，而不允許有剩餘或未使用的記憶體。

基本上，核心不會有任何應用程式或使用者資料的直接知識。相反地，它會在頁面快取中管理應用程式與使用者資料。如果記憶體不足，部份的記憶體資料會寫入交換分割區或檔案中，這部份一開始就能用 `mmap` 指令的協助來讀取 (請參閱 `man mmap`)。

核心也可以有其他的快取，例如 *slab* 快取，網路存取的快取資料會儲存於此處。這可以解釋 `/proc/meminfo` 中計數器之間的不同。它們大部分 (但非全部) 都可以透過 `/proc/slabinfo` 來存取。

不過，如果您的目標是要得知目前使用了多少 RAM，請在 `/proc/meminfo` 中尋找此資訊。

12.1.7 man 頁面和資訊頁面

某些 GNU 應用程式 (例如 `tar`) 不再支援 `man` 頁面。針對這些指令，請使用 `--help` 選項來取得 `info` 頁面的快速綜覽，這些頁面將提供更深入詳盡的說明。`Info` 是 GNU 的超文字系統。您可以輸入 `info info` 來讀取此系統的介紹。您可以輸入 `emacs -f info` 或直接在主控台中使用 `info`，以便使用 Emacs 檢視 `info` 頁面。您也可以使用 `tkinfo`、`xinfo` 或說明系統來檢視資訊頁面。

12.1.8 使用 man 指令選取 man 頁面。

若要閱讀 `man` 頁面，請輸入 `man man_page`。如果不同區段中存在同名的 `man` 頁面，所有的這些 `man` 頁面都會列出，並會顯示對應的區段號碼。請選取要顯示的那個頁面。如果您未在幾秒內輸入區段號碼，將會顯示第一個 `man` 頁面。

如果您要將此行為設定為預設系統行為，請在外圍程序啟始化檔案 (例如 `~/ .bashrc`) 中設定 `MAN_POSIXLY_CORRECT=1`。

12.1.9 GNU Emacs 的設定

GNU Emacs 是個複雜的工作環境。以下幾個小節包含在 GNU Emacs 啟動時組態檔案的處理情形。更多相關資訊可在 <http://www.gnu.org/software/emacs/> 取得。

啟動時，Emacs 會讀取多個檔案，其中包含使用者、系統管理員以及供應商的自定設定或預設組態設定。啟始化檔案 `~/.emacs` 會從 `/etc/skel` 安裝至個別使用者的主目錄。`.emacs` 接著會讀取 `/etc/skel/.gnu-emacs` 檔案。如果要自定程式，請將 `.gnu-emacs` 複製到主目錄 (利用 `cp /etc/skel/.gnu-emacs ~/.gnu-emacs` 指令)，並依照您的需求來設定。

`.gnu-emacs` 定義 `~/.gnu-emacs-custom` 檔案為自定檔案。如果使用者是使用 Emacs 中的自定選項來進行設定，這些設定會儲存至 `~/.gnu-emacs-custom` 中。

透過 SUSE Linux Enterprise Server，emacs 套件可將檔案 `site-start.el` 安裝至目錄 `/usr/share/emacs/site-lisp` 中。`site-start.el` 檔案會在啟始化檔案 `~/.emacs` 前載入。此外，`site-start.el` 會確保那些以 Emacs 附加套件來散佈的特定組態檔案皆能自動載入，例如 `psgml`。此類型的組態檔案也位於 `/usr/share/emacs/site-lisp` 中，並且會以 `suse-start-` 為開頭。本地系統管理員可在 `default.el` 中指定整個系統的設定。

有關這些檔案的詳細資訊可在 *Init File* 下的 Emacs 資訊檔案中取得：[info://emacs/InitFile](http://www.gnu.org/software/emacs/InitFile)。關於如何在需要時停止載入這些檔案的資訊，也可在此找到。

Emacs 的元件分成數個套件：

- emacs 基本套件。
- emacs-x11 (通常已安裝)：具有 X11 支援的程式。
- emacs-nox：沒有 X11 支援的程式。
- emacs-info：info 格式的線上文件。
- emacs-el：以 emacs lisp 編寫的未編譯文件庫檔案。執行期間用不到這類檔案。

- 需要時可安裝多種附加產品套件：emacs-auctex (LaTeX)、psgml (SGML 與 XML)、gnuserv (用戶端與伺服器作業) 以及其他。

12.2 虛擬主控台

Linux是多重使用者及多工的作業系統。這些功能的優點即使在獨立的個人電腦系統中一樣令人讚賞。在文字模式中，有六個虛擬主控台可用。使用Alt+F1到Alt+F6可以在虛擬主控台之間進行切換。第七個主控台保留給X使用，第十個主控台可以顯示核心訊息。您可以修改/etc/inittab檔案來指定較多或較少的主控台。

若要在不關閉主控台的情況下，從X切換到主控台，請使用Ctrl+Alt+F1到Ctrl+Alt+F6這些鍵。若要回到x，請按Alt+F7。

12.3 鍵盤配置

若要標準化程式的鍵盤配置，請變更下列的檔案：

```
/etc/inputrc  
/etc/X11/Xmodmap  
/etc/skel/.emacs  
/etc/skel/.gnu-emacs  
/etc/skel/.vimrc  
/etc/csh.cshrc  
/etc/termcap  
/usr/share/terminfo/x/xterm  
/usr/share/X11/app-defaults/XTerm  
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

這些變更僅會影響使用terminfo項目的應用程式，或其組態檔是被直接變更的應用程式(vi、emacs等等)。未隨附於此系統的應用程式必須相容於這些預設值。

在X下，可以按照/etc/X11/Xmodmap中的說明啟用組合鍵(複合鍵)。

使用X鍵盤延伸程式(XKB)，可以進行進一步的設定。GNOME(gswitchit)以及KDE(kxkb)桌面環境也會使用此延伸程式。

提示：如需更多資訊

XKB 的相關資訊，可參閱 `/usr/share/doc/packages/xkeyboard-config` 中所列的文件 (`xkeyboard-config` 套件的一部分)。

12.4 語言與國家專用的設定

本系統已在很大程度上進行了國際化，可以根據當地的需求進行修改。國際化 (*I18N*) 允許特定的當地語系化 (*L10N*)。I18N 與 L10N 這兩個縮寫是取首尾兩個字母，兩字母中間再加上省略的字母數目。

設定位於 `/etc/sysconfig/language` 中所定義的 `LC_` 變數。這不僅是指本地語言支援，還包括訊息 (語言)、字元集、排序順序、時間和日期、數字及貨幣等類別。每種類別都可以用自己的變數來直接定義，或用在 `language` 檔案中的主要變數來間接定義 (請參閱 `locale man` 頁面)。

`RC_LC_MESSAGES`、`RC_LC_CTYPE`、`RC_LC_COLLATE`、`RC_LC_TIME`、`RC_LC_NUMERIC`、`RC_LC_MONETARY`

這些變數會傳送到外圍程序，但不會包含 `RC_` 字首，並代表列出的類別。相關外圍程序設定檔會列於下面。目前的設定可以用 `locale` 指令來顯示。

`RC_LC_ALL`

此變數 (如果設定) 會覆寫先前所提到的變數值。

`RC_LANG`

如果沒有設定前面的變數，則此為備用變數。依照預設，只會設定 `RC_LANG`。這讓使用者更容易輸入自己的值。

`ROOT_USES_LANG`

有 `yes` 或 `no` 兩個變數。如果設為 `no`，`root` 始終可以在 `POSIX` 環境中作業。

變數可以用 `YaST sysconfig` 編輯器來設定 (請參閱第 9.3.1 節「使用 `YaST Sysconfig` 編輯器變更系統組態」[106頁])。這樣的變數值中包含語言碼、國碼、編碼及輔助按鍵。個別的元件會以特定的字元來連接：

```
LANG=<language>[_<COUNTRY>].<Encoding>[@<Modifier>]
```

12.4.1 一些範例

您必須將語言與國碼一起設定。語言設定必須符合 <http://www.evertype.com/standards/iso639/iso639-en.html> 和 <http://www.loc.gov/standards/iso639-2/> 中的標準 ISO 639。國碼列在 ISO 3166 中，請參閱 http://en.wikipedia.org/wiki/ISO_3166。

只有設定那些可以在 `/usr/lib/locale` 中找到的可用描述檔案的值，才會有意義。您可以用 `localedef` 指令從 `/usr/share/i18n` 中的檔案建立其他描述檔；描述檔屬於 `glibc-i18ndata` 套件的一部份。`en_US.UTF-8` (針對美式英文) 的描述檔可以用以下指令建立：

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

```
LANG=en_US.UTF-8
```

如果安裝期間選擇美式英文的話，則此為預設設定。如果您選擇了其他語言，則仍然可以使用該語言，但會以 **UTF-8** 做為字元編碼。

```
LANG=en_US.ISO-8859-1
```

這會將語言設成英文、國家設成美國、字元集設成 **ISO-8859-1**。此字元集並不支援歐元符號，但有時對於尚未支援 **UTF-8** 的程式卻非常實用。然後，有些程式將會評估定義字元集的 (此例為 **ISO-8859-1**) 的字串，像是 **Emacs**。

```
LANG=en_IE@euro
```

上方範例在語言設定中明確包括歐元符號。這項設定現在基本上已不再使用，因為 **UTF-8** 也涵蓋歐元符號。它只有在應用程式支援 **ISO-8859-15** 而不支援 **UTF-8** 時才有用。

在較早的版本中，對 `/etc/sysconfig/language` 進行任何變更之後，都需要執行 **SuSEconfig**。之後，**SuSEconfig** 會將變更寫入 `/etc/SuSEconfig/profile` 及 `/etc/SuSEconfig/csh.login`。登入時，這些檔案由 `/etc/profile` (對於 **Bash**) 或 `/etc/csh.login` (對於 **tcsh**) 讀取。

在近期的版本中，`/etc/profile.d/lang.sh` 取代了 `/etc/SuSEconfig/profile`，`/etc/profile.d/lang.csh` 取代了 `/etc/SuSEconfig/csh.login`。但如果這兩個舊檔案存在，登入系統時仍會讀取這兩個檔案。

現在，該程序的處理過程如下所示：

- 對於 **Bash**：/etc/profile 會讀取 /etc/profile.d/lang.sh，後者會分析 /etc/sysconfig/language。
- 對於 **tcsh**：在登入時，/etc/csh.login 會讀取 /etc/profile.d/lang.csh，後者會分析 /etc/sysconfig/language。

如此可確保對 /etc/sysconfig/language 的任何變更在下次登入相應的外圍程序時即會生效，而不必先執行 **SuSEconfig**。

使用者可以適當地編輯自己的 ~/.bashrc 來覆寫系統預設值。例如，若不想讓整個系統的程式訊息皆使用 en_US，請加入 LC_MESSAGES=es_ES，以便改用西班牙文來顯示訊息。

12.4.2 ~/.i18n 中的地區設定

如果您對區域設定的系統預設值不滿意，可以根據 **Bash** 指令碼語法在 ~/.i18n 中變更設定值。~/.i18n 中的項目會覆寫 /etc/sysconfig/language 中的系統預設值。使用相同的變數名稱，但不使用 RC_ 名稱空間字首。例如，以 LANG 取代 RC_LANG：

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

12.4.3 語言支援的設定

按照規定，在訊息類別中的檔案僅會儲存於對應的語言目錄中 (像是 en)，以便有備用可用。如果您將 LANG 設為 en_US，而且 /usr/share/locale/en_US/LC_MESSAGES 中的訊息檔案不存在的話，則它會回到 /usr/share/locale/en/LC_MESSAGES 中。

您也可以定義備用鍊，例如，不列塔尼文之於法文，或是加里斯亞文之於西班牙文之於葡萄牙文：

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

如有需要，請改用挪威文變體 Nynorsk 與 Bokmal (讓其他備用為 no):

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

或

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

請注意，在挪威文中，會以不同方式處理 LC_TIME。

如果無法適當的辨識界定位數群組的分隔符號，可能會發生問題。如果 LANG 設定為類似 de 的兩個字母的語言碼，但卻使用 /usr/share/lib/de_DE/LC_NUMERIC 中的定義檔 glibc，就會發生這種情形。因此，LC_NUMERIC 必須設定為 de_DE，讓系統能辨識分隔符號定義。

12.4.4 如需更多資訊

- *The GNU C Library Reference Manual* 的「Locales and Internationalization」一章。包含在 glibc-info 中。該套件可從 SUSE Linux Enterprise SDK 中取得。SDK 是 SUSE Linux Enterprise 的附加產品，可從 http://www.novell.com/developer/sle_sdk.html 下載。
- Markus Kuhn 所寫的 *UTF-8 and Unicode FAQ for Unix/Linux*，目前網址如下：
<http://www.cl.cam.ac.uk/~mgk25/unicode.html>。
- Bruno Haible 提供的 *Unicode-Howto*，可從以下網址取得：
<http://tldp.org/HOWTO/Unicode-HOWTO-1.html>。

印表機操作

SUSE® Linux Enterprise Server 可支援以多種類型的印表機進行列印，包括遠端網路印表機。您可以手動設定印表機，也可以使用 YaST。如需組態設定指示，請參閱第 8.5 節「設定印表機」(第 8 章「使用 YaST 設定硬體元件」, ↑部署指南)。圖形和指令行公用程式都可用來啟動和管理列印工作。如果您的印表機無法如預期般運作，請參閱第 13.7 節「疑難排解」[159頁]。

CUPS (Common Unix Printing System, 通用 UNIX 列印系統) 是 SUSE Linux Enterprise Server 中的標準列印系統。

印表機可藉由介面 (例如 USB 或網路) 和印表機語言加以區分。購買印表機時，請確定印表機的介面 (例如 USB 或平行埠) 是否也可在您的硬體上找到，並請確定印表機的語言符合所需。印表機可根據下列三種印表機語言來分類：

PostScript 印表機

Linux 和 Unix 內部列印系統以 PostScript 印表機語言產生和處理大部分列印工作。如果印表機可直接處理 PostScript 文件，且不需轉換到列印系統中其他階段，潛在錯誤來源的次數便會減少。

標準印表機 (PCL 和 ESC/P 語言)

雖然這些印表機語言很舊，它們仍在擴充以處理印表機的新功能。如果已知印表機語言，列印系統可以藉由 Ghostscript 的協助，將 PostScript 工作轉換為對應的印表機語言。此處理階段稱為解譯。最知名的語言是大多數 HP 印表機與類似產品使用的 PCL，以及 Epson 印表機使用的 ESC/P。這些印表機語言通常都受 Linux 支援，並可產生不錯的列印效果。Linux 可能無法提供一些特殊的印表機功能。除了 HP 所開發的 HPLIP (HP Linux Imaging and Printing, HP Linux 成像與列印) 之外，目前沒有印表機製造商在開發 Linux 驅動程式以及以開放原始碼授權的方式將驅動程式提供給 Linux 散發者。

專屬印表機 (也稱為 GDI 印表機)

這些印表機並不支援任何一般的印表機語言。它們使用自己的印表機語言，而當有新型號發行，那些語言也可能有所變更。這些印表機通常指有 Windows 驅動程式。如需相關資訊，請參閱第 13.7.1 節「沒有標準印表機語言模式支援的印表機」[159頁]。

在購買新印表機之前，請參考下列來源以檢查您想要購買的印表機之支援性：

<http://www.linuxfoundation.org/OpenPrinting/>

OpenPrinting 首頁，含印表機資料庫。資料庫會顯示最新的 Linux 支援狀態。但是，Linux 版本僅可與生產期間可用的驅動程式整合。因此，目前被評選為「完全支援」的印表機，在最新的 SUSE Linux Enterprise Server 版本發行之後，可能就將失去此稱號。因此，資料庫不一定能指出正確狀態，而僅提供估計值。

<http://pages.cs.wisc.edu/~ghost/>

Ghostscript 網頁。

`/usr/share/doc/packages/ghostscript-library/catalog.devices`
所含驅動程式的清單。

13.1 列印系統的工作流程

使用者會建立列印工作。列印工作包含要列印的資料和線上同時週邊作業器的資訊 (例如印表機的名稱或是印表機佇列的名稱)，另外還可以包含過濾器資訊 (例如印表機的特定選項)。

每一台印表機都至少有一個專屬的印表機佇列。暫存序列器會在佇列中列印工作，直到所需的印表機已準備好接收資料。當印表機備妥時，暫存序列器會透過過濾器與後端，傳送資料至印表機。

過濾器會將列印應用程式所產生的資料 (通常為 PostScript 或 PDF，但也會有 ASCII、JPEG 等) 轉換為印表機特定資料 (PostScript、PCL、ESC/P 等)。印表機的特性描述在 PPD 檔案中。PPD 檔案含有印表機特定選項以及在印表機上啟用它們所需的參數。過濾器系統可確保啟用使用者所選取的選項。

如果您是使用 PostScript 印表機，過濾器系統會將資料轉換為印表機特定的 PostScript。這並不需要印表機驅動程式。如果您使用非 PostScript 印表機，過濾

器系統會將資料轉換為印表機特定資料。這將需要印表機適用的印表機驅動程式。後端會從過濾器接收印表機特定的資料，然後將它傳送至印表機。

13.2 連接印表機的方法和通訊協定

有各種方法可將印表機連接到系統。CUPS 列印系統的組態無法辨識本地印表機和透過網路連接到系統的印表機。

► **System z:** CUPS 或 LPRng 不支援 z/VM 提供的可在本地連接到 IBM System z 大型主機的印表機或相似設備。在這些平台上，僅可透過網路列印。網路印表機的電纜必須根據印表機製造商的說明來安裝。 ◀

警告：在執行中的系統變更纜線連接

在將印表機連接到機器時，請不要忘記只有 USB 設備可在操作中插上和拔除。若要避免損壞您的系統或印表機，請先關機再變更任何非 USB 的連接。

13.3 安裝軟體

PPD (PostScript 印表機描述) 為描述內容 (如解析度) 和選項 (如雙面列印模組的可用性) 的電腦語言。這些描述是使用 CUPS 中各種印表機選項所需。沒有 PPD 檔案，列印資料會被轉送給處於「raw」狀態的印表機，這通常不是想要的狀態。在安裝 SUSE Linux Enterprise Server 時，會預先安裝很多 PPD 檔案。

若要設定 PostScript 印表機，最好的方法是取得適當的 PPD 檔。在標準安裝範圍中自動安裝的套件 `manufacturer-PPDs` 提供許多 PPD 檔案。請參閱第 13.6.2 節「各種套件中的 PPD 檔案」[157頁]和第 13.7.2 節「PostScript 印表機沒有可用的 PPD 檔案」[160頁]。

新的 PPD 檔案可儲存在 `/usr/share/cups/model/` 目錄中，或依照第 8.5.1.1 節「使用 YaST 新增驅動程式」(第 8 章「使用 YaST 設定硬體元件」, ↑部署指南) 中所述透過 YaST 新增到列印系統中。之後，便可在印表機設定期間選取該 PPD 檔案。

如果印表機製造商要求您安裝整個軟體套件，請謹慎處理。首先，這種安裝可能會導致 SUSE Linux Enterprise Server 無法提供支援，其次，列印指令的運作

方式可能不同，並且系統可能再也無法處理其他製造商的設備。基於此原因，不建議安裝製造商軟體。

13.4 網路印表機

網路印表機可支援各種通訊協定，有些甚至可同時支援。雖然大部分受支援的通訊協定已標準化，但有一些製造商還是會修改標準。這樣，製造商只會針對一部分作業系統提供驅動程式。不幸地，他們很少提供 Linux 驅動程式。目前的情況是，您無法以每一個通訊協定均能在 Linux 中順暢執行的假設來行事。因此，您必須試驗各種選項以達到功能性組態。

CUPS 支援 `socket`、`LPD`、`IPP` 和 `smb` 通訊協定。

`socket`

socket 指將純文字列印資料直接傳送到 TCP 通訊端的連線。經常使用的 `socket` 連接埠號碼為 9100 或 35。設備 URI (資源識別字串) 的語法為 `socket://印表機的 IP:連接埠`，例如 `socket://192.168.2.202:9100/`。

LPD (行列式印表機精靈，Line Printer Daemon)

RFC 1179 中有對 LPD 通訊協定的詳細介紹。在此通訊協定下，部分工作相關資料 (如印表機佇列的 ID) 會先於傳送實際列印資料傳送。因此，在設定 LPD 通訊協定時，必須指定印表機佇列。不同印表機製造商的執行具有足夠彈性接受任何名稱做為印表機佇列。如有需要，印表機手冊應該會指出要使用的名稱。通常使用 `LPT`、`LPT1`、`LP1` 或類似名稱。LPD 服務的連接埠號碼為 515。某個設備 URI 的範例為 `lpd://192.168.2.202/LPT1`。

IPP (網際網路列印通訊協定，Internet Printing Protocol)

IPP 是相對較新的通訊協定 (1999 年)，它以 HTTP 通訊協定為基礎。有了 IPP，可比使用其他通訊協定傳輸更多工作相關資料。CUPS 使用 IPP 進行內部資料傳輸。正確設定 IPP 必須要有列印佇列的名稱。IPP 的連接埠號碼為 631。設備 URI 的範例為 `ipp://192.168.2.202/ps` 和 `ipp://192.168.2.202/printers/ps`。

SMB (Windows 共享)

CUPS 也支援在連接到 Windows 共享的印表機上列印。此用途使用的通訊協定為 SMB。SMB 使用的埠號有 137、138 和 139。設備 URI 的範例為 `smb://user:password@workgroup/smb.example.com/printer`、

```
smb://user:password@smb.example.com/printer 和  
smb://smb.example.com/printer。
```

必須在設定組態之前決定印表機支援的通訊協定。如果製造商未提供所需資訊，可使用 `nmap` 指令 (隨附於 `nmap` 套件) 來確定通訊協定。`nmap` 會檢查主機上是否有開啟的連接埠。例如：

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

13.4.1 以指令行工具設定 CUPS

CUPS 可透過 `lpinfo`、`lpadmin` 與 `lpoptions` 等指令行工具來設定。您需要包含後端 (如並列和參數) 的設備 URI。若要判斷系統中的設備 URI 是否有效，請使用以下 `lpinfo -v | grep "://"` 指令：

```
# lpinfo -v | grep "://"
direct usb://ACME/FunPrinter%20XL
direct parallel:/dev/lp0
```

使用 `lpadmin`，CUPS 伺服器管理員可新增、移除或管理列印佇列。若要新增印表機佇列，請使用下列語法：

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

然後設備 (`-v`) 會變為可用 `queue` (`-P`)，使用指定的 PPD 檔案 (`-P`)。這表示如果要手動設定印表機，您必須知道 PPD 檔案以及設備 URI。

請勿使用 `-E` 做為第一選項。對於所有 CUPS 指令，第一個引數 `-E` 設定使用加密連接。若要啟用印表機，必須依照下列範例所示使用 `-E`：

```
lpadmin -p ps -v parallel:/dev/lp0 -P \  
/usr/share/cups/model/Postscript.ppd.gz -E
```

下列範例是設定網路印表機：

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \  
/usr/share/cups/model/Postscript-levell.ppd.gz -E
```

如需 `lpadmin` 的更多選項，請參閱 `lpadmin(8)` 的 `man` 頁面。

在印表機設定期間，某些選項會設成預設。可針對每一個列印工作修改這些選項 (視所使用的列印工具而定)。也可以使用 YaST 變更這些預設選項。使用指令行工具，可依下列方式設定預設選項：

- 1 首先，列出所有選項：

```
lpoptions -p queue -l
```

範例：

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

啟用的預設選項前面會加上星號(*)，用以識別。

- 2 以 lpadmin 變更選項：

```
lpadmin -p queue -o Resolution=600dpi
```

- 3 檢查新設定：

```
lpoptions -p queue -l
```

```
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

當一般使用者執行 lpoptions 時，設定會寫入 ~/.cups/lpoptions。然而，root 設定會寫至 /etc/cups/lpoptions。

13.5 由指令行開始列印

若要由指令行進行列印，請輸入 `lp -d 佇列名稱 檔案名稱`；請以相對應的名稱來取代 *佇列名稱* 及 *檔案名稱*。

有些應用程式有賴 lp 指令來進行列印。在此情況下，請在應用程式列印對話方塊中 (通常並未指定 *檔案名稱*) 輸入正確的指令，例如 `lp -d 佇列名稱`。

13.6 SUSE Linux Enterprise Server 中的特殊功能

CUPS 的許多功能已經可適用於 SUSE Linux Enterprise Server。此處涵蓋部份最重要的變更。

13.6.1 CUPS 與防火牆

執行 SUSE Linux Enterprise Server 的預設安裝後，SuSEFirewall2 即會啟用，且網路介面會設定為處於「外部區域」中，這會阻擋內送流量。如需 SuSEFirewall2 組態的詳細資訊，請參閱第 15.4 節「SuSEfirewall2」(第 15 章「*Masquerading and Firewalls*」, ↑*Security Guide*)。

13.6.1.1 CUPS 用戶端

CUPS 用戶端通常在位於防火牆之後的受信任網路環境中的一般工作站上執行。在此情況下，建議將網路介面設定為處於「內部區域」中，以便可從該網路中存取工作站。

13.6.1.2 CUPS 伺服器

如果 CUPS 伺服器位於受防火牆保護的受信任網路環境中，則應將網路介面設定為處於防火牆的「內部區域」中。建議您在受信任的網路環境中設定 CUPS 伺服器，否則請留心使用特殊防火牆規則與 CUPS 組態中的安全性設定加以保護。

13.6.2 各種套件中的 PPD 檔案

YaST 印表機組態使用安裝於 `/usr/share/cups/model/` 中的 PPD 檔案來設定 CUPS 的佇列。為了尋找適合印表機型號的 PPD 檔案，YaST 會對照硬體偵測期間確定的廠商和型號比較所有 PPD 檔案內的廠商和型號。基於此原因，YaST 印表機組態將從 PPD 檔案中取出的廠商和型號資訊產生資料庫。

僅使用 PPD 檔案且不使用其他資訊來源的組態，好處在於 `/usr/share/cups/model/` 中的 PPD 檔案可自由修改。例如，如果您只有 PostScript 印表機，通常不需要 `cups-drivers` 套件中的 Foomatic PPD 檔案，或 `gutenprint` 套件中的 Gutenprint PPD 檔案。您可以直接將 PostScript 印表機的 PPD 檔案複製到 `/usr/share/cups/model/` (如果在 `manufacturer-PPDs` 套件中尚未存在)，以達到印表機的最佳組態。

13.6.2.1 cups 套件中的 CUPS PPD 檔案

cups 套件中的一般 PPD 檔案已經以 PostScript Level 1 和 Level 2 印表機適當的 Foomatic PPD 檔案補充。

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

13.6.2.2 cups-drivers 套件中的 PPD 檔案

一般情況下，Foomatic 印表機過濾器 `foomatic-rip` 會與非 PostScript 印表機的 Ghostscript 搭配使用。適當的 Foomatic PPD 檔案有 `*NickName: ... Foomatic/Foomatic/Ghostscript driver` 和 `*cupsFilter: ... foomatic-rip` 的項目。這些 PPD 檔案位於 cups-drivers 套件中。

YaST 通常偏好 `manufacturer-PPD` 檔案。但如果沒有適合的 `manufacturer-PPD` 檔案，將會選取包含項目 `*NickName: ... Foomatic ...` (推薦) 的 Foomatic PPD 檔案。

13.6.2.3 gutenprint 套件中的 Gutenprint PPD 檔案

除了 `foomatic-rip` 之外，來自 Gutenprint (以前稱為 GIMP-Print) 的 CUPS 過濾器 `rastertogutenprint` 也可以用於許多非 PostScript 印表機。此過濾器和適合的 Gutenprint PPD 檔案可在 gutenprint 套件中找到。Gutenprint PPD 檔案位於 `/usr/share/cups/model/gutenprint/` 中，並含有項目 `*NickName: ... CUPS+Gutenprint` 和 `*cupsFilter: ... rastertogutenprint`。

13.6.2.4 位於 manufacturer-PPDs 套件中印表機製造廠商的 PPD 檔案

`manufacturer-PPDs` 套件包含具有充分自由授權的印表機製造廠商所發行的 PPD 檔案。PostScript 印表機應該以印表機製造廠商的適合 PPD 檔案來設定，因為有此檔案才可使用 PostScript 印表機的所有功能。YaST 偏好來自 `manufacturer-PPDs` 的 PPD 檔案。如果型號名稱不符，YaST 就無法使用

manufacturer-PPDs 套件中的 PPD 檔案。如果對於類似型號 (如 Funprinter 12xx 系列), manufacturer-PPDs 套件僅包含一個 PPD 檔案, 則可能出現此情況。在此情況下, 請手動分別選取 YaST 中的 PPD 檔案。

13.7 疑難排解

下列章節涵蓋印表機硬體和軟體最常遭遇的問題, 以及解決或避免這些問題的方式。涵蓋的主題包括 GDI 印表機、PPD 檔案和連接埠組態, 並討論了一般網路印表機問題、列印瑕疵、佇列處理。

13.7.1 沒有標準印表機語言模式支援的印表機

這些印表機不支援任何的一般印表機語言, 且只有特殊的專屬控制序列才能處理。因此它們僅可在製造廠商針對其開發驅動程式的作業系統版本上使用。GDI 是 Microsoft* 為繪圖設備所開發的程式設計介面。製造廠商通常只提供 Windows 適用的驅動程式, 而由於 Windows 驅動程式使用 GDI 介面, 因此這些印表機也稱為 *GDI 印表機*。實際問題不在於程式設計介面, 而是這些印表機僅可使用對應印表機型號的專用印表機語言處理。

部分 GDI 印表機可切換到 GDI 模式或某種標準印表機語言來操作。如果手邊有印表機手冊, 可以參閱其中內容。某些型號需要特殊的 Windows 軟體才能進行切換 (請注意, 從 Windows 列印時, Windows 印表機驅動程式可能都會將印表機切換回 GDI 模式)。對於其他 GDI 印表機, 則可以使用標準印表機語言的延伸模組。

部分製造廠商提供其印表機的專用驅動程式。專用印表機驅動程式的壞處在於, 其不保證可與安裝的列印系統搭配使用, 也不保證適用於各種硬體平台。相反的, 支援標準印表機語言的印表機不需依賴特殊的列印系統版本或特殊硬體平台。

與其費時費力研究如何讓專用 Linux 驅動程式運作, 購買一台支援標準印表機語言 (最好是 PostScript) 的印表機可能更符合成本效益。如此可一次解決所有驅動程式問題、減少安裝與設定特殊驅動程式軟體以及取得列印系統中新開發所需的驅動程式更新的需要。

13.7.2 PostScript 印表機沒有可用的 PPD 檔案

如果 `manufacturer-PPDs` 套件不包含適用於 PostScript 印表機的 PPD 檔案，可以使用印表機製造商提供的驅動程式 CD 中的 PPD 檔案，或從印表機製造商的網頁下載適合的 PPD 檔案。

如果 PPD 檔案以壓縮保存檔 (.zip) 或自解壓縮保存檔 (.exe) 形式提供，請以 `unzip` 解壓縮。首先，檢閱 PPD 檔案的授權條款。然後，請使用 `cupstestppd` 公用程式來檢查 PPD 檔案是否符合「Adobe PostScript Printer Description File Format Specification, version 4.3」(Adobe PostScript 印表機說明檔案格式規格，版本 4.3)。如果公用程式傳回「FAIL」，就表示 PPD 檔案非常嚴重，可能造成重大問題。應該要減少 `cupstestppd` 所報告的問題點。若有需要，請詢問印表機製造廠商以取得適合的 PPD 檔案。

13.7.3 平行埠

最安全的方法是將印表機直接連接到第一平行埠，並在 BIOS 中選取下列平行埠設定值：

- I/O 位址：378 (十六進位)
- 中斷：無關
- 模式：Normal、Spp 或 Output Only
- DMA：停用

如果沒有這些設定值，印表機無法在平行埠上定址，請依照 BIOS 中的設定值，以 0x378 的格式在 `/etc/modprobe.conf` 中明確輸入 I/O 位址。如果有兩個平行埠，I/O 位址分別設為 378 和 278 (十六進位)，請以 0x378,0x278 格式輸入。

如果沒有使用中斷 7，可以使用 範例 13.1「`/etc/modprobe.conf`：第一平行埠的中斷模式」[161 頁] 中所示的項目啟用。在啟用中斷模式之前，請檢查檔案 `/proc/interrupts` 以瞭解哪些中斷已經在使用中。只會顯示目前正在使

用中的中斷。這可能因為作用中的硬體元件而有變化。其他任何設備都不能使用平行埠的中斷。如果您不確定，請以 `irq=none` 使用輪詢模式。

範例 13.1 `/etc/modprobe.conf`: 第一平行埠的中斷模式

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

13.7.4 網路印表機連接方式

查明網路問題

將印表機直接連接到電腦。基於測試因素，請將印表機設為本地印表機。如果可以，問題便與網路相關。

檢查 TCP/IP 網路

TCP/IP 網路和名稱解析必須可作用。

檢查遠端 `lpd`

使用以下指令來測試是否可在主機上建立到 `lpd` (連接埠 515) 的 TCP 連接：

```
netcat -z host 515 && echo ok || echo failed
```

如果無法建立到 `lpd` 的連接，可能是 `lpd` 不在作用中，或是有基本網路問題。

以使用者 `root` 的身分，使用以下指令來查詢 (可能很長) 遠端主機上佇列的狀態報告，假使對應的 `lpd` 在作用中且主機接受查詢：

```
echo -e "\004queue" \  
| netcat -w 2 -p 722 host 515
```

如果 `lpd` 沒有回應，它可能不在作用中，或是有基本網路問題。如果 `lpd` 有回應，回應應該會顯示主機上的佇列為何無法列印。如果您收到類似範例 13.2 「來自 `lpd` 的錯誤訊息」 [161 頁] 中的回應，問題可能是由遠端 `lpd` 所造成的。

範例 13.2 來自 `lpd` 的錯誤訊息

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

檢查遠端 cupsd

CUPS 網路伺服器預設每 30 秒在 UDP 連接埠 631 上廣播一次其佇列。因而可以使用下面的指令來測試網路中是否有廣播 CUPS 網路伺服器。請確定在執行指令之前停止本地 CUPS 精靈。

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

如果廣播 CUPS 網路伺服器存在，輸出將如 範例 13.3 「來自 CUPS 網路伺服器的廣播」 [162頁] 中所示。

範例 13.3 來自 CUPS 網路伺服器的廣播

```
ipp://192.168.2.202:631/printers/queue
```

► **System z:** 請注意，IBM System z 乙太網路設備預設不會接收廣播。 ◀

可使用以下指令來測試是否可建立到主機上 cupsd (連接埠 631) 的 TCP 連線：

```
netcat -z host 631 && echo ok || echo failed
```

如果無法建立與 cupsd 的連接，則表明 cupsd 可能不在作用中或可能有基本的網路問題。假設對應的 cupsd 在作用中，而且主機可以接受查詢，則 `lpstat -h host -l -t` 會傳回 `host` 上所有佇列的狀態報告 (可能很大)。

此指令可用來測試主機上的佇列是否可接受由單一換行字元組成的列印工作。應該不會印出任何資料。可能會退出一張空白頁。

```
echo -en "\r" \  
| lp -d queue -h host
```

網路列印或列印伺服器盒疑難排解

在列印伺服器盒中執行的線上同時週邊作業器在執行大量列印工作時，有時會造成問題。這是列印伺服器盒中的線上同時週邊作業器所造成的，因此無法解決。處理方式是，透過 TCP 插槽將印表機直接連接到列印伺服器盒，以規避列印伺服器盒中的線上同時週邊作業器。請參閱第 13.4 節「網路印表機」 [154頁]。

利用此方法，可減少列印伺服器盒在不同資料格式之間的轉換問題 (TCP/IP 網路和本地印表機連接)。若要使用此方法，您必須知道列印伺服器盒上的 TCP 連接埠。如果印表機連接到列印伺服器盒且電源開啟，此 TCP 埠通常可在列印伺服器盒電源開啟一段時間之後，以 nmap 套件的 nmap 公用程式決定。例如，`nmap IP-address` 會傳送列印伺服器盒的以下輸出：

Port	State	Service
23/tcp	open	telnet
80/tcp	open	http
515/tcp	open	printer
631/tcp	open	cups
9100/tcp	open	jetdirect

此輸出表示連接到列印伺服器盒的印表機可透過連接埠 9100 上的 TCP 插槽定址。根據預設，nmap 僅會檢查幾個 `/usr/share/nmap/nmap-services` 中所列出一般熟知的連接埠。若要檢查所有可能的連接埠，請使用指令 `nmap -p from_port-to_port IP-address`。這可能會花費一些時間。如需詳細資訊，請參閱 nmap 的 `man` 頁面。

輸入以下指令

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

將字元字串或檔案直接傳送到對應連接埠以測試印表機是否可在此連接埠上定址。

13.7.5 列印成品損毀而無錯誤訊息

對列印系統而言，在 CUPS 後端完成資料至接收者 (印表機) 的資料傳輸時，列印工作便完成。如果接收者的進一步處理失敗 (例如，印表機無法列印印表機特定資料)，列印系統並不知道。如果印表機無法列印印表機特定資料，請選取更適合印表機的 PPD 檔案。

13.7.6 停用佇列

如果到接收者的資料傳輸在數次嘗試之後完全失敗，CUPS 後端 (如 USB 或 socket) 會向列印系統報告錯誤 (向 `cupsd`)。在報告資料傳輸失敗之前，允許失敗嘗試的次數，由後端決定。因為進一步的嘗試可能徒勞無功，`cupsd` 會停止對應佇列的列印。排除問題的起因之後，系統管理員必須以指令 `cupsenable` 重新啟動列印。

13.7.7 CUPS 瀏覽：刪除列印工作

如果 CUPS 網路伺服器透過瀏覽向用戶端主機廣播它的佇列，而且在用戶端主機上有適合的本地 `cupsd` 在作用中，用戶端 `cupsd` 會從應用程式接收列印工作，並將它們轉送給伺服器上的 `cupsd`。當伺服器上的 `cupsd` 接受列印工作時，系統會為其指定一個新工作號碼。因此，用戶端主機上的工作號碼和伺服器上的工作號碼不同。列印工作通常會立刻轉送，所以無法以用戶端主機上的工作編號來刪除，因為用戶端 `cupsd` 一旦將列印工作轉送給伺服器 `cupsd`，便認為列印工作已完成。

若要刪除伺服器上的列印工作，假使伺服器尚未完成列印工作(即尚未將工作完全傳送至印表機)，請使用類似 `lpstat -h cups.example.com -o` 的指令來決定伺服器上的工作編號。使用此工作號碼，伺服器上的列印工作便可刪除：

```
cancel -h cups.example.com queue-jobnumber
```

13.7.8 損毀的列印工作與資料傳輸錯誤

如果您在列印過程中關閉印表機或電腦，列印工作將保留在佇列中。一旦電腦(或印表機)重新開啟，列印工作將繼續進行。必須以 `cancel` 將損毀的列印工作從佇列中移除。

如果列印工作損毀，或是主機和印表機之間的通訊發生問題，印表機會印出數頁含有不明字元的紙張，因為它無法正確地處理資料。若要修正這種狀況，請執行下列步驟：

- 1 若要停止列印，請從噴墨印表機取出所有紙張，或是打開雷射印表機的紙匣。高品質的印表機會有按鈕可取消目前的列印成品。
- 2 列印工作可能仍在佇列中，因為只有將工作完全傳送到印表機之後，才會移除。使用 `lpstat -o` 或 `lpstat -h cups.example.com -o` 檢查目前佇列中的佇列。使用 `cancel queue-jobnumber` 或 `cancel -h cups.example.com queue-jobnumber` 刪除列印工作。
- 3 即使列印工作已從佇列刪除，部份資料可能仍會傳送到印表機。請檢查對應佇列的 CUPS 後端程序是否仍在執行中，並將它終止。例如，對於連接到平行埠的印表機，可使用指令 `fuser -k /dev/lp0` 來終止所有仍在存取印表機的程序(更精確的說，就是平行埠)。

- 4 將印表機關閉一段時間以完全重設印表機。然後裝入紙張並開啟印表機電源。

13.7.9 除錯 CUPS 列印系統

使用以下標準程序以找出 CUPS 列印系統中的問題：

- 1 設定 `/etc/cups/cupsd.conf` 中的 `LogLevel debug`。
- 2 停止 `cupsd`。
- 3 移除 `/var/log/cups/error_log*` 以避免必須搜尋很大的記錄檔。
- 4 啟動 `cupsd`。
- 5 重覆造成問題的動作。
- 6 檢查 `/var/log/cups/error_log*` 中的訊息以辨識問題的起因。

13.7.10 如需更多資訊

許多特定問題的解決方法在「SUSE 知識庫」(<http://www.suse.com/support/>) 中都有說明。請搜尋文字 CUPS 找到相關文章。

使用 udev 進行動態核心設備管理

14

核心可以新增或移除執行中系統內幾乎所有的設備。設備狀態的變更(已插入或移除設備)必須傳播至使用者空間。一旦插入並辨識出設備，就必須立刻進行設定。如果辨識到的設備狀態發生任何變更，必須通知該設備的使用者。udev 會提供所需的基礎結構，以便動態維護 `/dev` 目錄中的設備節點檔案和符號連結。udev 規則能將外部工具插入核心設備事件處理。如此，您可以自定 udev 設備處理，例如，新增特定的程序檔以在核心設備處理過程中執行，或是在設備處理過程中要求並輸入其他資料進行評估。

14.1 `/dev` 目錄

`/dev` 中的設備節點可用來存取對應的核心設備。透過 udev，`/dev` 目錄會反映核心的目前狀態。每個核心設備都有一個對應的設備檔案。如果設備與系統的連接中斷，該設備節點就會遭到移除。

`/dev` 目錄的內容保存在暫存檔案系統中，而且所有檔案都會在每次系統開機時顯示。根據系統設計，手動建立或修改的檔案在重新開機後都將遺失。無論可存放於 `/lib/udev/devices` 目錄的對應核心設備狀態為何，靜態檔案和目錄都必須存在於 `/dev` 目錄中。在系統啟動時，該目錄內容將複製到 `/dev` 目錄，並具備與 `/lib/udev/devices` 中檔案相同的擁有權和許可權。

14.2 核心 uevent 和 udev

`sysfs` 檔案系統會輸出必要的設備資訊。每個核心已偵測和啟始化的設備，都會建立包含其設備名稱的目錄。其中會包含設備特定的屬性內容。

每次新增或移除設備時，核心都會傳送 `uevent` 來通知 `udev` 此變更。`udev` 精靈會在啟動時從 `/etc/udev/rules.d/*.rules` 檔案中讀取並剖析一次所有指定的規則，然後將剖析結果保留在記憶體中。如果變更、新增或移除了規則檔案，精靈可以使用指令 `udevadm control reload_rules` 重新載入所有規則在記憶體內部的表示。此動作也可以在執行 `/etc/init.d/boot.udev reload` 時完成。如需有關 `udev` 規則及其語法的詳細資訊，請參閱第 14.6 節「透過 `udev` 規則影響核心設備事件的處理」[170頁]。

每個收到的事件都將與提供的規則集合進行比對。這些規則可新增或變更事件環境識別碼、要求要建立之設備節點的特定名稱、新增指向該節點的符號連結，或是新增要在設備節點建立後執行的程式。驅動程式核心 `uevent` 是從核心網路連結插槽接收。

14.3 驅動程式、核心模組和設備

核心匯流排驅動程式會查探設備。核心(kernel)會為每個偵測到的設備建立一個內部設備結構，而驅動程式核心(core)會向 `udev` 精靈傳送一個 `uevent`。匯流排設備會以特殊格式的 ID 識別本身，表明其為何種設備。通常這些 ID 會包含廠商和產品 ID，以及其他子系統特定值。每個匯流排都會指定自己的 ID 配置，即所謂的 `MODALIAS`。核心會接收這些設備資訊，並根據這些資訊設定 `MODALIAS` ID 字串，然後隨事件一起傳送該字串。例如，USB 滑鼠的 ID 字串將如下所示：

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

每個設備驅動程式都包含有設備可處理的已知別名清單。清單會包含在核心模組檔案本身。`depmod` 程式會讀取 ID 清單，並且為目前所有可用模組在核心的 `/lib/modules` 目錄中建立 `modules.alias` 檔案。透過此基礎結構，模組載入方式就會像在每次出現帶有 `MODALIAS` 識別碼的事件時呼叫 `modprobe` 一樣容易。如果是呼叫 `modprobe $MODALIAS`，此次呼叫就會比對設備的已組織設備別名和模組指定別名。如果有找到符合項目，該模組就可載入。以上這一切都是由 `udev` 自動觸發。

14.4 開機和初始設備設定

在 `udev` 精靈執行之前，於開機過程中發生的所有設備事件都會遺失，這是因為處理這些事件的基礎結構位於根檔案系統中，在該階段無法使用。為彌補這一損失，核心在 `sysfs` 檔案系統中之每部設備的設備目錄中都提供了一份 `uevent` 檔案。使用 `add` 寫入該檔案，核心便可重新傳送與開機期間所遺失的相同事件。負責 `/sys` 中所有 `uevent` 檔案的簡易迴圈，可以再次觸發所有事件，建立設備節點並執行設備設定。

例如，開機期間出現的 USB 滑鼠可能無法由早期的開機邏輯啟始化，這是因為當時尚無法使用驅動程式。設備探查事件遺失，而且無法找到設備的核心模組。`udev` 只需在根目錄檔案系統可用後向核心要求所有設備事件，這樣 USB 滑鼠設備的事件就會再次執行，因此並不需要手動搜尋可能連接的設備。現在，它會在已掛接根目錄檔案系統中找到核心模組，並讓 USB 滑鼠完成啟始化。

從使用者空間的角度，執行期間的設備冷插拔 (ColdPlud) 順序和設備探查並沒有明顯的不同。這兩種情況都會使用相同規則來進行比對，而且會執行相同的設定程式。

14.5 監控執行中的 `udev` 精靈

`udevadm monitor` 程式可用來視覺化驅動程式核心事件以及 `udev` 事件程序的時間。

```
UEVENT[1185238505.276660] add    /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV  [1185238505.279198] add    /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV  [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV  [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
```

```
UDEV [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

UEVENT 行會顯示核心已透過網路連結傳送的事件。UDEV 行會顯示已完成的 **udev** 事件處理常式。列印時間是百萬分之一秒。介於 UEVENT 和 UDEV 之間的時間是指 **udev** 處理此事件所耗費的時間，或者是 **udev** 精靈延遲執行以便此事件能與執行中相關事件同步的時間。例如，硬碟分割區的事件始終會等待主要磁碟設備事件完成，因為分割區事件可能與主要磁碟事件向硬體查詢的資料有關。

`udevadm monitor --env` 會顯示完整的事件環境：

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

udev 也會將訊息傳送到 `syslog`。控制哪些訊息要傳送到 `syslog` 的預設 `syslog` 優先程度是在 **udev** 的組態檔 `/etc/udev/udev.conf` 中指定。執行精靈的記錄優先程度可使用 `udevadm control log_priority=level/number` 來變更。

14.6 透過 **udev** 規則影響核心設備事件的處理

udev 規則可以比對核心新增至事件本身的任何內容，或者核心輸出到 `sysfs` 的任何資訊。規則也可向外部程式要求其他資訊。每個事件都會與所有指定規則進行比對。所有規則都位於 `/etc/udev/rules.d` 目錄中。

規則檔案中的每一行都包含至少一個鍵值組合。鍵類型共有兩種，包括比對和指定鍵。當所有比對鍵都與指定值相符時就會套用規則，而該指定值就會指定給指定鍵。相符規則可以指定設備節點的名稱、新增指向該節點的符號連結，或是在事件處理過程中執行指定的程式。如果找不到任何符合規則，就會使用預設的設備節點名稱來建立設備節點。如需有關規則語法和系統提供之用於比

對或輸入資料的鍵的詳細資訊，請參閱 `udev man` 頁面。以下範例規則提供了對 `udev` 規則語法的基本介紹。這些範例規則摘自 `/etc/udev/rules.d/50-udev-default.rules` 下的 `udev` 預設規則集。

範例 14.1 範例 `udev` 規則

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

主控台規則包含三個鍵：一個比對鍵 (`KERNEL`) 以及兩個指定鍵 (`MODE`、`OPTIONS`)。 `KERNEL` 比對規則用於搜尋類型為主控台的所有項目的設備清單。只有完全符合的項目才有效，才會觸發此規則讓其執行。 `MODE` 鍵用於將特殊權限指派給設備節點，在此案例中，僅此設備的擁有者才會被指派讀取與寫入權限。 `OPTIONS` 鍵用於將此規則做為要套用至所有此類型設備的最後一條規則。符合此特殊設備類型的任何後續規則都不會生效。

序列設備規則在 `50-udev-default.rules` 中雖已不再可用，但仍值得瞭解一下。它包含兩個比對鍵 (`KERNEL` 和 `ATTRS`) 與一個指派鍵 (`SYMLINK`)。 `KERNEL` 鍵用於搜尋類型為 `ttyUSB` 的所有設備。使用 `*` 萬用字元時，此鍵可比對多部此類設備。第二個比對鍵 `ATTRS` 用於檢查 `sysfs` 中針對 `ttyUSB` 設備的 `product` 屬性檔案是否包含特定字串。指派鍵 (`SYMLINK`) 用於觸發將符號連結新增至 `/dev/pilot` 下的此設備。此鍵中使用的運算子 (`+=`) 將告知 `udev` 額外執行此動作，即使先前或之後的規則會新增其他符號連結也是如此。由於此規則包含兩個比對鍵，因此僅當兩個條件均滿足時才適用。

印表機規則可處理 `USB` 印表機，它包含兩個比對鍵，必須同時套用這兩個鍵才能套用整個規則 (`SUBSYSTEM` 與 `KERNEL`)。三個指定鍵用於命名此設備類型 (`NAME`)、建立符號設備連結 (`SYMLINK`) 以及對此設備類型的成員進行分組 (`GROUP`)。在 `KERNEL` 鍵中使用 `*` 萬用字元可使其符合多部 `lp` 印表機設備。可以在 `NAME` 與 `SYMLINK` 鍵中使用替代項，透過內部設備名稱延伸這些字串。例如，第一部 `lp USB` 印表機的符號連結會讀取 `/dev/usb/lp0`。

核心韌體載入程式規則可讓 **udev** 在執行時期透過外部輔助程式程序檔載入其他韌體。**SUBSYSTEM** 比對鍵可搜尋韌體子系統。**ACTION** 鍵可檢查是否已新增任何屬於韌體子系統的設備。**RUN+=** 鍵可觸發執行 `firmware.sh` 程序檔以查找要載入的韌體。

某些一般特性適用於所有規則：

- 每條規則都包含一個或多個以逗號分隔的鍵值對。
- 鍵的操作由運算子決定。**udev** 規則支援多種不同的運算子。
- 每個指定值必須括在引號中。
- 規則檔案中的每一行都表示一條規則。如果某規則的長度超出一行，請將 \ 加入到不同行中，就如同在外圍程序語法中一樣。
- **udev** 規則支援符合 `*`、`?` 與 `[]` 模式的外圍程序式模式。
- **udev** 規則支援替代項。

14.6.1 在 **udev** 規則中使用運算子

建立鍵時，您可以根據要建立的鍵類型從多個不同的運算子中進行選擇。比對鍵通常僅用於尋找符合或明顯不符合搜尋值的值。比對鍵可包含以下運算子：

==

比較是否相等。如果鍵包含搜尋模式，則所有符合此模式的結果均有效。

!=

比較是否不相等。如果鍵包含搜尋模式，則所有符合此模式的結果均有效。

指派鍵可使用以下運算子：

=

將某個值指派給鍵。如果鍵先前包含值清單，則此鍵將重設並僅指派單一值。

+=

將某個值新增至包含項目清單的鍵。

:=

指派最終值。不允許後續規則再做任何變更。

14.6.2 在 udev 規則中使用替代項

udev 規則支援使用佔位符與替代項。使用方式與任何其他程序檔中的方式類似。在 udev 規則中可以使用以下替代項：

%r, \$root

依預設為設備目錄 /dev。

%p, \$devpath

DEVPATH 的值。

%k, \$kernel

KERNEL 的值或內部設備名稱。

%n, \$number

設備編號。

%N, \$temprnode

設備檔案的暫存名稱。

%M, \$major

設備的主要編號。

%m, \$minor

設備的次要編號。

%s{屬性}, \$attr{屬性}

sysfs 屬性的值 (由屬性指定)。

%E{變數}, \$attr{變數}

環境變數的值 (由變數指定)。

%c, \$result

PROGRAM 的輸出。

%%

% 字元。

\$\$

\$ 字元。

14.6.3 使用 udev 比對鍵

比對鍵定義要套用 udev 規則所必須滿足的條件。以下為可用的比對鍵：

ACTION

事件動作的名稱，例如新增或移除設備時的 add 或 remove。

DEVPATH

事件設備的設備路徑，例如 DEVPATH=/bus/pci/drivers/ipw3945，用於搜尋與 ipw3945 驅動程式相關的所有事件。

KERNEL

事件設備的內部 (核心) 名稱。

SUBSYSTEM

事件設備的子系統，例如 SUBSYSTEM=usb，適用於與 USB 設備相關的所有事件。

ATTR{ 檔案名稱 }

事件設備的 sysfs 屬性。例如，若要比對 vendor 屬性檔案名稱中包含的字串，可以使用 ATTR{vendor}=="On[sS]tream"。

KERNELS

讓 udev 向上搜尋符合設備名稱的設備路徑。

SUBSYSTEMS

讓 udev 向上搜尋相符設備子系統名稱的設備路徑。

DRIVERS

讓 udev 向上搜尋相符設備驅動程式名稱的設備路徑。

ATTRS{ 檔案名稱}

讓 udev 向上搜尋與 sysfs 屬性值相符之設備的設備路徑。

ENV{ 鍵}

環境變數的值，例如 ENV{ID_BUS}="ieee1394，用於搜尋與 FireWire 匯流排 ID 相關的所有事件。

PROGRAM

讓 udev 執行外部程式。若要成功執行，程式必須以離開碼零返回。RESULT 鍵可使用程式的輸出 (列印至 stdout)。

RESULT

比對上次 PROGRAM 呼叫的輸出字串。即可將此鍵包含於相同規則中 (如 PROGRAM 鍵)，也可含於後續規則中。

14.6.4 使用 udev 指定鍵

與上述比對鍵不同，指定鍵不會說明必須滿足的條件，而是將值、名稱和動作指定給 udev 維護的設備節點。

NAME

要建立之設備節點的名稱。如果規則已設定了節點名稱，則將忽略適用於此節點的所有其他含 NAME 鍵的規則。

SYMLINK

與要建立的節點相關聯之符號連結的名稱。可以為多項比對規則新增符號連結以便使用設備節點進行建立。您還可以使用空格字元分隔符號連結名稱，從而為一項規則中的一個節點指定多個符號連結。

OWNER、GROUP、MODE

新設備節點的權限。在此處指定的值將覆寫已編譯的任何項目。

ATTR{ 鍵}

指定要寫入事件設備之 sysfs 屬性的值。如果使用運算子 ==，也會使用此鍵來比對 sysfs 屬性的值。

ENV{ 鍵 }

告知 udev 將某變數輸出到環境中。如果使用運算子 ==，也會使用此鍵來比對環境變數。

RUN

告知 udev 將某程式新增至要為此設備執行的程式清單。對極短任務套用此項時要格外小心，以免封鎖此設備的其他事件。

LABEL

在 GOTO 可以跳轉之處新增一個標籤。

GOTO

告知 udev 跳過多項規則並根據 GOTO 鍵所參考之標籤對應的規則繼續。

IMPORT{ 類型 }

將變數載入事件環境，如外部程式的輸出。udev 可輸入多種不同類型的變數。如果未指定任何類型，udev 會根據檔案權限的可執行位元嘗試自行決定類型。

- program 可告知 udev 執行外部程式並輸入其輸出。
- file 可告知 udev 輸入文字檔。
- parent 可告知 udev 輸入父代設備中儲存的鍵。

WAIT_FOR_SYSFS

告知 udev 等待系統為特定設備建立指定的 sysfs 檔案。例如，
WAIT_FOR_SYSFS="ioerr_cnt" 通知 udev 等待，直到 ioerr_cnt 檔案建立。

OPTIONS

OPTION 鍵可以包含多個值：

- last_rule 告知 udev 忽略所有後續規則。
- ignore_device 告知 udev 完全忽略此事件。
- ignore_remove 告知 udev 忽略針對該設備的所有後續移除事件。

- `all_partitions` 告知 `udev` 為區塊設備上的所有可用分割區建立設備節點。

14.7 永久設備命名

動態設備目錄和 `udev` 規則基礎結構讓系統可以為所有磁碟設備提供固定名稱，無論設備的辨識順序或所使用的連線為何。核心所建立的每個相應區塊設備，都會採用針對特定匯流排、磁碟類型或檔案系統所設計的工具進行檢查。`udev` 會根據核心動態提供的設備節點名稱，維護指向設備的永久符號連結類別：

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

14.8 udev 使用的檔案

`/sys/*`

由 Linux 核心提供的虛擬檔案系統，可輸出所有目前已知設備。`udev` 用此資訊在 `/dev` 中建立設備節點。

`/dev/*`

動態建立的設備節點和開機時從 `/lib/udev/devices/*` 複製的靜態內容。

下列檔案和目錄包含了 `udev` 基礎結構的重要元件：

`/etc/udev/udev.conf`

`udev` 主組態檔。

`/etc/udev/rules.d/*`

`udev` 事件符合規則。

`/lib/udev/devices/*`

靜態 `/dev` 內容。

`/lib/udev/*`

`udev` 規則中呼叫的協助程式。

14.9 如需更多資訊

如需關於 `udev` 基礎結構的詳細資訊，請參閱下列 `man` 頁面：

`udev`

關於 `udev`、鍵、規則和其他重要組態問題的一般資訊。

`udevadm`

`udevadm` 可用於控制 `udev` 的執行時期行為、要求核心事件、管理事件佇列以及提供簡單的除錯機制。

`udev`

關於 `udev` 事件管理精靈的資訊。

X Window System

X Window System (X11) 是 UNIX 中既成現實標準的圖形化使用者介面。X 採網路結構，可讓應用程式在一個主機上啟動而在透過任何種類的網路 (LAN 或國際網路) 連接的其他主機上顯示。本章說明 X Window System 環境的安裝與最佳化，並提供有關在 SUSE® Linux Enterprise Server 中使用字型的背景資訊。

提示：IBM System z：設定圖形使用者介面

X.Org 不支援 IBM System z 的輸入或輸出設備。因此，本節說明的組態程序皆不適用。如需 IBM System z 的更多相關資訊，請參閱第 4 章「在 IBM System z 上安裝」(↑部署指南)。

15.1 手動設定 X Window System

依照預設，X Window System 是以 SaX2 介面設定的，如第 8.2 節「設定圖形卡和顯示器」(第 8 章「使用 YaST 設定硬體元件」, ↑部署指南) 中所述。但也可手動編輯組態檔案進行設定。

警告：錯誤的 X 組態可能會損壞您的硬體

進行 X Window System 組態時請務必小心。在完成組態之前，絕對不可以啟動 X Window System。錯誤設定的系統會對硬體造成無法挽回的損害 (特別是對固定頻率的監視器)。本書與 SUSE Linux Enterprise Server 的創作者對於產生的任何損害概不負責。本資訊是仔細研究的結果，但不保證提及的所有方法都正確以及不會損害您的硬體。

指令 `sax2` 可建立 `/etc/X11/xorg.conf` 檔案。這是 X Window System 的主要組態檔。這裡有您的圖形卡、滑鼠以及顯示器相關的所有設定。

重要：使用 X -configure

若之前嘗試 SUSE Linux Enterprise Server 的 SaX2 失敗，則請使用 `x -configure` 設定您的 X 設定。如果您的設定包含專屬的僅二進位驅動程式，則 `x -configure` 無法工作。

下列段落會描述組態檔 `/etc/X11/xorg.conf` 的結構。它由多個段落組成，每一個都會處理組態的某個層面。每一個段落以關鍵字 `Section` <designation> 開始，並以 `EndSection` 結束。下列轉換會套用到所有部份：

```
Section "designation"
    entry 1
    entry 2
    entry n
EndSection
```

可用的段落類型列出在 表格 15.1 「`/etc/X11/xorg.conf` 中的段落」 [180頁] 中。

表格 15.1 `/etc/X11/xorg.conf` 中的段落

類型	代表意義
Files	用於字型與 RGB 顏色表的路徑。
ServerFlags	伺服器行為的一般切換器。
Module	伺服器應載入的模組清單。
InputDevice	鍵盤和特殊輸入設備 (觸控板、搖桿裝置等) 之類的輸入設備均在此區段設定。這個段落含有 Driver 的重要參數以及定義 Protocol 與 Device 的選項。您每個連接到電腦的設備通常有一個 InputDevice 段落。

類型	代表意義
Monitor	所用的伺服器。此區段的重要元素包括 Identifier (稍後的 Screen 定義中會提及)、重新整理速率 VertRefresh 以及同步頻率限制 (HorizSync 和 VertRefresh)。設定值以 MHz、kHz 和 Hz 提供。通常，伺服器會拒絕和監視器規格不對應的模式行。這樣可防止不小心將太高的頻率送往顯示器。
Modes	特定螢幕解析度的模式行參數。這些參數可以由 SaX2 依據使用者給定的值計算，通常不需要變更。如果您要連接固定頻率監視器，現在可以手動變更。在 /usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO 目錄 (howtoenh 套件中提供) 中的 HOWTO 檔案中，可以找到各個數值之意義的詳細資料。若要手動計算 VESA 模式，可以使用 cvt 工具。例如，若要計算解析度為 1680x1050、頻率為 60Hz 之顯示器的模式行，請使用指令 <code>cvt 1680 1050 60</code> 。
Device	特定圖形卡。它以本身的描述名稱表示。本節中可用的選項主要取決於所用的驅動程式。例如，如果使用 i810 驅動程式，可以在手冊頁 <code>man 4 i810</code> 中找到有關可用選項的詳細資訊。
Screen	這個段落和 Monitor 以及 Device 一起構成 X.Org 所有必要的設定。

類型	代表意義
	<p>在 Display 子區段中，指定虛擬螢幕的大小(Virtual)、ViewPort，以及與該螢幕一起使用的 Modes。</p> <p>請注意，某些驅動程式要求所有使用的組態都必須存在於 Display 區段的某個位置。例如，如果您使用筆記型電腦並想要使用比內部 LCD 大的外部顯示器，則可能需要在 Modes 行末尾新增比內部 LCD 支援的解析度更高的解析度。</p>
ServerLayout	單螢幕顯示或多螢幕顯示組態的配置。這個段落連結輸入設備 InputDevice 和顯示設備 Screen。
DRI	提供資訊給「直接算圖基礎結構(DRI)」。

Monitor、Device 與 Screen 將做詳細說明。如需其他段落的進一步資訊，請參閱 X.Org 和 xorg.conf 的手冊頁。

xorg.conf 中可能有多個不同的 Monitor 和 Device 段落。也可能有多個 Screen 段落。ServerLayout 段落決定使用這些段落中的哪些段落。

15.1.1 Screen 段落

Screen 段落是由 monitor 和 device 段落組成，已決定要使用的解析度和色彩深度。Screen 段落可能如同 範例 15.1 「/etc/X11/xorg.conf 檔的螢幕段落」[182頁] 一般。

範例 15.1 /etc/X11/xorg.conf 檔的螢幕段落

```
Section "Screen"❶
    DefaultDepth 16❷
    SubSection "Display"❸
```



```

    Depth      16④
    Modes       "1152x864" "1024x768" "800x600"⑤
    Virtual     1152x864⑥
EndSubSection
SubSection "Display"
    Depth      24
    Modes       "1280x1024"
EndSubSection
SubSection "Display"
    Depth      32
    Modes       "640x480"
EndSubSection
SubSection "Display"
    Depth      8
    Modes       "1280x1024"
EndSubSection
Device        "Device[0]"
Identifier     "Screen[0]"⑦
Monitor        "Monitor[0]"
EndSection

```

- ① Section 決定段落類型，在此情況下為 Screen。
- ② DefaultDepth 決定若無指定色彩深度的話，預設使用的色彩深度。
- ③ 會為每種色彩深度指定不同的 Display 子段落。
- ④ Depth 決定與該組 Display 設定搭配使用的色彩深度。可能的值為 8、15、16、24 與 32，但並不是每個值都可用於所有 X 伺服器模組或解析度。
- ⑤ Modes 段落包括可能螢幕解析度的清單。X 伺服器將由左而右檢查這個清單。對於每一個解析度，X 伺服器會在 Modes 段落搜尋適合的 Modeline。Modeline 同時由顯示器與圖形卡的功能決定。Monitor 設定值將決定 Modeline 的結果。

第一個找到的解析度是 Default mode。按 **Ctrl + Alt + +** (數字鍵盤)，可以向右切換到清單中的下一個解析度。按 **Ctrl + Alt + -** (數字鍵盤)，可以切換到上一個解析度。您可以在 X 執行中變更解析度。

- ⑥ Display 子段落最後一行的 Depth 16 指虛擬螢幕大小。虛擬螢幕可能的最大大小由圖形卡上安裝的記憶體數量以及所要的色彩深度決定，而不是顯示器的最大解析度。如果省略此行，虛擬解析度便是實體解析度。因為目前的圖形卡都附有大量的視訊記憶體，您可以建立非常大的虛擬桌面。不過，如果將大部份的視訊記憶體用於虛擬桌面，將可能無法使用 3D 功能。例如，如果卡上有 16MB 的視訊 RAM，虛擬螢幕最大可使用 4096x4096 像素，8 位元色彩深度。不過，不建議將所有記憶體用於虛擬螢幕，特別是加速卡，因為卡的記憶體還要用於各種字型與圖形的快取。

- ⑦ Identifier 行 (此處為 Screen[0]) 對這個段落提供一個定義的名稱，以便對下列 ServerLayout 段落提供唯一性參照。Device 和 Monitor 行指定屬於這個定義的圖形卡和顯示器。它們透過本身對應的名稱或識別碼和 Device 以及 Monitor 段落連結。以下詳細討論這些段落。

15.1.2 Device 段落

Device 段落描述特定的圖形卡。xorg.conf 中的設備項目數沒有限制，但每一個設的名稱要使用關鍵字 Identifier (識別碼) 來區別。若您安裝多張圖形卡，段落將只依序編號。第一個稱為 Device[0]，第二個稱為 Device[1]，以下類推。以下檔案顯示摘自一台使用 Matrox Millennium PCI 圖形卡的電腦 (如 SaX2 所設定) 之 Device 區段的一段文字：

```
Section "Device"
    BoardName      "MGA2064W"
    BusID          "0:19:0"❶
    Driver         "mga"❷
    Identifier     "Device[0]"
    VendorName     "Matrox"
    Option         "sw_cursor"
EndSection
```

- ❶ BusID 表示要在其中安裝圖形卡的 PCI 或 AGP 插槽。這個值和指令 lspci 顯示的 ID 相符。X 伺服器需要十進位格式的詳細資料，但 lspci 以十六進位格式顯示這些值。SaX2 會自動偵測 BusID 的值。
- ❷ SaX2 會自動設定 Driver 的值，並指定您的圖形卡要使用的驅動程式。如果是 Matrox Millennium 圖形卡，驅動程式模組稱為 mga。X 伺服器會在定義於 drivers 子目錄的 Files 段落中的 ModulePath 中搜尋。在標準安裝中，此為 /usr/lib/xorg/modules/drivers 目錄或適用於 64 位元作業系統目錄的 /usr/lib 64/xorg/modules/drivers 目錄。名稱會附加 _drv.o，因此，如果是 mga 驅動程式，將載入驅動動程式檔案 mga_drv.o。

X 伺服器或驅動程式的行為可以透過附加的選項來操作。Device 段落中的選項 sw_cursor 便是一個範例。它可以停用硬體滑鼠游標並描述使用軟體的滑鼠指標。驅動程式模組不同，可用的選項也各異 (可以在 /usr/share/doc/packages/套件名稱目錄內驅動程式模組的描述檔案中找到)。通常情況下，也可以在手冊頁 (man xorg.conf、man 4 <驅動程式模組> 和 man 4 晶片) 中找到有效的選項。

如果圖形卡有多個視訊連接器，可將此卡的各個不同設備設定為單個檢視窗。請使用 **SaX2** 以此方式設定圖形介面。

15.1.3 Monitor 和 Modes 段落

和 **Device** 段落類似，**Monitor** 和 **Modes** 段落分別描述一個顯示器。組態檔 `/etc/X11/xorg.conf` 可以含有沒有個數限制的 **Monitor** 段落。每個 **Monitor** 段落都會參考帶有 **UseModes** 行 (若可用) 的 **Modes** 段落。如果沒有可用於 **Monitor** 段落的 **Modes** 段落，**X** 伺服器將從一般同步值計算適當的值。**ServerLayout** 段落指定相關的 **Monitor** 段落。

顯示器定義應該由有經驗的使用者進行設定。模式行是 **Monitor** 段落的重要組成部份。模式行可設定對應解析度的水平與垂直計時。顯示器內容，特別是允許的頻率，儲存在 **Monitor** 區段中。可以使用公用程式 `cvt` 產生標準 **VESA** 模式。如需詳細資訊，請參閱 `cvt` 手冊頁 (`man cvt`)。

警告

除非您深入瞭解監視器與圖形卡功能，否則請勿變更模式行，因為這樣做可能會嚴重損壞您的監視器。

想自行開發顯示器描述的人員，應非常熟悉 `/usr/share/X11/doc` 文件的內容。安裝 `xorg-x11-doc` 套件以尋找 **PDF** 與 **HTML** 頁面。

在今天，需要手動指定模式行的的情況非常少見。如果您使用先進的多頻顯示器，依規則，**X** 伺服器可以透過 **DDC** 直接從顯示器讀取允許頻率以及最佳解析度，如 **SaX2** 組態區段中所述。如果因某種原因而不適用，請使用 **X** 伺服器內附的一種 **VESA** 模式。此模式對大多數圖形卡與顯示器組合都起作用。

15.2 安裝與設定字型

在 **SUSE Linux Enterprise Server** 上安裝其他字型非常簡單。只要將字型複製到位於 **X11** 字型路徑中的任何目錄即可 (請參閱第 15.2.1 節「**X11** 核心字型」[186頁])。若要啟用字型，安裝目錄應為 `/etc/fonts/fonts.conf` 中所設定目錄的子目錄 (請參閱第 15.2.2 節「**Xft**」[187頁])，或以 `/etc/fonts/suse-font-dirs.conf` 包含於此檔案中。

以下內容摘自 `/etc/fonts/fonts.conf`。此檔案為適用於大多數組態的標準組態檔案。它還定義了包含目錄 `/etc/fonts/conf.d`。在此目錄中，所有以兩位數值開頭的檔案或符號連結將由 `fontconfig` 載入。關於此功能的詳細說明，請參閱 `/etc/fonts/conf.d/README`。

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/ .fonts</dir>
```

`/etc/fonts/suse-font-dirs.conf` 是自動產生的，目的是為了將 (多半是協力廠商) 應用程式 (如 LibreOffice、Java 或 Adobe Reader) 中包含的字型拉進來。常見項目如下所示：

```
<dir>/usr/lib/Adobe/Reader9/Resource/Font</dir>
<dir>/usr/lib/Adobe/Reader9/Resource/Font/PFM</dir>
```

若要在整個系統上安裝其他字型，請以 `root` 身分手動將字型檔案複製到合適的目錄，如 `/usr/share/fonts/truetype`。此外，這個作業可以透過「KDE 控制中心」中的 KDE 字型安裝程式來執行。結果完全相同。

您也可以建立符號連結，來替代複製實際字型。例如，如果您擁有掛接 Windows 分割區上的授權字型並且想要使用它們，便可能需要這樣做。接下來，請執行 `SuSEconfig --module fonts`。

`SuSEconfig --module fonts` 會執行指令碼 `/usr/sbin/fonts-config` 來處理字型組態。關於此指令碼的詳細資訊，請參閱其手冊頁 (`man fonts-config`)。

點陣字型、TrueType 與 OpenType 字型以及 Type1 (PostScript) 字型的程序完全相同。所有這些字型類型可安裝到任何目錄。

X.Org 包含兩種完全不同的字型系統：舊的「X11 核心字型系統」與新設計的「*Xft* 與 *fontconfig*」系統。以下數節簡短描述這兩種系統。

15.2.1 X11 核心字型

目前，X11 核心字型系統不僅支援點陣字型，也支援縮放字型如 Type1 字型、TrueType 與 OpenType 字型。縮放字型僅支援不需要消除鋸齒及子像素 (subpixel)

處理的字型，含有更多語言的文字符號之縮放字型所需的載入時間也越長。也支援 Unicode 字型，但是處理速度較慢且需要更多的記憶體。

X11 核心字型系統具有某些先天性的弱點。該字型系統已過時，無法再以任何有效的方法擴充。保留這種字型是為了回溯相容，但最好儘可能使用更先進的 Xft 和 fontconfig 系統。

為了能夠進行作業，X 伺服器必須知道它有哪些字型可用，以及系統中的哪些地方可以找到這些字型。這是由 FontPath 變數負責處理，該變數包含所有有效系統字型目錄的路徑。每個目錄中的 fonts.dir 檔案，可以列出目錄中可用的字型有哪些。FontPath 是 X 伺服器在啟動時產生的。它會在 /etc/X11/xorg.conf 組態檔案的 FontPath 項目中，搜尋一個有效的 fonts.dir 檔案。這些項目會在 Files 區段中找到。使用 xset q 顯示實際的 FontPath。也可以使用 xset 在執行時變更此路徑。若要新增其他路徑，請使用 xset+fp <path>。若要移除不要的路徑，請使用 xset-fp <path>。

如果 X 伺服器已經啟動，掛接目錄中新安裝的字型可以透過指令 xsetfp rehash 來設成可用。這個指令以 SuSEconfig--module fonts 執行。由於指令 xset 必須存取執行中的 X 伺服器，因此只有在 SuSEconfig--module fonts 是從可存取之執行中 X 伺服器的外圍程序啟動時才有效。實現此目的最簡單的方法是輸入 su 和 root 密碼，以取得 root 權限。su 可以將啟動 X 伺服器之使用者的存取權傳送到 root 外圍程序。要檢查字型是否安裝正確以及是否可以透過 X11 核心字型系統來使用，請使用 xlsfonts 指令來列出所有可用字型。

根據預設，SUSE Linux Enterprise Server 使用 UTF-8 地區設定。因此，最好使用 Unicode 字型 (在 xlsfonts 的輸出中，字型名稱的結尾為 iso10646-1)。xlsfonts | grep iso10646-1 可以列出所有可用的 Unicode 字型。SUSE Linux Enterprise Server 隨附的 Unicode 字型絕大部分都至少具有歐洲語言所需的文字符號 (舊編碼方式為 iso-8859-*)。

15.2.2 Xft

從一開始，Xft 的程式設計人員便確保了能支援平滑美觀的可縮放字型。如果使用 Xft，字型將由使用字型的應用程式處理，而不是如 X11 核心字型系統那樣由 X 伺服器處理。在這種方式，個別的應用程式需要存取實際字型檔並完全控制文字符號的處理方式。多種語言文字的正确顯示基礎便是由此構成。直接存

取字型檔對於在列印中內嵌字型，來保證列印出的外觀和螢幕輸出一致非常有用。

在 SUSE Linux Enterprise Server 中，KDE 和 GNOME 這兩個桌面環境、Mozilla 以及其他許多應用程式預設已使用 Xft。越來越多的應用程式已經從舊 X11 核心字型系統改用 Xft。

Xft 使用 `fontconfig` 程式庫來尋找字型以及操作字型的處理方式。`fontconfig` 的內容由全域組態檔案 `/etc/fonts/fonts.conf` 控制。特殊組態應新增至 `/etc/fonts/local.conf` 與使用者特定的組態檔案 `~/.fonts.conf`。這些 `fontconfig` 組態檔每一個都必須以下列開頭

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

並以下列結束

```
</fontconfig>
```

要新增字型搜尋目錄，請附加下列行：

```
<dir>/usr/local/share/fonts/</dir>
```

不過，通常並不需要這樣做。依預設，使用者專屬目錄 `~/.fonts` 已經輸入到 `/etc/fonts/fonts.conf` 中。因此，安裝額外的字型時，只要將它們複製到 `~/.fonts` 即可。

您還可以插入操作字型外觀的規則。例如，輸入

```
<match target="font">
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>
```

可以停用所有字型的消除鋸齒效果，或輸入

```
<match target="font">
  <test name="family">
    <string>Luxi Mono</string>
    <string>Luxi Sans</string>
  </test>
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>
```

可以停用特定字型的消除鋸齒效果。

依預設，大部份的應用程式都是使用字型名稱 `sans-serif` (或相等的 `sans`)、`serif` 或 `monospace`。這些都不是真實的字型，而是可以解析為適當字型的別名，視語言設定而定。

使用者很容易在 `~/.fonts.conf` 新增規則來將這些別名解析為屬意的字型：

```
<alias>
  <family>sans-serif</family>
  <prefer>
    <family>FreeSans</family>
  </prefer>
</alias>
<alias>
  <family>serif</family>
  <prefer>
    <family>FreeSerif</family>
  </prefer>
</alias>
<alias>
  <family>monospace</family>
  <prefer>
    <family>FreeMono</family>
  </prefer>
</alias>
```

因為幾乎所有的應用程式都預設使用這些別名，所以幾乎整個系統會受到影響。這樣，您幾乎可以簡單地隨處使用喜歡的字型而不必針對個別應用程式修改字型設定。

請使用指令 `fc-list` 來找出已安裝且可用的字型。例如，指令 `fc-list` 指令可傳回所有字型的清單。若要找出含有希伯來文 (`:lang=he`) 所有文字符號的可用縮放字型 (`:scalable=true`)、這些字型的名稱 (`family`)、樣式 (`style`)、粗細 (`weight`) 以及包含這些字型的檔案名稱，請輸入下列指令：

```
fc-list ":lang=he:scalable=true" family style weight
```

這個指令的輸出看起來如下：

```
Lucida Sans:style=Demibold:weight=200
DejaVu Sans:style=Bold Oblique:weight=200
Lucida Sans Typewriter:style=Bold:weight=200
DejaVu Sans:style=Oblique:weight=80
Lucida Sans Typewriter:style=Regular:weight=80
DejaVu Sans:style=Book:weight=80
```

```
DejaVu Sans:style=Bold:weight=200
Lucida Sans:style=Regular:weight=80
```

可以使用 `fc-list` 來查詢的重要參數：

表格 15.2 *fc-list* 的參數

參數	意義及可用值
family	字型系列的名稱，例如，FreeSans。
foundry（製造商）	字型的製造商，例如，urw。
style（樣式）	字型樣式，例如，Medium(中)、Regular(標準)、Bold(粗體)、Italic(斜體)或是Heavy(特粗)。
lang	字型支援的語言，例如，de表示德文、ja表示日文、zh-TW表示繁體中文，zh-CN表示簡體中文。
weight	字型粗細，例如80表示一般，200表示粗體。
slant（斜度）	通常，斜度0表示沒有斜度，100表示斜體。
file	字型檔案的名稱。
outline（外框）	true（真）表示外框字型，false（偽）表示其他字型。
scalable（縮放）	true（真）表示縮放字型，false（偽）表示其他字型。
bitmap（點陣）	true（真）表示點陣字型，false（偽）表示其他字型。

參數	意義及可用值
<code>pixelsize</code> (點大小)	以點表示的字型大小。這個選項和 <code>fc-list</code> 一起使用時只對點陣字型有意義。

15.3 如需更多資訊

請安裝 `xorg-x11-doc` 和 `howtoenh` 套件來取得更多有關 X11 的深度資訊。可在專案的首頁 <http://www.x.org> 上找到關於 X11 開發的更多資訊。

手冊頁中詳細描述了 `xorg-x11-driver-video` 套件隨附的很多驅動程式。例如，如果使用 `nv` 驅動程式，可以在 `man 4 nv` 中找到有關此驅動程式的詳細資訊。

有關協力廠商驅動程式的資訊可在 `/usr/share/doc/packages/<套件名稱>` 中找到。例如，安裝套件後，`x11-video-nvidiaG01` 的文件就位於 `/usr/share/doc/packages/x11-video-nvidiaG01` 中。

使用 FUSE 存取檔案系統

FUSE 是使用者空間中的檔案系統 (*file system in userspace*) 的縮寫。這表示您可以以非特權使用者的身分設定並掛接檔案系統。一般情況下，您必須是 `root` 才能執行此任務。FUSE 自身就是一個核心模組。將 FUSE 與外掛程式結合便能延伸其功能，幾乎可存取所有檔案系統，如遠端 SSH 連線、ISO 影像及其他。

16.1 設定 FUSE

您必須先安裝套件 `fuse` 才能使用 FUSE。是否需要以獨立套件形式提供的其他外掛程式，取決於要使用的檔案系統。FUSE 外掛程式未與 SUSE Linux Enterprise 一起提供。

一般而言，您無需設定 FUSE 即可直接使用。但建議您建立可將所有掛接點組合於其中的目錄。例如，可以建立目錄 `~/mounts` 並在該處插入不同檔案系統的子目錄。

16.2 可用的 FUSE 外掛程式

FUSE 與外掛程式相關聯。下表列出了常見的外掛程式。FUSE 外掛程式未與 SUSE Linux Enterprise 一起提供。

表格 16.1 可用的 *FUSE* 外掛程式

<code>fuseiso</code>	掛接包含 ISO9660 檔案系統的 CD-ROM 影像
<code>ntfs-3g</code>	掛接 NTFS 卷冊 (包含讀寫支援)
<code>sshfs</code>	基於 SSH 檔案傳輸通訊協定的檔案系統用戶端
<code>wdfs</code>	掛接 WebDAV 檔案系統

16.3 如需更多資訊

如需詳細資訊，請參閱 FUSE 的首頁 <http://fuse.sourceforge.net>。

III. 行動電腦

Linux 的行動計算功能

人們多半會將行動計算與筆記型電腦、PDA、行動電話以及它們彼此間的資料交換聯想在一起。行動硬體元件 (如外接硬碟、隨身碟或數位相機) 可以連接到筆記型電腦或桌上電腦系統。行動計算環境需要許多軟體元件，而且有些應用程式是專為行動用途量身訂製的。

17.1 筆記型電腦

筆記型電腦的硬體與一般桌上電腦系統不同。因為可交換性、空間要求和耗電量之類的準則必須考慮在內。行動硬體的製造廠商開發了一些標準介面，例如 PCMCIA (國際個人電腦記憶卡協會)、Mini PCI 和 Mini PCIe，可以使用它們來擴充筆記型電腦的硬體。這些標準涵蓋了記憶卡、網路介面卡、ISDN 和數據機卡，以及外接硬碟。

提示：SUSE Linux Enterprise Server 和 Tablet PC

SUSE Linux Enterprise Server 也支援 Tablet PC。Tablet PC 隨附的觸控板/數位板可讓您使用數位筆甚至是指尖直接在螢幕上編輯資料，而無需使用滑鼠和鍵盤。它們的安裝與設定方式與所有其他系統非常相似。如需安裝和設定 Tablet PC 的詳細資料，請參閱第 20 章「*使用 Tablet PC*」[231 頁]。

17.1.1 省電

製造筆記型電腦時採用了電能優化系統元件，因此不必靠電力系統就可以使用該類電腦。它們在省電的貢獻上至少與作業系統的貢獻一樣重要。對於可影響筆記型電腦電源的使用以及影響使用電池電源之操作時間的各種方法，SUSE® Linux Enterprise Server 均可提供支援。下列清單以遞減排序陳述對省電的貢獻：

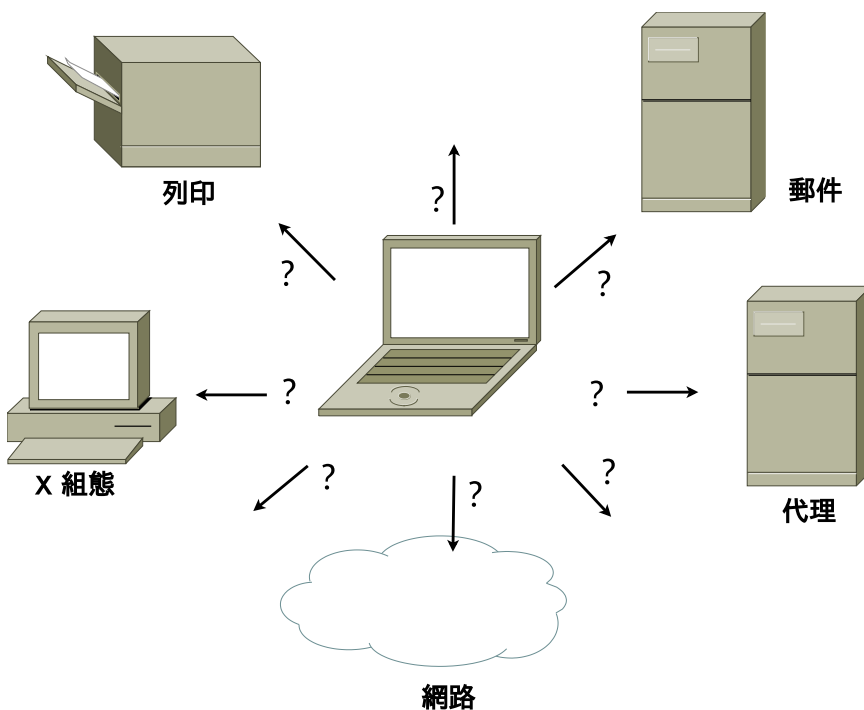
- 調節 CPU 速度.
- 暫停時關閉顯示器亮度.
- 手動調整顯示器亮度.
- 將未使用的 HotPlug 配件 (USB CD-ROM、外接滑鼠、未使用的 PCMCIA 卡、WLAN 等) 解除連接。
- 閒置時降低硬碟轉速.

有關 SUSE Linux Enterprise Server 中電源管理的詳細背景資訊，請參閱第 19 章「[電源管理](#)」[223頁]。

17.1.2 與變動作業環境的整合

您的系統在用於行動計算時，常需與變動的作業環境搭配。許多服務與環境息息相關，因而基礎用戶端必須經過重新設定。SUSE Linux Enterprise Server 可以為您處理這項任務。

圖形 17.1 將行動電腦整合到現有環境中



筆記型電腦在小型家用網路及公司網路之間來回交替使用的情形，影響的服務包括：

網路

包括 IP 位址指定、名稱解析、網際網路連線、以及與其他網路的連線。

列印

視網路而定，必須出現可用印表機及可用列印伺服器目前的資料庫。

電子郵件和代理

列印時，對應伺服器的清單必須是最新的。

X (圖形環境)

如果您的筆記型電腦暫時性地連接到投影機或外接顯示器，則必須要有不同的顯示器組態。

SUSE Linux Enterprise Server 提供了數種將筆記型電腦整合到現有作業環境的方法：

NetworkManager

NetworkManager 是特地為筆記型電腦的行動網路量身訂做的。它能讓您在多種網路環境或不同類型的網路 (例如 GPRS、EDGE 或 3G 等行動寬頻、無線 LAN 和乙太網路) 之間輕鬆地自動切換。NetworkManager 支援無線 LAN 中的 WEP 與 WPA-PSK 加密。亦支援撥接連接 (使用 smpppd)。兩種桌面環境 (GNOME 和 KDE) 都包含 NetworkManager 的前端工具。如需有關桌面 applet 的更多資訊，請參閱第 26.4 節「使用 KNetworkManager」[359頁] 與第 26.5 節「使用 GNOME NetworkManager Applet」[364頁]。

表格 17.1 NetworkManager 的使用案例

我的電腦...	使用 NetworkManager
是筆記型電腦	是
有時候會連接到不同網路	是
提供網路服務 (例如 DNS 或 DHCP)	否
只使用靜態 IP 位址	否

在不應由 NetworkManager 處理網路組態時，請使用 YaST 工具來設定網路連線。

提示：DNS 組態和各種類型的網路連線

如果您常常攜帶筆記型電腦出差，並且需要變更不同類型的網路連接，則只要使用 DHCP 正確指定所有 DNS 位址，NetworkManager 便可正常工作。如果某些連線使用靜態 DNS 位址，請將該位址新增至 /etc/sysconfig/network/config 中的 NETCONFIG_DNS_STATIC_SERVERS 選項。

SLP

服務位置通訊協定 (SLP) 簡化了筆記型電腦到現有網路的連線。沒有 SLP，筆記型電腦的管理員通常需要熟知網路中的可用服務。SLP 廣播特定類型服務的可用性到本地網路中的所有用戶端。支援 SLP 的應用程式可以處理由

SLP 分派出來的資訊，而且能夠自動設定。SLP 還可用來安裝系統，縮短對適用安裝來源的搜尋時間。如需有關 SLP 的詳細資訊，請參閱第 22 章「網路中的 SLP 服務」[303頁]。

17.1.3 軟體選項

行動用途的許多特殊任務領域是由專屬軟體所負責的：系統監控(特別是電池電量)、資料同步化，以及與週邊和網際網路的無線通訊。以下幾節涵蓋了 SUSE Linux Enterprise Server 為每項任務提供的最重要的應用程式。

17.1.3.1 系統監控

以下為 SUSE Linux Enterprise Server 提供的兩種 KDE 系統監控工具：

電源管理

「**電源管理**」是一款可讓您調整與 KDE 桌面行為關聯之節能的應用程式。一般情況下，這款應用程式可透過「**電池監視器**」系統匣圖示來存取，該圖示因目前的供電類型而有所不同。您還可以透過「**Kickoff 應用程式啟動器**」來開啟其組態對話方塊：「**應用程式**」>「**設定桌面**」>「**進階**」>「**電源管理**」。

按一下「**電池監視器**」系統匣圖示可以存取用於設定其行為的選項。您可以從顯示的五個電源設定檔中選擇最適合您需要的那一個。例如，「**簡報**」規劃停用了螢幕保護程式和整體的電源管理，因此您的簡報不會被系統事件所干擾。按一下「**更多...**」會開啟一個更複雜的組態螢幕。您可在此處編輯個人設定檔，設定進階電源管理選項與通知，如筆記型電腦上蓋關閉時或電池電量低時執行什麼操作。

系統監視器

「**系統監視器**」(也稱為「**KSysguard**」)會將度量系統參數收集到一個監控環境中。依預設，它會在 2 個分頁中顯示輸出資訊。「**程序表**」提供目前執行之程序的詳細資訊，例如 CPU 負載、記憶體使用率，或程序 ID 編號及 nice 值。您可以自定收集之資料的顯示和過濾方式。若要新增新的程序資訊類型，請按一下程序表的標頭，然後選擇要隱藏或新增至檢視窗的欄。還可以在各資料頁監控不同的系統參數，或透過網路同時收集各種機器的資料。KSysguard 也能在沒有 KDE 環境的機器上做為精靈來執行。如需有關此程式的詳細資訊，請參閱其整合的說明功能或 SUSE 說明頁。

GNOME 環境中使用「**電源管理偏好設定**」和「**系統監視器**」。

17.1.3.2 同步化資料

在沒有連接網路的行動機器與公司中連接網路的工作站之間切換時，必須讓所有個體間已處理的資料保持同步。這些資料可能包括出差時以及在公司內都需要用到的電子郵件資料夾、目錄以及個別檔案。這兩種情況中的解決方案如下：

同步化電子郵件

使用IMAP帳戶在公司網路中儲存您的電子郵件。然後使用任何已啟用IMAP的中斷連接電子郵件用戶端 (Mozilla Thunderbird Mail、Evolution 或 KMail)，從工作站存取電子郵件。電子郵件用戶端需要設定，如此「傳送郵件」會永遠存取相同的資料夾。這樣可確保完成同步化程序後，所有訊息及其狀態資訊都能使用。使用郵件用戶端中實作的用於傳送郵件的SMTP伺服器，代替全系統MTA postfix 或 sendmail 來接收有關未傳送郵件的可靠回應。

同步化檔案與目錄

有數種公用程式適合用來同步化筆記型電腦與工作站之間的資料。使用最廣的是一項名為rsync的指令行工具。如需詳細資訊，請參閱其手冊頁(`man 1 rsync`)

17.1.3.3 無線通訊

筆記型電腦不僅可以使用電纜連接家用或公司網路，還可以透過無線方式連接其他電腦、周邊設備、行動電話或PDA。Linux支援三種類型的無線通訊：

WLAN

WLAN採用了最廣泛的無線技術，是唯一適合操作大型、甚至極端分散網路的模式。個別機器可以彼此連接，形成一個獨立的無線網路或存取網際網路。稱為存取點的設備，是做為啟用WLAN設備的基礎工作站，而且扮演存取網際網路的中介角色。行動使用者可以在存取點之間切換，端視所在位置及哪個存取點提供最佳連接而定。與行動電話的通訊方式類似，供WLAN使用者使用的大型網路，不用將它們連結到特定位置才能存取。如需有關WLAN的詳細資訊，請參閱第18章「無線區域網路」[207頁]。

藍芽

藍芽在所有無線技術中的應用範圍最廣泛。它可以用於電腦(筆記型電腦)與PDA或行動電話之間的通訊，像IrDA的功能一樣。也可以用來連接覆蓋範圍內的各台電腦。連接鍵盤或滑鼠等無線系統元件時，也可以使用藍芽。不過，此技術的範圍還不足以連接遠端系統與網路。WLAN是穿透實體障礙物(如牆)進行通訊的選用技術。

IrDA

IrDA 是最短距離的無線技術。兩邊的通訊方必須位於彼此可見的距離內。無法克服如牆之類的障礙物。IrDA 的一個應用方式是從筆記型電腦傳輸檔案到行動電話。可使用 IrDA 來涵蓋筆記型電腦到行動電話的短距離。長距離傳送檔案到收件者是由行動網路處理。IrDA 的另一種應用是在公司內以無線方式傳輸列印工作。

17.1.4 資料安全性

理想而言，您應使用多種方式保護筆記型電腦上的資料，不受未授權的存取。可以從下列三大面向來採取適當的安全性措施：

防止竊取

不論在什麼時候，都要避免機器遭到竊取。各種保全工具 (例如鎖鏈) 都可以在零售店中買到。

增強式驗證

除了透過登入和密碼進行標準驗證之外，還使用生物驗證。SUSE Linux Enterprise Server 支援指紋驗證。如需詳細資訊，請參閱第 7 章「*Using the Fingerprint Reader*」(↑*Security Guide*)。

保全系統上的資料

重要資料在傳輸時不僅要加密，在硬碟上也要加密。這樣在竊取的情況中可確保其安全。如需使用 SUSE Linux Enterprise Server 建立加密分割區的資訊，請參閱第 11 章「*Encrypting Partitions and Files*」(↑*Security Guide*)。另一種情況是在使用 YaST 新增使用者時建立加密的主目錄。

重要：資料安全性和暫停寫入到磁碟

暫停寫入到磁碟時，不會卸載加密分割區。因此，任何人只要偷到硬體並且將硬碟復原，即可使用分割區上的資料。

網路安全性

任何資料傳輸，不論其傳輸方式為何，我們都應保護其安全。有關 Linux 及網路的一般安全性議題，請參閱第 1 章「*Security and Confidentiality*」(↑*Security Guide*)。與無線網路相關的安全性措施，請參閱第 18 章「*無線區域網路*」[207頁]。

17.2 行動硬體

SUSE Linux Enterprise Server 能夠自動偵測 Firewire (IEEE 1394) 或 USB 上的行動儲存設備。*行動儲存設備*這個詞，包含了任何種類的 FireWire 或 USB 硬碟、USB 隨身碟或數位相機。只要這些設備一透過對應介面與系統連接，即可自動偵測與設定。GNOME 和 KDE 的檔案管理員都提供靈活的行動硬體項目處理方式。若要安全卸載所有這些媒體，請使用檔案管理員 KDE 或 GNOME 的「安全移除」(KDE) 或「卸載卷冊」(GNOME) 功能。

外接磁碟 (USB 和 FireWire)

系統正確辨識外接硬碟後，其圖示就會出現在檔案管理員中。按一下圖示，會顯示設備的內容。在此可以建立、編輯或刪除資料夾及檔案。若要重新命名磁碟的系統指定名稱，請在圖示上按一下滑鼠右鍵所開啟的功能表中，選取對應的功能表項目。此名稱的變更，僅限顯示於檔案管理員中。因此，掛接於 `/media` 中設備的描述符號不會受影響。

USB 隨身碟

這些設備由系統處理，如外接硬碟一樣。同樣可以在檔案管理員中重新命名項目。

17.3 行動電話和 PDA

桌上電腦或筆記型電腦可以透過藍芽或 IrDA 進行通訊。有些型號支援兩種通訊協定，而有些則僅支援其中一種。兩種通訊協定的使用範圍及相關的延伸說明文件已經在第 17.1.3.3 節「無線通訊」[202頁]中提及。行動電話通訊協定的組態，於手冊中均有說明。

Evolution 與 Kontact 均支援在 Palm, Inc. 生產的手持裝置之間進行同步化作業。與設備的首次連線可以在精靈的協助下輕鬆完成。設定 Palm Pilot 的支援後，必須判斷應該同步化哪些類型的資料 (通訊錄、約會等)。

17.4 如需更多資訊

有關行動設備與 Linux 所有問題的參考重點，請參閱 <http://tuxmobil.org/>。該網站的各個區段，對應筆記型電腦、PDA、行動電話及其他行動硬體中軟體和硬體的各個方面。

<http://tuxmobil.org/> 的類似方法由 <http://www.linux-on-laptops.com/> 提供。在此可以找到有關筆記型電腦和掌上型設備的資訊。

關於筆記型電腦相關議題，SUSE 提供了專屬的郵件清單 (使用德文)。請參閱 <http://lists.opensuse.org/opensuse-mobile-de/>。在此清單上，使用者與開發人員討論了 SUSE Linux Enterprise Server 行動計算的所有觀念。以英文張貼的文章會收到回應，但是大部分的歸檔資訊僅有德文版本。使用 <http://lists.opensuse.org/opensuse-mobile/> 可獲取英文張貼的文章。

<http://en.opensuse.org/OpenSync> 中提供了關於 OpenSync 的資訊。

無線區域網路

無線 LAN 或無線區域網路 (WLAN) 已成為行動運算中不可或缺的一環。如今，大多數的筆記型電腦都有內建的 WLAN 卡。本章介紹如何使用 YaST 設定 WLAN 卡，如何對傳輸進行加密，以及如何使用秘訣提示。

18.1 WLAN 標準

WLAN 卡使用由 IEEE 組織提出的 802.11 標準進行通訊。此標準最初用於最大傳輸率 2 MBit/s。其間已增加許多新的標準來提高資料傳輸率。這些補充項目定義調變、傳輸輸出及傳輸率等詳細資訊 (請參閱表格 18.1 「WLAN 標準綜覽」 [207 頁])。此外，很多公司都實作具有專利權或草擬功能的硬體。

表格 18.1 WLAN 標準綜覽

名稱	頻段 (GHz)	最大傳輸率 (MBit/s)	記事
802.11 舊	2.4	2	過時的；實際上無法取得終端設備
802.11a	5	54	較少干涉
802.11b	2.4	11	較不普遍

名稱	頻段 (GHz)	最大傳輸率 (MBit/s)	記事
28.29oz	2.4	54	常見，與 11b 向後相容
802.11n	2.4 與/或 5	300	通用
802.11ad	2.4/5/60	最多 7000	於 2012 年發行，目前較不普遍

SUSE® Linux Enterprise Server 不支援 802.11 舊版網路卡。支援使用 802.11a、802.11b、802.11g 與 802.11n 的大多數網路卡。新卡通常符合 802.11n 標準，但也有使用 802.11g 的卡。

18.2 運作模式

使用無線網路時，您可以用各種不同的技術和組態來確保快速、高品質的安全連接。不同的作業類型適合不同的設定方式。選擇正確的驗證方法相當困難。可用的加密方法會有不同的優缺點。

無線網路基本可分為三種網路模式：

受管理模式 (基礎結構模式)，透過存取點

管理網路中有一個管理元件，即存取點。在此模式 (又稱為基礎結構模式) 下，網路上所有 WLAN 工作站的連線都會通過該存取點，此存取點亦可連接至乙太網路。此模式會使用各種不同的驗證機制 (WPA 等)，以便確定只有獲得授權的工作站才可以連接。

臨機操作模式 (對等網路)

臨機操作網路中沒有存取點。由於工作站之間可直接進行通訊，因此臨機操作網路通常比受管理網路要快。不過，臨機操作網路中的傳輸範圍及參與工作站的數目相當有限。也不支援 WPA 驗證。如果您想要使用 WPA 安全性，就不應當使用臨機操作模式。

主要模式

在主要模式中，網路卡被用作存取點。但只有在 WLAN 卡支援此模式時才會如此。如需 WLAN 卡的詳細資訊，請造訪 <http://linux-wless.passsys.nl>。

18.3 驗證

無線網路比有線網路更容易受到攔截和危害，因此各項標準均包含驗證和加密方式。在較早版本的 IEEE 802.11 標準中，可在 WEP 條款 (有線等值隱密) 下找到這些項目的說明。然而，WEP 已證實不夠安全 (請參閱第 18.6.3 節「安全性」[219頁])。為此，WLAN 業者 (組成「Wi-Fi 聯盟」) 定義了一項稱為 WPA 的擴充標準，用於提高 WEP 的安全性。較新版的 IEEE 802.11i 標準中包含了 WPA 及一些其他驗證和加密方式。IEEE 802.11i 又稱為 WPA2，因為 WPA 建立於 802.11i 的草擬版本之上。

目前管理網路時會使用各種不同的驗證機制，以便確定只有獲得授權的工作站才可進行連接：

無 (開放)

開放的系統，即不需要驗證的系統。任何工作站均可加入網路。但您還是可以使用 WEP 加密，請參閱第 18.4 節「加密」[210頁]。

共用金鑰 (根據 IEEE 802.11)

此程序使用 WEP 金鑰進行驗證。不過，並不建議採用此程序，因為它使 WEP 金鑰更容易受到攻擊。攻擊者只需要截聽工作站與存取點間的通訊達足夠的時間就行了。在驗證過程中，雙方交換相同的資訊，先是以加密的形式，然後是以未加密形式。這樣就可以利用適合的工具重新建構金鑰。由於此方式是以 WEP 金鑰來驗證和加密，因此無法提高網路的安全性。擁有正確 WEP 金鑰的工作站可以驗證、加密及解密。缺乏金鑰的工作站則無法解密已收到的封包。因此，不論是否需要驗證其身份，該工作站均無法進行通訊。

WPA-PSK (或 WPA-個人，根據 IEEE 802.1x)

WPA-PSK (PSK 即 Pre-Shared Key (預先共用金鑰) 的縮寫) 的作用方式與共用金鑰程序相似。所有連接工作站及存取點都要有相同的金鑰。此金鑰長度為 256 位元，且通常以密碼片語的方式輸入。本系統不需要如 WPA-EAP 一樣複雜的金鑰管理，並且更適合個人使用。因此，WPA-PSK 有時稱為 WPA「家用」。

WPA-EAP (或 WPA-企業，根據 IEEE 802.1x)

WPA-EAP (可延伸的驗證通訊協定) 實際上並非驗證系統，而是用來傳送驗證資訊的協定。WPA-EAP 用來保護企業中的無線網路。在私人網路中幾乎很少用到。因此，WPA-EAP 有時稱為 WPA「企業」。

WPA-EAP 需要 Radius 伺服器才能驗證使用者。EAP 提供三種不同的方法，用於連接至伺服器以及向伺服器進行驗證：

- 傳輸層安全性 (EAP-TLS)：TLS 驗證的進行依賴於伺服器和用戶端相互的證書交換。首先，伺服器會向評估它的用戶端提供其憑證。如果用戶端認為該憑證有效，就會接著向伺服器提供其憑證。雖然 TLS 是安全的，它仍需要網路中的工作憑證管理基礎結構。這種基礎結構在私有網路中很難找到。
- 通道式傳輸層安全性 (EAP-TTLS)
- 受保護的可延伸驗證通訊協定 (EAP-PEAP)：TTLS 和 PEAP 都是包含兩個階段的通訊協定。第一個階段是建立安全性連線，第二個階段是交換用戶端驗證資料。它們需要的憑證管理負荷 (如果有的話) 遠低於 TLS。

18.4 加密

可使用各種不同的加密方式，防止未經授權者讀取無線網路中交換的資料封包，或進入網路：

WEP (定義於 IEEE 802.11 中)

此標準使用 RC4 加密演算法，最初的金鑰長度為 40 位元，後來增加為 104 位元。視 24 位元的啟始向量是否包含其中而定，其長度通常為 64 位元或 128 位元。然而此標準具有某些弱點。此系統所產生的金鑰可能受到攻擊。儘管如此，使用 WEP 仍然比完全不加密網路來得好。

某些廠商已實作了非標準「動態 WEP」。其功能與 WEP 完全相同並具有同樣的弱點，唯一的區別在於，金鑰會透過金鑰管理服務定期進行變更。

TKIP (定義於 WPA/IEEE 802.11i 中)

此金鑰管理協定定義於 WPA 標準中，使用與 WEP 相同的加密演算法，其弱點則均已消除。因為每個資料封包都有一個新的金鑰，所以攻擊這些金鑰等於白費力氣。TKIP 與 WPA-PSK 必須搭配使用。

CCMP (定義於 IEEE 802.11i 中)

CCMP 說明金鑰管理。通常與 WPA-EAP 搭配使用，但也可配合 WPA-PSK 使用。根據 AES 的規定所進行的加密，比 WEP 標準下的 RC4 加密更安全。

18.5 使用 YaST 進行設定

重要：無線網路安全方面的風險

第三者可在未加密的 WLAN 連接上截取所有的網路資料。請務必使用其中一種受支援的驗證和加密方式保護您的網路流量。

請使用硬體允許的最佳加密方式。不過，若要使用某種加密方式，網路中的所有設備都必須支援此方式，否則它們無法互相通訊。例如，如果您的路由器支援 WEP 及 WPA，但無線區域網路卡的驅動程式只支援 WEP，那麼您可以使用 WEP 這種最不常用的加密方式。不過，即使是使用 WEP 進行不嚴密的加密也比完全不加密要好。如需詳細資訊，請參閱第 18.4 節「加密」[210頁]和第 18.6.3 節「安全性」[219頁]。

若要使用 YaST 來設定無線 LAN，您需要定義下列參數：

IP 位址

使用靜態 IP 位址，或讓 DHCP 伺服器動態地將 IP 位址指定給介面。

操作模式

定義如何將機器整合到 WLAN 中，視網路拓撲而定。如需的背景資訊，請參閱第 18.2 節「運作模式」[208頁]。

網路名稱 (ESSID)

用於識別網路的唯一字串。

驗證和加密詳細資料

根據網路使用的驗證和加密方式，您需要輸入一或多個金鑰和/或證書。

有多個輸入選項可用來輸入相應的金鑰：「密碼片語」、「ASCII」（僅用於 WEP 驗證方式）以及「16 進位」。

18.5.1 取消啟動 NetworkManager

安裝期間通常會偵測無線區域網路卡。如果您的機器是行動電腦，預設通常會啟動 NetworkManager。如果您要改為使用 YaST 來設定無線區域網路卡，則需要先取消啟動 NetworkManager：

- 1 以 `root` 使用者身分啟動 YaST。
- 2 在 YaST Control Center 中，選取「網路設備」>「網路設定」開啟「網路設定」對話方塊。

如果您的網路目前是透過 NetworkManager 控制，一則警告訊息就會顯示，告知您無法透過 YaST 編輯網路設定。

- 3 若要允許使用 YaST 進行編輯，請按一下「確定」關閉該訊息，然後在「全域選項」索引標籤上啟用「使用 *ifup* 的傳統方法」。
- 4 若要進一步設定組態，請繼續第 18.5.2 節「存取點的組態」[212頁]或第 18.5.3 節「建立臨時網路」[216頁]。

否則請按一下「確定」確認變更，以便寫入網路組態。

18.5.2 存取點的組態

本節介紹如何設定無線區域網路卡以連接至 (外部) 存取點，或如何使用無線區域網路卡做為存取點 (如果您的無線區域網路卡支援此用途)。有關沒有存取點的網路的組態，請參閱第 18.5.3 節「建立臨時網路」[216頁]。

過程 18.1 設定無線區域網路卡以使用存取點

- 1 啟動 YaST，然後開啟「網路設定」對話方塊。
- 2 切換到「綜覽」索引標籤，此處會列出系統偵測到的所有網路卡。如需一般網路組態的詳細資訊，請參閱第 21.4 節「使用 YaST 手動設定網路連線」[258頁]。
- 3 從清單中選擇無線網路卡並按一下「編輯」以開啟「網路卡設定」對話方塊。
- 4 在「位址」索引標籤中，設定機器是使用動態還是靜態 IP 位址。通常設定成使用「DHCP」獲取「動態位址」即可。

- 5 按「**下一步**」前進至「**無線網路卡組態**」對話方塊。
- 6 若要使用無線區域網路卡來連接至存取點，請將「**操作模式**」設定為「**管理的**」。

但是，如果您要使用無線區域網路卡做為存取點，請將「**操作模式**」設定為「**主要**」。請注意，並非所有無線區域網路卡都支援此模式。

注意：使用 WPA-PSK 或 WPA-EAP

若要使用 WPA-PSK 或 WPA-EAP 驗證模式，就必須將操作模式設定為「**管理的**」。

-
- 7 若要連接至特定網路，請輸入「**網路名稱 (ESSID)**」。或者，按一下「**掃描網路**」並從可用無線網路的清單中選取一個網路。

在無線網路中，所有工作站都要有相同的 ESSID 才能互相通訊。如果未指定 ESSID，無線區域網路卡會自動與訊號強度最佳的存取點關聯。

注意：WPA 驗證需要 ESSID

如果選取「**WPA**」驗證，則必須設定網路名稱 (ESSID)。

-
- 8 為網路選取「**驗證模式**」。哪種模式合適，視無線區域網路卡的驅動程式和網路中其他設備的功能而定。
 - 9 如果之前選擇將「**驗證模式**」設定為「**沒有加密**」，請按「**下一步**」完成組態設定。對提示存在此潛在安全性風險的訊息進行確認，然後按一下「**確定**」離開「**綜覽**」索引標籤 (顯示新設定的無線區域網路卡)。

如果您之前選擇的是任何其他驗證模式，請繼續過程 18.2, “輸入加密詳細資料” [214頁]。

圖形 18.1 YaST：設定無線網路卡



The image shows the 'Wireless Network Card Configuration' window in YaST. At the top, there is a title bar and a subtitle '無線網路卡組態'. Below the subtitle, a note states: '可在此處設定無線網路連接的 最重要設定。『操作模式』取決於網路拓撲。模式 可以是『臨時操作』（沒有存取點對等網路）、... 其他'.

The main configuration area is titled '無線裝置設定' (Wireless Device Settings). It contains the following fields and controls:

- 操作模式(B):** A dropdown menu with '管理的' (Managed) selected.
- 網路名稱 (ESSID)(I):** A text input field with a dropdown arrow and a '掃描網路' (Scan Networks) button.
- 驗證模式(A):** A dropdown menu with 'WEP - 開放' (WEP - Open) selected.
- 金鑰輸入類型** (Key Input Type): Radio buttons for '通關密碼(E)' (Selected), 'ASCII(A)', and '16 進位(H)' (Hex).
- 加密金鑰(E):** A text input field for the key.
- Buttons at the bottom: '專家設定(O)' (Expert Settings), 'WEP 金鑰(W)' (WEP Key), '中止(B)' (Cancel), '上一步(B)' (Previous), and '下一步(N)' (Next).

過程 18.2 輸入加密詳細資料

下列驗證方式需要加密金鑰：「WEP - 開放」、「WEP - 共用金鑰」以及「WPA-PSK」。

WEP 驗證方式通常只需要一個金鑰，不過，您最多可為工作站定義 4 個不同的 WEP 金鑰。其中的一個金鑰必須設定為預設金鑰並用於加密。其他三個用於解密。預設使用的金鑰長度為 128 位元，但您也可以將長度設定為 64 位元。

為了提高安全性，WPA-EAP 使用 RADIUS 伺服器來驗證使用者。在伺服器上進行驗證可以使用三種不同的方式：TLS、TTLS 和 PEAP。WPA-EAP 需要的身分證明與證書視用於 RADIUS 伺服器的驗證方式而定。您可以請求系統管理員提供所需的資訊和身分證明。YaST 可搜尋 `/etc/cert` 下的任何憑證。因此，請將指定給您的憑證儲存到此位置，並將對這些檔案的存取權限限制為 0600 (擁有者讀取和寫入)。

1 若要輸入「WEP - 開放」或「WEP - 共用金鑰」的金鑰：

1a 將「金鑰輸入類型」設定為「密碼片語」、「ASCII」或「16 進位」。

1b 輸入相應的「加密金鑰」(通常僅使用一個金鑰)：

如果您選取了「密碼片語」，請輸入一個單字或一個字元串，系統會根據此內容按照指定的金鑰長度 (預設為 128 位元) 建立金鑰。

「*ASCII*」必須輸入 5 個字元以建立 64 位元金鑰；輸入 13 個字元以建立 128 位元金鑰。

「16 進位」則必須輸入 10 個字元以建立 64 位元金鑰，或 26 個字元以在 16 進位表示法中建立 128 位元金鑰。

1c 若要將金鑰長度調整為較低的位元率 (較舊的硬體可能需要如此)，請按一下「*WEP* 金鑰」並將「金鑰長度」設定為「64」位元。「*WEP* 金鑰」對話方塊還會顯示到目前為止所有輸入的 *WEP* 金鑰。除非有另一個金鑰已明確設定為預設金鑰，否則 YaST 一律使用第一個金鑰做為預設金鑰。

1d 若要為 *WEP* 輸入更多金鑰或修改其中一個金鑰，請選取相應的項目，然後按一下「編輯」。選取「金鑰輸入類型」，然後輸入金鑰。

1e 按一下「確定」確認您的變更。

2 若要為「*WPA-PSK*」輸入金鑰：

2a 選取輸入方法「密碼片語」或「16 進位」。

2b 輸入相應的「加密金鑰」。

在「密碼片語」模式下，必須輸入 8 至 63 個字元。在「16 進位」模式下，必須輸入 64 個字元。

3 如果您選擇了「*WPA-EAP*」驗證，請按「下一步」切換到「*WPA-EAP*」對話方塊，在此處輸入網路管理員提供給您的身分證明和證書。

3a 選取 *RADIUS* 伺服器用於驗證的「*EAP* 模式」。接下來需要輸入哪些詳細資料，視選取的「*EAP* 模式」而定。

3b 若為 *TLS*，請提供「身分」、「用戶端證書」、「用戶端金鑰」以及「用戶端金鑰密碼」。為了提高安全性，您還可以設定用於驗證伺服器真實性的「伺服器證書」。

TTLS 與 PEAP 需要「身分」和「密碼」，而「伺服器證書」和「匿名身分」則可以選擇性提供。

3c 按一下「詳細資料」，進入用於設定 WPA-EAP 的進階驗證對話方塊。

3d 選擇 EAP-TTLS 或 EAP-PEAP 通訊第二階段 (內部驗證) 的「驗證方式」。可選的方式視您在上一個對話方塊中所選的 RADIUS 伺服器驗證方式而定。

3e 如果自動確定設定沒有運作，請選擇某個特定「PEAP 版本」以強制使用特定的 PEAP 實作。

4 按一下「確定」確認您的變更。「綜覽」索引標籤即會顯示新設定之無線區域網路卡的詳細資料。

5 按一下「確定」以完成組態設定並離開該對話方塊。

18.5.3 建立臨時網路

某些情況下，可以連接兩個配有 WLAN 卡的電腦。若要使用 YaST 建立臨時網路，請執行以下操作：

1 啟動 YaST，然後開啟「網路設定」對話方塊。

2 切換到「綜覽」索引標籤，從清單中選擇您的無線網路卡，然後按一下「編輯」以開啟「網路卡設定」對話方塊。

3 選擇「靜態指定的 IP 位址」，然後輸入以下資料：

- 「IP 位址」：192.168.1.1。例如，要將第二部電腦上的此位址變更為 192.168.1.2。
- 「子網路遮罩」：/24
- 「主機名稱」：選擇所需的名稱。

4 按「下一步」繼續。

- 5 將「*操作模式*」設定為「*臨機操作*」。
 - 6 選擇「*網路名稱 (ESSID)*」。可以是任意名稱，但必須在臨機操作網路中的每部電腦上使用。
 - 7 為網路選取「*驗證模式*」。哪種模式合適，視無線區域網路卡的驅動程式和網路中其他設備的功能而定。
 - 8 如果之前選擇將「*驗證模式*」設定為「*沒有加密*」，請按「*下一步*」完成組態設定。對提示存在此潛在安全性風險的訊息進行確認，然後按一下「*確定*」離開顯示新設定之無線區域網路卡的「*綜覽*」索引標籤。
- 如果您之前選擇的是任何其他驗證模式，請繼續過程 18.2, “輸入加密詳細資料” [214頁]。
- 9 如果未安裝 `smpppd`，YaST 會要求您安裝。
 - 10 相應地設定網路中的其他無線區域網路卡，設定時請使用相同的「*網路名稱 (ESSID)*」、相同的「*驗證模式*」，但需使用不同的 IP 位址。

18.5.4 設定其他組態參數

設定無線區域網路卡時，通常無需變更預先設定的設定。但是，如果您需要詳細設定 WLAN 連線的組態，YaST 可讓您變更下列設定：

通道

WLAN 工作站可在其上正常運作的通道的規格。只有「*臨機操作*」和「*主要*」模式需要設定此項。在「*管理*」模式下，網路卡會自動搜尋可用的通道以連接存取點。

位元率

視您網路的效能而定，您可以設定點對點間特定的傳輸位元率。在預設值為「*自動*」的情況下，系統會試著選擇使用最高的資料傳輸率。有些 WLAN 卡不支援位元率的設定。

存取點

在擁有多個存取點的環境中，只要指定 MAC 位址即可預選其中一個存取點。

電源管理

當您外出時，省電技術可讓您的電池供電時間達到最久。如需電源管理的詳細資訊，請參閱第 19 章「[電源管理](#)」[223 頁]。使用電源管理可能會影響連線品質，增加網路延遲時間。

若要存取進階選項：

- 1 啟動 YaST，然後開啟「[網路設定](#)」對話方塊。
- 2 切換到「[綜覽](#)」索引標籤，從清單中選擇您的無線網路卡，然後按一下「[編輯](#)」以開啟「[網路卡設定](#)」對話方塊。
- 3 按「[下一步](#)」前進至「[無線網路卡組態](#)」對話方塊。
- 4 按一下「[進階設定](#)」。
- 5 在「[臨機操作](#)」模式中，必須從提供的通道 (11 至 14 個，取決於您所在的國家) 中選取其中之一，讓您的工作站可與其他工作站通訊。在「[主要](#)」模式下，需要指定一個「[通道](#)」，以便您的網路卡可以用它來提供存取點功能。此選項的預設值為「[自動](#)」。
- 6 選取要使用的「[位元率](#)」。
- 7 輸入要連接的「[存取點](#)」的 MAC 位址。
- 8 選擇是否「[使用電源管理](#)」。
- 9 按一下「[確定](#)」確認變更，然後依序按「[下一步](#)」和「[確定](#)」完成組態設定。

18.6 設定 WLAN 的秘訣與技巧

下列工具和秘訣可協助您監控並提高 WLAN 的速度、穩定性及安全性。

18.6.1 公用程式

wireless-tools 套件包含允許設定無線區域網路特定參數並取得統計資料的公用程式。如需相關資訊，請參閱http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html。

18.6.2 穩定性及速度

無線網路的效能及可靠性，要看連線工作站是否能從其他工作站收到清楚的訊號。牆壁之類的障礙物會大大減弱訊號強度。訊號強度愈弱，傳輸速度愈慢。作業期間，可以在指令行(連線品質欄位)上使用 iwconfig 公用程式或是使用 KDE 或 GNOME 提供的 NetworkManager Applet，來檢查訊號強度。若您的訊強度出現問題，試著將您的設備安裝在其他地方，或調整您存取點的天線方向。許多 PCMCIA WLAN 卡都有輔助天線，可大幅提高接收度。由廠商指定的速率(例如 54 MBit/s) 為一額定值，代表推定的最大值。實際上，最大資料量從始至終都沒能達到該值的一半。

iwspy 指令可以顯示 WLAN 統計資料：

```
iwspy wlan0
wlan0      Statistics collected:
    00:AA:BB:CC:DD:EE : Quality:0  Signal level:0  Noise level:0
    Link/Cell/AP      : Quality:60/94  Signal level:-50 dBm  Noise level:-140
    dBm (updated)
    Typical/Reference : Quality:26/94  Signal level:-60 dBm  Noise level:-90
    dBm
```

18.6.3 安全性

如果您要建立一個無線網路，請記得在缺乏安全措施的情況下，任何在傳輸範圍內的人都可輕易地進入您的網路。因此，應確定啟用加密方式。所有 WLAN 卡和存取點都支援 WEP 加密。雖然不是安全無虞，但仍足以阻礙可能的攻擊。

若網路供私人使用，請使用 WPA-PSK (如果可用)。儘管在絕大多數硬體元件上，Linux 都支援 WPA，但一些驅動程式並不支援 WPA。WPA 在較舊的存取點和具有 WLAN 功能的路由器上可能也不適用。對於這類設備，請檢查是否可以透過韌體更新來實作 WPA。如果沒有 WPA，則 WEP 仍然比完全不加密來得好。對於需要進階安全性的企業來說，只有在執行 WPA 的情況下才可操作無線網路。

為驗證方法使用增強式密碼。例如，網頁 <https://www.grc.com/passwords.htm> 會隨機產生 64 位元密碼。

18.7 疑難排解

如果您的 WLAN 卡沒有回應，請檢查以下幾方面：

1. 您是否知道無線區域網路卡的設備名稱？通常會是 wlan0。使用工具 `ifconfig` 對此進行檢查。
2. 是否檢查過所需的韌體？如需詳細資訊，請參閱 `/usr/share/doc/packages/wireless-tools/README.firmware`。
3. 路由器的 ESSID 是否已被廣播並且可以看到 (即未隱藏)？

18.7.1 檢查網路狀態

指令 `iwconfig` 可為您提供有關無線連線的重要資訊。例如，執行下面這一行指令將顯示 ESSID、無線模式、頻率、是否加密以及連線品質等：

```
iwconfig wlan0
wlan0 IEEE 802.11abg ESSID:"guest"
      Mode:Managed Frequency:5.22GHz Access Point: 00:11:22:33:44:55
      Bit Rate:54 Mb/s Tx-Power=13 dBm
      Retry min limit:7 RTS thr:off Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality:62/92 Signal level:-48 dBm Noise level:-127 dBm
      Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
      Tx excessive retries:10 Invalid misc:0 Missed beacon:0
```

此外，也可以透過 `iwlist` 指令獲取先前的資訊。例如，執行下面這一行指令將顯示目前的位元速率：

```
iwlist wlan0 rate
wlan0      unknown bit-rate information.
          Current Bit Rate=54 Mb/s
```

如果要瞭解有多少存取點可用，可以使用 `iwlist` 指令。它會給出單元式清單，類似於：

```
iwlist wlan0 scanning
wlan0 Scan completed:
  Cell 01 - Address: 00:11:22:33:44:55
    Channel:40
    Frequency:5.2 GHz (Channel 40)
    Quality=67/70 Signal level=-43 dBm
    Encryption key: off
    ESSID:"Guest"
    Bit Rates: 6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s;
                24 Mb/s; 36 Mb/s; 48 Mb/s
    Mode: Master
    Extra:tsf=0000111122223333
    Extra: Last beacon: 179ms ago
    IE: Unknown: ...
```

18.7.2 多重網路設備

現代的筆記型電腦通常具備一張網路卡和一張 WLAN 卡。如果您以 DHCP 來設定這兩者 (自動指定位址)，則可能會出現名稱解析和預設閘道的問題。如果您可以偵測到路由器，卻無法瀏覽網際網路，表示已出現此問題。支援資料庫提供本主題的文章，網址是：http://old-en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients。

18.7.3 Prism2 網路卡的問題

有許多驅動程式可用於裝有 Prism2 晶片的設備。各種不同的網路卡多多少少都可以與不同的驅動程式配合運作。使用這些卡時，WPA 只能配合 hostap 驅動程式來運作。如果這些網路卡無法順利運作，或完全無法運作，或者您想使用 WPA，請參閱 /usr/share/doc/packages/wireless-tools/README.prism2。

18.8 如需更多資訊

如需詳細資訊，請參閱以下頁面：

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html

Linux「無線工具」的開發者 Jean Tourrilhes 在其網頁中提供大量有關無線網路的有用資訊。

tuxmobil.org

有關使用 Linux 行動電腦的實用資訊。

<http://www.linux-on-laptops.com>

有關在筆記型電腦上使用 Linux 的詳細資訊。

電源管理

► **System z:** 本章所描述的功能與硬體，IBM System z 不提供，因此本章的內容與這些平台無關。 ◀

電源管理對筆記型電腦十分重要，對其他系統也很有用。ACPI (Advanced Configuration and Power Interface，進階組態和電源介面) 可以在所有現代電腦(筆記型電腦、桌上型電腦和伺服器) 上使用。電源管理技術需要配備合適的硬體與 BIOS 常式。大多數筆記型電腦和許多新式的桌上型電腦及伺服器都符合這些需求。此技術還可以控制 CPU 頻率比例，這有助於省電及降低噪音。

19.1 省電功能

省電功能不僅對於筆記型電腦的行動用途很重要，對於桌上型系統也很重要。主要功能以及在 ACPI 中的用途包括：

待命

不支援。

暫停 (記憶體)

此模式會將整個系統狀態寫入 RAM 中。接著，除了 RAM 以外，整個系統都會進入睡眠狀態。在此狀態中，電腦所使用的電源極少。此狀態的好處是可以在幾秒內將工作復原到暫停之前的狀態，而不用開機或重新啟動應用程式。此功能等同於 ACPI 狀態 S3。

睡眠 (暫停磁碟)

在此操作模式，會將整個系統狀態寫入硬碟，然後關閉系統。至少要有與 RAM 一樣大的交換分割區，才能寫入所有作用中資料。要從此狀況重新啟用需耗時 30 到 90 秒。還原時會回到暫停前的狀態。有些製造商會為此模式提供有用的混合功能，例如 IBM Thinkpad 中的 RediSafe。對應的 ACPI 狀態為 S4。在 Linux 中，暫停寫入到磁碟是由獨立於 ACPI 之外的核心常式來執行。

電池監視器

ACPI 會檢查電池充電狀態並提供相關資訊。此外，ACPI 會在電力到達某個關鍵狀態時，協調要執行的動作。

自動關閉電源

關機後，電腦會關閉電源。此功能很重要，尤其是在電池用盡前所執行的自動關機。

處理器速度控制

與 CPU 連結時有三種方式可節省電源：頻率和電壓比例 (也稱為 PowerNow! 或 Speedstep)、調節，以及讓處理器進入睡眠狀態 (C 狀態)。依據電腦的操作模式，也可以合併這些操作方法。

19.2 進階組態與電源介面 (ACPI)

ACPI 主要用於讓作業系統設定和控制個別的硬體元件。ACPI 取代了「電源管理隨插即用 (PnP)」與「進階電源管理 (APM)」。它能提供一些資訊，包括電池、交流電轉接器、溫度、風扇以及關閉蓋子或電池電力不足等系統事件。

BIOS 會提供一些表格，內含關於個別元件與硬體的存取方法等資訊。作業系統會使用這些資訊來執行任務，像是指定中斷或啟用和停用元件。因為作業系統會執行儲存於 BIOS 中的指令，所以 BIOS 實行會決定其功能。ACPI 能偵測和載入的表格在 `/var/log/boot.msg` 中可以找到。請參閱第 19.2.2 節「疑難排解」[225頁]，以取得更多有關 ACPI 問題疑難排解的資訊。

19.2.1 控制 CPU 效能

CPU 可以使用三種方式省電：

- 頻率和電壓比例

- 調節時鐘頻率 (T 狀態)
- 使處理器進入睡眠狀態 (C 狀態)

依據電腦的操作模式的不同，這些方法可合併使用。省電也表示能降低系統溫度，減低風扇的使用頻率。

頻率比例及調節只在處理器忙碌時使用，因為在處理器閒置時，必定會套用最經濟的 C 狀態。如果 CPU 正忙碌，頻率比例是建議的省電方法。通常處理器僅有部份的工作負載。在此情況中，可以使用較低的頻率。通常，最佳方法是使用依核心需求調節器來控制動態頻率比例。

調節應做最後手段使用，例如，在高度系統負載下仍要延伸電池操作時間時。不過在調節過多時，有些系統無法運作順暢。此外，當 CPU 要做的事不多時，調節 CPU 是無意義的動作。

如需更多資訊，請參閱第 11 章「*Power Management*」(↑系統分析與調整指南)。

19.2.2 疑難排解

共有兩種不同類型的問題。一方面是核心的 ACPI 程式碼包含無法及時偵測到的錯誤。在這種情況中，將會有可供下載的解決方案。問題通常是因 BIOS 而起。有時，會刻意在 BIOS 中整合與 ACPI 規格不符的技術，以避免在其他常見作業系統中出現 ACPI 實作錯誤。會在黑名單中將那些在 ACPI 實行中有重大錯誤的硬體元件記錄下來，以避免 Linux 核心對這些元件使用 ACPI。

發生問題時要做的第一件事是更新 BIOS。如果電腦未能開機，下列中的某一個開機參數也許有幫助：

`pci=noacpi`

不使用 ACPI 來設定 PCI 設備。

`acpi=ht`

僅執行一個簡單的資源組態。不將 ACPI 用於其他目的。

`acpi=off`

關閉 ACPI。

警告：未使用 ACPI 的開機問題

有些較新的機器 (尤其是 SMP 系統及 AMD64 系統) 需透過 ACPI 以正確設定硬體。關閉這些機器的 ACPI 會發生隨之而來的問題。

有時，透過 USB 或 FireWire 連接的硬體會另機器混淆。如果機器拒絕開機，則拔除所有不需要的硬體插頭，並再試一次。

開機後，可使用 `dmesg | grep -2i acpi` 指令來監控系統的開機訊息 (或所有訊息，因為也可能是 ACPI 以外的因素構成問題)。如果在分析 ACPI 表格時發生問題，可以將最重要的表格 DSDT (*Differentiated System Description Table*，區分系統描述表) 替換為改良版本。在此情況中，會忽略 BIOS 的錯誤 DSDT。程序在第 19.4 節「疑難排解」[228頁] 中描述。

在核心組態中，有個啟用 ACPI 除錯訊息的切換。如果具有 ACPI 除錯功能的核心已編譯並安裝，則會發出詳細資訊。

如果您曾遇到 BIOS 問題或硬體問題，建議您聯絡製造商。尤其是哪些一直未提供 Linux 支援的製造商，更應該出面解決這些問題。唯有讓製造商得知他們有不少使用 Linux 的客戶，他們才會嚴肅地處理這些問題。

19.2.2.1 如需更多資訊

- <http://tldp.org/HOWTO/ACPI-HOWTO/> (詳細的 ACPI HOWTO，內含 DSDT 修補程式)
- <http://www.acpi.info> (進階組態與電源介面規格)
- <http://www.lesswatts.org/projects/acpi/> (Sourceforge 的 ACPI4Linux 計劃)
- <http://acpi.sourceforge.net/dsdt/index.php> (Bruno Ducrot 的 DSDT 修補程式)

19.3 硬碟的休眠

在 Linux 中，可在不需使用硬碟時，讓硬碟完全進入睡眠狀態，或是讓硬碟以更省電、更安靜的方式來運作。在目前的筆記型電腦中，您不用手動關閉硬碟，

因為它們會在不用的時候自動進入省電操作模式。不過，如果您想最大限度地省電，可以使用 `hdparm` 指令嘗試下面的幾種方法。

該指令能修改各種硬碟設定。`-y` 選項能立即將硬碟切換到待命模式。`-Y` 能讓您進入睡眠。`hdparm -s x` 則會讓硬碟閒置一段時期後關閉。如下所示取代 `x`：0 會停用此機制，使得硬碟持續執行。1 到 240 的值將乘以 5 秒。241 到 251 的值則是以 30 分鐘為一個單位，依序從 30 分鐘的閒置到 11 倍的 330 分鐘的閒置。

可以使用 `-B` 選項來控制硬碟內部的省電選項。可從 0 到 255 中選取一個值，以最大化省電效果或最大化電力輸出。其結果視硬碟用途而定，難以評估。如果要減少硬碟噪音，請使用 `-M` 選項。從 128 到 254 中選取一個值，以決定要安靜或快速。

通常，要讓硬碟進入睡眠不是件容易的事。在 Linux 中，會有多個程序寫入硬碟中，因而重複喚醒硬碟。因此，有必要去瞭解 Linux 如何處理那些要寫入硬碟的資料。首先，會將所有資料在 RAM 中做緩衝處理。`pdflush` 精靈會監控此緩衝區。當資料到達特定的時間限制，或當緩衝區已填滿至某一程度時，會將緩衝區的內容注入硬碟。緩衝區的大小則動態地由記憶體地的大小及系統負載來決定。依預設，`pdflush` 會設成較短的間隔，以最大化資料的完整性。`pdflush` 每 5 秒檢查一次緩衝區，並將資料寫入硬碟。以下變數較為重要：

```
/proc/sys/vm/dirty_writeback_centisecs
```

包含 `pdflush` 執行緒喚醒前的延遲時間 (以百分之一秒為單位)。

```
/proc/sys/vm/dirty_expire_centisecs
```

定義最遲應在其後將改動分頁寫出的時間框架。預設值為 3000，即 30 秒。

```
/proc/sys/vm/dirty_background_ratio
```

`pdflush` 開始寫入改動分頁之前改動分頁的最大百分比。預設值為 5%。

```
/proc/sys/vm/dirty_ratios
```

改動分頁超過此總記憶體的百分比時，系統會強制執行程序以在其時間片段內將改動寫入緩衝區，而不是繼續寫入改動。

警告：損害資料完整性

變更 `pdflush` 精靈的設定會損害資料的完整性。

除了這些程序之外，Btrfs、Ext3、Ext4 記錄檔案系統及其他檔案系統不經由 `pdflush` 便將中繼資料寫入硬碟，也會使得硬碟無法減速。

另一個重要因素在於啟動程式的行為方式。例如，好的編輯器會定期為修改中的檔案，將隱藏備份檔寫入硬碟，因而喚醒硬碟。停用這類功能可能會傷害資料的完整性。

與此相關，`postfix` 郵件精靈會使用 `POSTFIX_LAPTOP` 變數。如果將此變數設為 `yes`，`postfix` 會減少存取硬碟的頻率。

19.4 疑難排解

所有錯誤訊息和警示會記錄在檔案 `/var/log/messages` 中。下列幾節涵蓋了一些最常見的問題。

19.4.1 以硬體支援啟用 ACPI，但沒有作用

如果您遇到 ACPI 問題，請使用 `dmesg | grep -i acpi` 指令搜尋 `dmesg` 的輸出，以取得 ACPI 特定的訊息。

必須更新 BIOS 以解決問題。請到您筆記型電腦製造商的首頁，尋找更新的 BIOS 版本並安裝。請詢問製造商以符合最新 ACPI 規格。在 BIOS 更新後，如果錯誤持續發生，請繼續以更新的 DSDT 取代您 BIOS 中的錯誤 DSDT 表格：

過程 19.1 更新 BIOS 中的 DSDT 表格

為執行下面的程序，請確定下列套件已安裝：`kernel-source`、`pmtools` 與 `mkinitrd`。

- 1 從 <http://acpi.sourceforge.net/dsdt/index.php> 下載您系統的 DSDT。檢查檔案是否已解壓縮，並以所示副檔名 `.aml` (ACPI 機器語言) 編譯。如果是此狀況，請繼續步驟 3。
- 2 如果下載的表格副檔名為 `.asl` (ACPI 原始語言)，請執行以下指令編譯該檔案：

```
iasl -sa file.asl
```

- 3 將(產生的)檔案 `DSDT.aml` 複製到任何位置(建議複製到 `/etc/DSDT.aml`)。
- 4 編輯 `/etc/sysconfig/kernel` 並將路徑與 `DSDT` 檔案搭配。
- 5 啟動 `mkinitrd`。每當您安裝核心並使用 `mkinitrd` 來建立 `initrd` 檔案時，這個經過修改的 `DSDT` 都會在系統啟動時整合並載入。

19.4.2 CPU 頻率沒有作用

請參閱核心來源以瞭解您的處理器是否受支援。您需要特殊核心模組或模組選項以啟用 CPU 頻率控制。如果 `kernel-source` 套件已安裝，則此資訊可在 `/usr/src/linux/Documentation/cpu-freq/*` 中找到。

19.4.3 暫停和待命沒有作用

由於 `DSDT` 實做 (BIOS) 的錯誤，`ACPI` 系統在暫停或待命時可能會有問題。若這樣的話，請更新 BIOS。

當系統嘗試卸載錯誤模組時，系統會停止或不觸發暫停事件。如果您不卸載模組或停止服務(導致無法成功暫停)，也可能發生此狀況。在兩種情況下，都請嘗試辨識無法啟動休眠模式的錯誤模組。記錄檔案 `/var/log/pm-suspend.log` 包含了有關目前的狀況及錯誤之所在的詳細資訊。修改 `/usr/lib/pm-utils/defaults` 中的 `SUSPEND_MODULES` 變數，在暫停或待機之前先卸載有問題的模組。

19.5 如需更多資訊

- http://en.opensuse.org/SDB:Suspend_to_RAM — 如何使暫停寫入到 RAM 運作
- <http://old-en.opensuse.org/Pm-utils> — 如何修改一般暫停架構

使用 Tablet PC

SUSE® Linux Enterprise Server 具有對 Tablet PC 的支援。在下列資訊中，瞭解如何安裝並設定 Tablet PC，探索一些可接受數位筆輸入的有用的 Linux* 應用程式。

支援下列 Tablet PC：

- 具有序列及 USB Wacom 手寫板(筆式輸入)、觸控螢幕或多個觸控設備的 Tablet PC。
- 具有 FinePoint 設備 (例如 Gateway C210X/M280E/CX2724 或 HP Compaq TC1000) 的 Tablet PC。
- 具有觸控式螢幕設備 (例如 Asus R2H、Clevo TN120R、Fujitsu Siemens Computers P-Series、LG C1、Samsung Q1/Q1-Ultra) 的 Tablet PC。

安裝 Tablet PC 套件並正確設定數位裝置後，可以使用筆 (亦稱手寫筆) 輸入來執行下列動作與應用程式：

- 登入 KDM 或 GDM
- 解除 KDE 和 GNOME 桌面螢幕的鎖定
- 也可由其他指標設備 (例如滑鼠或觸控板) 觸發的動作，例如在螢幕上移動游標，啟動應用程式，關閉、移動視窗以及調整視窗大小，切換視窗焦點，以及拖放物件
- 在 X Window System 的應用程式中使用筆勢辨識

- 使用 GIMP 繪圖
- 使用 Jarnal、Xournal 等應用程式做記筆記或素描，或者使用 Dasher 編輯大量文字

20.1 安裝 Tablet PC 套件

Tablet PC 所需的套件包含在 TabletPC 安裝模式中 — 如果安裝時選取了該選項，以下套件應已安裝在您的系統中：

- `cellwriter`：字元手寫輸入面板
- `jarnal`：基於 Java 的筆記應用程式
- `xournal`：用於記筆記和素描的應用程式
- `xstroke`：適用於 X Window System 的筆勢辨識程式
- `xvkbd`：適用於 X Window System 的虛擬鍵盤
- `x11-input-fujitsu`：適用於 Fujitsu P-Series 手寫板的 X 輸入模組
- `x11-input-evtouch`：具有觸控式螢幕之某些 Tablet PC 的 X 輸入模組
- `xorg-x11-driver-input`：適用於輸入設備的 X 輸入模組，包括適用於 Wacom 設備的模組。

如果未安裝這些套件，則需要透過指令行手動安裝所需套件，或選取 TabletPC 模式在 YaST 中進行安裝。

20.2 設定手寫板設備

安裝期間預設會設定手寫板或觸控式設備。如果在設定 Wacom 設備組態時遇到問題，可以在指令行上使用 `xsetwacom` 來變更設定。

20.3 使用虛擬鍵盤

若要登入 KDE 或 GNOME 桌面或解除螢幕鎖定，可以像往常一樣輸入使用者名稱和密碼，也可以透過虛擬鍵盤 `xvkbd` (顯示於登入欄位下方) 來輸入。若要設定鍵盤或存取整合式說明，請按一下左下角的「`xvkbd`」欄位，並開啓 `xvkbd` 主功能表。

如果輸入不可見 (或者未傳送到所需視窗)，請在 `xvkbd` 中按一下「焦點」鍵以重新導向至焦點，然後按一下將取得鍵盤事件的視窗。

圖形 20.1 `xvkbd` 虛擬鍵盤



如果登入後要使用 `xvkbd`，請從主功能表啟動，或者在外圍程序中使用 `xvkbd`。

20.4 旋轉顯示器

請使用 `KRandRTray` (KDE) 或 `gnome-display-properties` (GNOME) 以手動方式即時旋轉顯示畫面或調整顯示畫面大小。`KRandRTray` 與 `gnome-display-properties` 都是用於 X 伺服器之 `RANDR` 延伸的 Applet。

請從主功能表啟動 `KRandRTray` 或 `gnome-display-properties`，也可以輸入 `krandrtray` 或 `gnome-display-properties` 從外圍程序啟動 Applet。啟

動 Applet 後，Applet 圖示通常會顯示在系統匣內。如果 `gnome-display-properties` 圖示未自動出現在系統匣中，請確定「顯示器解析度設定」對話方塊中的「在面板中顯示畫面」已啟用。

若要使用 `KRandRTray` 旋轉顯示畫面，請在圖示上按一下滑鼠右鍵並選取「設定顯示」。從組態對話方塊中選取所需的方向。

若要使用 `gnome-display-properties` 旋轉顯示畫面，請在圖示上按一下滑鼠右鍵並選取所需的方向。您的顯示器會立即旋轉到新的方向。圖形手寫板的方向也會隨之發生變化，因此它仍可以正確解譯出筆的移動。

如果在變更桌面方向時出現問題，如需詳細資訊，請參閱第 20.7 節「疑難排解」[238頁]。

20.5 使用筆勢辨識

SUSE Linux Enterprise Server 包括適用於筆勢辨識的 `CellWriter` 和 `xstroke`。兩個應用程式均接受將筆或其他指向設備產生的筆劃當做 X Window System 上應用程式的輸入。

20.5.1 使用 CellWriter

透過 `CellWriter`，您可以將字元寫入儲存格的網格 — 寫入後立即會以字元為依據進行辨識。完成寫入後，可以將該輸入傳送至目前焦點所在的應用程式。使用 `CellWriter` 進行筆勢辨識之前，需要訓練應用程式以辨識您的手寫：您需要訓練特定按鍵對應中的每個字元 (未經訓練的字元不會啟用，因此無法使用)。

過程 20.1 訓練 CellWriter

- 1 從主功能表啟動 `CellWriter` 或在指令行輸入 `cellWriter`。首次啟動時，`CellWriter` 會自動以訓練模式啟動。在訓練模式中，將顯示目前所選按鍵對應的字元集。
- 2 將要用於字元的筆勢輸入到相關的字元儲存格中。一旦開始輸入文字，背景色彩即會變更為白色，而字元本身則顯示為淺灰色。多次重複此筆勢直到字元顏色變為黑色。不可識別的字元以淺灰色或棕色背景標示 (視桌面的色彩配置而定)。

- 3 重複此步驟直到針對所有所需字元完成 CellWriter 訓練。
- 4 若要為另一種語言訓練 CellWriter，請按一下「設定」按鈕並從「語言」索引標籤選取語言。「關閉」組態對話方塊。按一下「訓練」按鈕並在「CellWriter」視窗之右下角的下拉式方塊中選取按鍵對應。現在重複新按鍵對應的訓練。
- 5 完成按鍵對應訓練後，按一下「訓練」按鈕以切換至一般模式。

在一般模式下，CellWriter 視窗會顯示要在其中輸入筆勢的一對空白儲存格。按一下「輸入」按鈕後，字元才會傳送至其他應用程式，所以在輸入字元之前可以進行更正或刪除。信任度低的已辨識字元將以反白顯示。若要更正輸入，請在儲存格上按一下滑鼠右鍵，隨即會出現內容功能表。若要刪除字元，請使用筆之橡皮擦，或使用滑鼠中鍵清除儲存格。完成在 CellWriter 中的輸入後，請按一下應用程式視窗定義將接收輸入的應用程式。然後按一下「Enter」將輸入傳送至應用程式。

圖形 20.2 用 CellWriter 進行筆勢辨識



按一下「按鍵」按鈕，將取得可取代手寫辨識的虛擬鍵盤。

若要隱藏 CellWriter，請關閉 CellWriter 視窗。應用程式即會在系統匣中以一個圖示顯示。若要再次顯示輸入視窗，請按一下系統匣中的圖示。

20.5.2 使用 Xstroke

透過 xstroke，您可以將筆或其他指向設備產生的筆劃當做 X Window System 上應用程式的輸入。xstroke 字母系統是一種單筆劃字母系統，類似於 Graffiti* 字母系統。啟動後，xstroke 會將輸入傳送到目前聚焦的視窗。

- 1 可以從主功能表啟動 xstroke，或者在外圍程序中使用 xstroke 來啟動。這會在您的系統匣上新增一個鉛筆圖示。

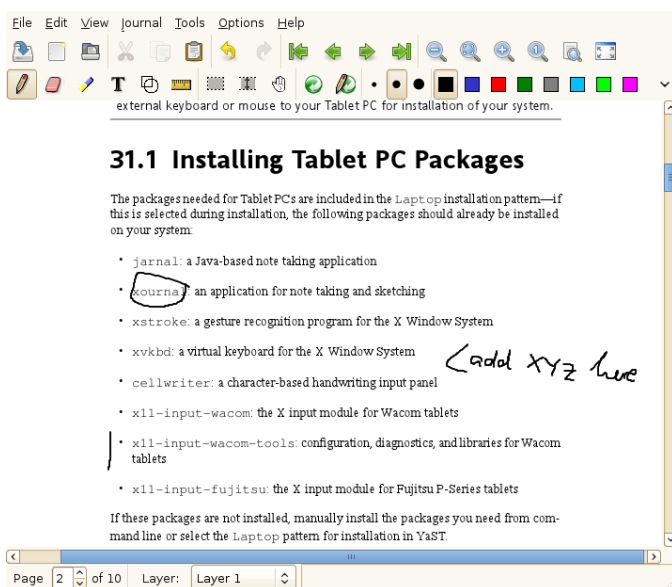
- 2 啟動要使用手寫筆為其建立文字輸入的應用程式(例如，終端機視窗、文字編輯器或 LibreOffice Writer)。
- 3 若要啟用筆劃辨識模式，按一下鉛筆圖示即可。
- 4 使用筆或其他指標設備執行圖形手寫板上的某些筆勢。`xstroke` 可以擷取筆勢，並將其轉換成文字，顯示在焦點所在的應用程式視窗中。
- 5 若要將焦點切換到不同的視窗，請用筆在所需視窗上按一下並按住片刻(或使用桌面控制中心內定義的鍵盤捷徑)。
- 6 若要停用筆勢辨識模式，請再次按一下鉛筆圖示。

20.6 使用筆來做筆記和素描

若要用手寫筆繪圖，可以使用專業的圖形編輯器(如 GIMP)，或者嘗試使用下列筆記應用程式之一：Xournal 或 Jarnal。在 Xournal 和 Jarnal 中，可以用筆來做筆記、繪圖或者為 PDF 檔案加入備註。做為適用於多種平台之 Java 為基礎的應用程式，Jarnal 還提供基本的協作功能。如需詳細資訊，請參閱 <http://www.dklevine.com/general/software/tcl000/jarnal-net.htm>。在儲存內容時，Jarnal 會以歸檔格式 (*.jaj) 儲存資料，該歸檔中另含一個 SVG 格式的檔案。

可以從主功能表啟動 Jarnal 或 Xournal，或者在外圍程序中輸入 `jarnal` 或 `xournal` 來啟動。例如，要在 Xournal 中為 PDF 檔案加入備註，可以選取「檔案」>「註釋 PDF」，然後從檔案系統中開啓 PDF 檔案。使用筆或其他指向設備註釋 PDF 檔案，然後選取「檔案」>「輸出到 PDF」以儲存變更。

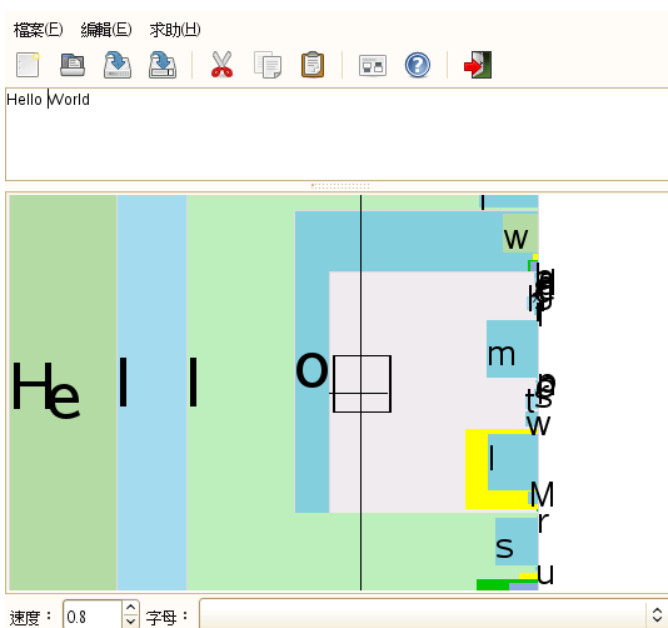
圖形 20.3 使用 Xournal 註釋 PDF



Dasher 是另一個有用的應用程式。它專門用於鍵盤輸入不適用或不可用的場合。接受少量的訓練後，僅憑一支筆 (或其他輸入設備 — 甚至是視線追蹤器所驅動的設備) 即可快速輸入大量的文字。

可以從主功能表啟動 Dasher，也可以在外圍程序中使用 dasher 來啟動。將筆向一個方向移動，應用程式將開始在右側縮放成字母。隨後，根據十字型游標中心產生的字母生成或聯想文字，並在視窗的上方輸出。若要停止或開始書寫，請用筆按一下顯示器。在視察底部修改成字速度。

圖形 20.4 使用 Dasher 編輯文字



Dasher 的概念適用於許多語言。如需詳細資訊，請造訪 Dasher 網站，其中提供了綜合性的文件、展示和訓練文字。其網址為 <http://www.inference.phy.cam.ac.uk/dasher/>

20.7 疑難排解

登入畫面上不顯示虛擬鍵盤

有時，登入畫面上不顯示虛擬鍵盤。若要解決此問題，請重新啟動 X 伺服器，方法是按 **Ctrl + Alt + <←**，或者在 Tablet PC 上按相應的鍵 (如果您使用的是不帶整合鍵盤的平板型號)。如果虛擬鍵盤仍未顯示，請將外部鍵盤連接到平板型號 Tablet PC，再使用硬體鍵盤登入。

Wacom 圖形手寫板的方向不會變更

在外圍程序內部使用 **xrandr** 指令即可變更顯示器的方向。輸入 **xrandr --help** 可檢視可用選項。若要同步變更圖形手寫板的方向，則需要依照下面的說明修改指令：

- 對於正常方向 (0° 旋轉):

```
xrandr -o normal && xsetwacom --set "Serial Wacom Tablet" Rotate NONE
```

- 對於 90° 旋轉 (順時針縱向):

```
xrandr -o right && xsetwacom --set "Serial Wacom Tablet" Rotate CW
```

- 對於 180° 旋轉 (橫向):

```
xrandr -o inverted && xsetwacom --set "Serial Wacom Tablet" Rotate HALF
```

- 對於 270° 旋轉 (逆時針縱向):

```
xrandr -o left && xsetwacom set --"Serial Wacom Tablet" Rotate CCW
```

請注意，上面的指令根據 `xsetwacom list` 指令的輸出而有所不同。用手寫筆或觸控式設備的輸出取代「序列 Wacom 手寫板」。如果您的 Wacom 設備支援觸控功能(可用手指在手寫板上移動游標)，則您還需要旋轉觸控設備。

20.8 如需更多資訊

此處提到的一些應用程式未提供配套的線上說明，但您可以在安裝系統的 `/usr/share/doc/package/packageName` 中或以下網站中，找到關於其用法與組態的一些有用資訊：

- 如需 Xournal 手冊，請參考 <http://xournal.sourceforge.net/manual.html>
- <http://jarnal.wikispaces.com/> 上提供了 Jarnal 文件
- <http://davesource.com/Projects/xstroke/xstroke.txt> 上提供了 xstroke man 頁面
- Linux Wacom 網站 http://sourceforge.net/apps/mediawiki/linuxwacom/index.php?title=Configuring_X 上提供了關於設定 X 的 HOWTO 資訊

- 從 <http://www.inference.phy.cam.ac.uk/dasher/> 可以找到詳細介紹 Dasher 專案之資訊的網站
- 如需有關 CellWriter 的詳細資訊和文件，請造訪 <http://risujin.org/cellwriter/>
- 如需有關 gnome-display-properties 的資訊，請造訪 <http://old-en.opensuse.org/GNOME/Multiscreen>。

IV. 服務

基本網路

Linux 提供所有必要的網路工具及功能，以整合到所有類型的網路結構。使用網路卡、數據機或其他設備進行的網路存取可以使用 YaST 來設定。也可使用手動方式來設定組態。本章僅討論基本機制及相關的網路組態檔案。

Linux 及其他 Unix 作業系統使用 TCP/IP 通訊協定。它不是單一網路通訊協定，而是能夠提供各種服務的網路通訊協定家族的一員。表格 21.1 「TCP/IP 通訊協定家族中的數種通訊協定」 [243 頁] 中所列的通訊協定，其用途是透過 TCP/IP 在兩個機器之間交換資料。由 TCP/IP 組合而成的各個網路形成了一個全球範圍的大網路，也稱為「網際網路」。

RFC 代表要求建議 (*Request for Comments*)。RFC 是描述作業系統及其應用程式的各種網際網路通訊協定和執行程序的文件。RFC 文件描述網際網路通訊協定的設定。若要擴展您對於某種通訊協定的瞭解，請參閱相應的 RFC 文件。

<http://www.ietf.org/rfc.html> 上提供了這些文件。

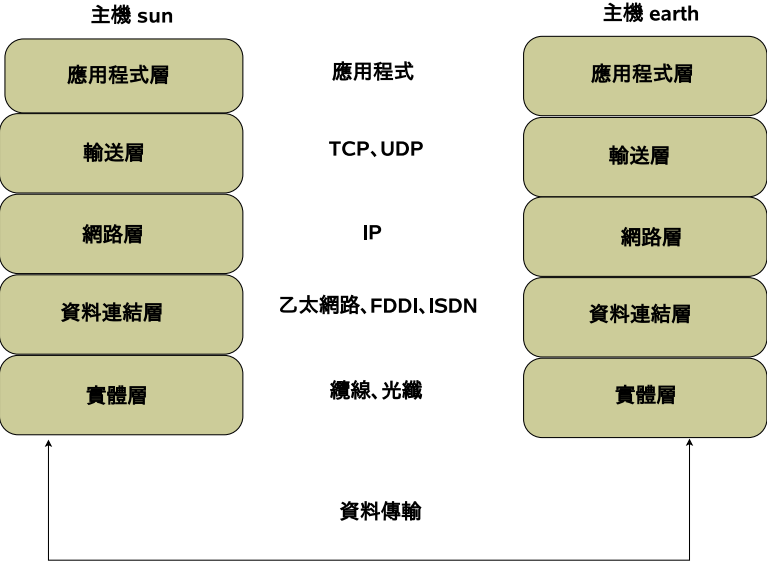
表格 21.1 TCP/IP 通訊協定家族中的數種通訊協定

協定	描述
TCP	傳輸控制通訊協定：連線導向的安全通訊協定。傳輸的資料首先由應用程式當做資料流傳送出去，然後再由作業系統轉換為適當格式。資料送達目的地主機的相關應用程式時，使用的仍是最初傳送的原始資料流格式。TCP 會判定傳輸期間是否遺失或打亂了資料。只要是資料

協定	描述
	順序很重要的地方，就會執行 TCP。
UDP	使用者資料包通訊協定：無連線、不安全的通訊協定。要傳送的資料以應用程式產生的封包形式加以傳送。不會保證資料抵達接收者時的順序，而且可能會發生資料遺失的情況。UDP 適用以記錄為導向的應用程式。它的特點是延遲時間比 TCP 短。
ICMP	網際網路控制訊息通訊協定：基本上，這不是適用一般使用者的通訊協定，而是發佈錯誤報表的特殊控制通訊協定，能夠控制參與 TCP/IP 資料傳送之機器的行為。此外，它還提供特殊的回音模式，可以使用 ping 程式檢視。
IGMP	網際網路群組管理通訊協定：此通訊協定在實做 IP 多點廣播時控制機器行為。

如圖形 21.1「TCP/IP 的簡化層模型」[245頁]中所顯示，資料交換發生在不同層。實際的網路層是透過 IP (網際網路通訊協定，Internet Protocol) 進行不安全的資料傳輸。在 IP 的上方，TCP (傳輸控制通訊協定，Transmission Control Protocol) 可以保證資料傳輸某種程度的安全性。IP 層是由基本的硬體相依通訊協定所支援，例如乙太網路。

圖形 21.1 TCP/IP 的簡化層模型

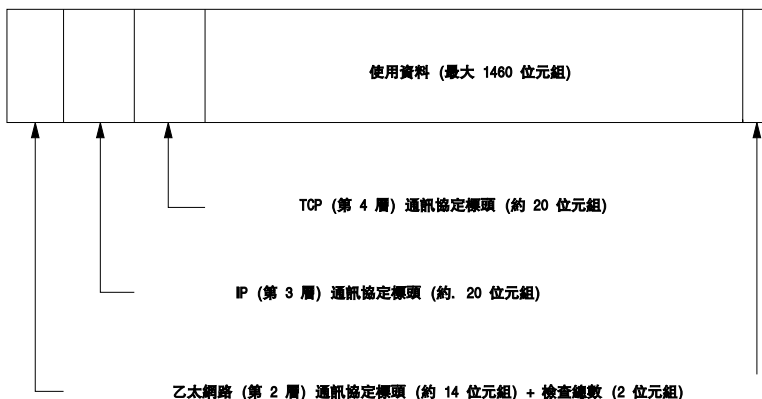


圖表提供每層的一或兩個範例。層的順序是依據抽象階層 (*abstraction level*)。最低層非常靠近硬體。不過，最上層對硬體而言幾乎是完全抽象的。每層都有自己的特殊功能。這些特殊功能通常隱含於其描述中。資料連結及實體層代表使用的實體網路 (如乙太網路)。

幾乎所有的硬體通訊協定都是採用封包導向模式。要傳輸的資料會收集在封包中 (無法一次全部傳送)。TCP/IP 封包的大小上限約為 64 KB。由於網路硬體可能有所限制，因此封包一般都很小。乙太網路上資料封包的最大上限約為 1500 個位元組。在乙太網路上傳送資料時，TCP/IP 封包的大小受限於此數量。如果傳送更多資料，則需要由作業系統傳送更多資料封包。

因為每層有自己指定的功能，關於每層的其他資訊必須儲存於資料封包中。這些資訊放在封包的「標頭」中。每層皆在產生的封包前端附加小的資料區塊，稱為通訊協定標頭。在乙太網路纜線上傳送的 TCP/IP 資料封包範例，可參閱在圖形 21.2「TCP/IP 乙太網路封包」[246頁]中的說明。proofsum 位於封包結尾，不在開頭處。這樣可幫助網路硬體簡化程序。

圖形 21.2 TCP/IP 乙太網路封包



當應用程式在網路上傳送資料時，資料會經過每一層，除實體層外，全部在 Linux 核心執行。每層都負責準備資料使其能夠傳送到下一層。最底層最後要負責傳送資料。接收到資料時則反轉執行整個程序。就如同洋蔥的層級一般，在每層中，會從已傳輸的資料上移除通訊協定標頭。最後，傳輸層負責讓目的地的應用程式可以使用資料。以這種方式，每層僅直接與上下兩層通訊。對於應用程式而言，無論資料是透過 100 MBit/s FDDI 網路或 56-Kbit/s 數據線進行傳輸，都沒有關係。同樣地，對於資料線而言，只要封包的格式正確，無論傳送的是哪種類型的資料也是無關的。

21.1 IP 位址與路由

在此節中的討論僅限於 IPv4 網路。如需有關 IPv6 通訊協定 (IPv4 的後繼者) 的資訊，請參閱第 21.2 節「IPv6—下一代的網際網路」[249頁]。

21.1.1 IP 位址

網際網路上的每台電腦都有唯一的 32 位元位址。這些 32 位元 (或 4 位元組) 一般所寫入的格式，如 範例 21.1 「寫入 IP 位址」[246頁] 中的第二列所述。

範例 21.1 寫入 IP 位址

```
IP Address (binary): 11000000 10101000 00000000 00010100
IP Address (decimal): 192. 168. 0. 20
```


採用十進位格式，四位元組以十進位數字系統撰寫，以句號分隔。IP 位址是指定給主機或網路介面。每個 IP 位址在全球範圍內只能使用一次。此規則有例外狀況，但下文中並未提及。

IP 位址中的點表示階層系統。直到 1990 年代，IP 位址仍嚴格地以類別加以分類。然而，事實證明此系統太過死板，因此已停止使用。現在，則是使用無類別路由 (*classless routing*)，即 CIDR (無類別網域間路由，*classless interdomain routing*)。

21.1.2 網路遮罩與路由

網路遮罩是用來定義子網路的位址範圍。如果兩台主機位於相同的子網路遮罩內，他們可以直接連接。如果不在同一個子網路遮罩內，則需要開道位址，由開道處理子網路的所有流量。若要檢查兩個 IP 位址是否位於同一子網路，只要使用網路遮罩「AND」兩個位址。如果結果相同，兩個 IP 位址位於同一個網路。如果不同，遠端的 IP 位址，即為遠端介面，只能透過開道來通訊。

若要瞭解網路遮罩如何作用，請參閱範例 21.2「連結 IP 位址到網路遮罩」[247頁]。網路遮罩由 32 位元組成，可辨認 IP 位址屬於哪個網路。這些位元為 1 標示 IP 位址中的對應位元，即表示為同屬一個網路。所有位元為 0 標示位元在子網路內。這表示愈多位元為 1，子網路就愈小。因為網路遮罩永遠由多個連續的 1 組成，也可以計算網路遮罩內的位元數。範例 21.2「連結 IP 位址到網路遮罩」[247頁]中，第一個 24 位元的網路也可寫成 192.168.0.0/24。

範例 21.2 連結 IP 位址到網路遮罩

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
-----
Result of the link:        11000000 10101000 00000000 00000000
In the decimal system:      192.      168.      0.      0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
-----
Result of the link:        11010101 10111111 00001111 00000000
In the decimal system:      213.      95.      15.      0
```

舉另外一個例子：使用相同乙太網路纜線連接的所有機器，通常位於同一個子網路中，而且可以直接存取。即使以交換器或橋接器實際分配子網路時，仍然可以直接連接這些主機。

位於本地子網路外的 IP 位址只能在設定目標網路的閘道時，才能與本地通訊。在大部分的狀況下，只能有一個閘道來處理所有對外的通訊。但是，您也可以為不同的子網路，設定多個閘道。

如果已經設定閘道，所有的外部 IP 封包會傳送到適當的閘道。然後此閘道會試圖以同樣方式傳送封包--主機對主機—直到連結到目標主機或封包 TTL (持續時間) 過期。

表格 21.2 特定位址

位址類型	描述
基本的網路位址	這是網路遮罩「及」網路中的任何位址，如 Result 下的範例 21.2 「連結 IP 位址到網路遮罩」 [247頁] 所顯示。此位址不能指定給任何主機。
廣播位址	基本來說，即為「存取此子網路的所有主機」。若要產生此位址，網路遮罩會以二進位格式反轉，連結到具有邏輯 OR 的基本網路位址。因此以上範例會得到 192.168.0.255。此位址無法指派給任何主機。
本地主機	位址 127.0.0.1 是指定到每個主機上的「迴路設備」(loopback device)。使用此位址以及完整迴路網路 127.0.0.0/8 中的所有位址 (使用 IPv4 定義)，可以設定與您自己機器之間的連線。如果使用 IPv6，則只有一個迴路位址 (:::1)。

因為 IP 位址在全世界必須是唯一的，您不能只選取隨機位址。如果要設立私人 IP 結構的網路，有三種位址網域可以使用。這些將無法從其他網際網路取得連結，因為他們無法透過網路傳送。這些位址網域在 RFC 1597 指定並列於 表格 21.3 「私人 IP 位址網域」 [249頁] 中。

表格 21.3 私人 IP 位址網域

網路/網路遮罩	網域
10.0.0.0/255.0.0.0	10.x.x.x
172.16.0.0/255.240.0.0	172.16.x.x – 172.31.x.x
192.168.0.0/255.255.0.0	192.168.x.x

21.2 IPv6—下一代的網際網路

重要：IBM System z：IPv6 支援

IBM System z 硬體 的 CTC 和 IUCV 網路連線不支援 IPv6。

由於全球資訊網 (WWW) 的出現，過去十五年內，越來越多的電腦透過 TCP/IP 進行通訊，網際網路的規模發生了爆炸性的增長。自從 CERN 的 Tim Berners-Lee (<http://public.web.cern.ch>) 於 1990 年發明 WWW 以來，網際網路主機的數量從幾千台成長為幾百萬台。

如前面所述，IPv4 位址僅由 32 個位元組成。而且，損失了一些 IP 位址—由於組織網路的方式，使得這些 IP 位址無法使用。您的子網路中可用的位址數目是位元數的平方減 2。例如，子網路有 2 個、6 個或 14 個位址可用。例如，如果要連接 128 個主機到網際網路，則子網路需要 256 個 IP 位址，但是其中只有 254 個可用，因為子網路結構本身需要用掉兩個 IP 位址：廣播與基本網路位址。

在目前的 IPv4 通訊協定之下，DHCP 或 NAT (網路位址轉譯，Network Address Translation) 是典型的機制，可用來避免位址可能不足的問題。搭配保持私人和公用位址空間分開的方式，能夠減輕短少的情形。其中產生的問題是在於其組態，設定麻煩且難於維護。若要在 IPv4 網路中設定主機，需要一些位址項目，如主機自己的 IP 位址、子網路遮罩、閘道位址，可能還需要名稱伺服器位址。您必須知道所有這些項目，且無法從其他地方取得。

透過 IPv6，位址短少及繁複組態的情形應該都成為過去式了。以下小節說明更多 IPv6 改善的部分及它帶來的好處，還有關於從舊通訊協定轉移到新通訊協定的資訊。

21.2.1 優點

新通訊協定帶來的最重要、最顯而易見的改善，是能夠大量擴充可用的位址空間。IPv6 位址是由 128 個位元值組成，而不是傳統的 32 位元。這樣提供了數以千兆的 IP 位址。

然而，IPv6 位址不僅是在長度方面與之前的位址不同；這些位置的內部結構也不同，可能包含有關系統及其所屬網路的更明確資訊。有關 IPv6 的詳細資訊，可以在第 21.2.2 節「定址類型與結構」[251 頁] 中找到。

以下是新通訊協定一些其他優勢的清單：

自動設定

IPv6 讓網路能夠「隨插即用」(plug and play)，表示新設定的系統不需經過任何手動設定，即可整合到(區域)網路。新主機使用其自動設定組態機制，從鄰近的路由器上可用的資訊取得自己的位址，依賴的是稱為「網路芳鄰探查」(Neighbor Discovery, ND)的通訊協定。這個方法不需要管理員的介入，而且不需要維護分配位址的中央伺服器，這是 IPv4 的另一個優勢，因為自動位址分配需要 DHCP 伺服器。

但是，如果路由器連接到交換器，它應傳送具有旗標的週期性通告，告知網路中的主機彼此如何進行互動。如需詳細資訊，請參閱 RFC 2462、`radvd.conf` (5) `man` 頁面以及 RFC 3315。

機動性

IPv6 能夠同時將數個位址指定給一個網路介面。這樣可讓使用者輕鬆存取多個網路，有時可與行動電話服務公司提供的國際漫遊服務相比：當您帶您的行動電話出國時，一到對應區域，電話就會自動登入外國服務，因此仍可用同一個號碼聯絡到您，且您也可和本國一樣撥打電話。

安全通訊

使用 IPv4，網路安全性是附加的功能。IPv6 包括 IPSec 為其中一個核心功能，允許系統在安全的通道上進行通訊，避免國際網路上的外人竊聽。

反向相容性

實際上，不可能一次將整個網際網路從 IPv4 切換到 IPv6。因此，很重要的是，兩個通訊協定不僅要能夠共存於網際網路上，也得要能夠共存於一個系統中。這是藉由相容的位址 (IPv4 位址可以輕易轉譯為 IPv6 位址) 以及使用一些通道來確保共存。請參閱第 21.2.3 節「IPv4 與 IPv6 的共存」[255 頁]。另外，系統可以仰賴「雙重堆疊 IP」(Dual Stack IP) 技術，同時支援這兩種

通訊協定，這表示系統有兩個完全分開的網路堆疊，如此一來，兩種通訊協定版本不會相互干擾。

透過多重廣播自量身訂做的服務

利用 IPv4，有些服務 (如 SMB) 需要廣播它們的封包到區域網路上的所有主機。IPv6 以更精細的方法，透過「多重廣播」(*multicasting*)—將一些主機定位為群組的一部分，讓伺服器定址主機 (這與透過「廣播」(*broadcasting*) 定位所有主機，或透過「單點廣播」(*unicasting*) 個別定址每個主機的方式不同)。定址為群組的主機，取決於具體的應用程式。例如，有些預先定義的群組可以定址所有名稱伺服器 (「所有名稱伺服器多重廣播群組」) 或所有路由器 (「所有路由器多重廣播群組」)。

21.2.2 定址類型與結構

如上述，目前 IP 通訊協定有兩個重要缺失：IP 位址的短缺越來越嚴重，以及設定網路與管理輪遞表成為複雜而繁重的任務。IPv6 透過擴充位址空間到 128 個位元解決了第一個問題。第二個問題的解決方式則是引入階層位址結構，結合配置網路位址的複雜技術，以及 *multihoming* (指定數個位址到一個設備，可以存取數個網路)。

使用 IPv6 時，瞭解三種不同類型的位址是很有用的：

單點傳播

這類位址恰好與一個網路介面有關聯。這類位址的封包僅傳送到一個目的地。因此，單點廣播位址用來傳送封包到區域網路或網際網路上的個別主機。

多重廣播

這類位址與一組網路介面有關聯。這類位址的封包會傳送到屬於該組的所有目的地。多重廣播位址主要由特定網路服務使用，可直接與特定主機群組通訊。

任點廣播 (Anycast)

這類位址與一組介面有關聯。這類位址的封包會根據基礎路由通訊協定的原則，傳送到最靠近傳送者的群組成員。使用任點廣播位址，讓主機更易於找出在指定網路區域中提供特定服務的伺服器。相同類型的所有伺服器擁有一樣的任點廣播位址。只要主機要求服務，它會從最靠近位置的伺服器接收回覆，由路由通訊協定決定。如果此伺服器因為某種原因失敗，通訊協定會自動選取第二個最靠近的伺服器，或是選取第三個伺服器，依此類推。

IPv6 位址由八個四位數欄位組成，每個都代表 16 個位元，以十六進位標記法寫入。位址與位址之間以冒號 (:) 分隔。指定欄位內的任何前導零位元組可以刪除，但是欄位內或尾端的零不能刪除。另一個慣例是多於四個連續的零位元組可能會摺疊成兩個冒號。然而，每個位址只允許一個 ::。這類的簡略的標記法，顯示於範例 21.3 「範例 IPv6 位址」 [252頁] 中，其中三行都是代表相同的位址。

範例 21.3 範例 IPv6 位址

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                                : 10 : 1000 : 1a4
```

IPv6 位址的每個部分都有定義的功能。第一個位元組形成字首，指定位址類型。中間的部分是位址的網路部分，但是可能不會使用。位址的尾端形成主機部分。透過 IPv6，在位址尾端的斜線後表示字首的長度，可以定義網路遮罩。位址如範例 21.4 「指定字首長度的 IPv6 位址」 [252頁] 中所示，包含的資訊是形成位址網路部分的前 64 個位元以及形成其主機部分的最後 64 個位元。換句話說，64 表示網路遮罩從左邊開始填入 64 個 1 位元值。就像 IPv4 一樣，IP 位址使用 AND 結合網路遮罩的值，判斷主機是否位於相同的子網路或另一個子網路。

範例 21.4 指定字首長度的 IPv6 位址

```
fe80::10:1000:1a4/64
```

IPv6 知道關於數個字首的預定類型。有一些顯示在 表格 21.4 「各種 IPv6 字首」 [252頁] 中。

表格 21.4 各種 IPv6 字首

字首 (十六進位)	定義
00	IPv4 位址與透過 IPv6 的 IPv4 相容位址。這些位址用來維護與 IPv4 的相容性。其使用仍然要求路由器能夠轉譯 IPv6 封包為 IPv4 封包。數個特殊的位址，如迴路設備的位址，也有此字首。
2 或 3 做為第一個數字	可彙總的全域單點廣播位址。在 IPv4 的情形中，可以指定介面形成部分的特定子網路。目前有下列位址空間：2001::/16 (產品品質位

字首 (十六進位)	定義
	址空間) 與 2002::/16 (6to4 位址空間)。
fe80::/10	連結本地位址。具有這種字首的位址不應該傳送，因此僅能從相同的子網路內連接。
fec0::/10	本地網站位址。這些位址可以傳送，但是僅能在所屬組織的網路內傳送。事實上，它們等同於目前私人網路位址空間的 IPv6 (例如，10.x.x.x)。
ff	這些都是多重廣播位址。

單點廣播位址由三個基本元件組成：

公用拓撲 (Public Topology)

第一個部分 (也包含上述的其中一種字首) 用來透過公用網際網路傳送封包。它包含了有關提供網際網路存取的公司或機構資訊。

網站拓撲 (Site Topology)

第二個部分包含有關傳送封包的目的地子網路的傳送資訊。

介面識別碼 (Interface ID)

第三個部分識別傳送封包的介面。它也允許 MAC 形成部分的位址。這個前提是 MAC 在全球是唯一的，由硬體製造商在設備中編碼固定識別碼，可相當程度地簡化組態程序。事實上，結合前 64 個位址位元形成 EUI-64 記號，加上從 MAC 取得的最後 48 個位元，而其餘的 24 個位元則包含有關記號類型的特殊資訊。如此一來，就可以指定 EUI-64 記號給沒有 MAC 的介面，例如以 PPP 或 ISDN 為基礎的介面。

在此基本結構的最上層，IPv6 會分辨五種不同類型的單點廣播位址：

:: (未指定的)

第一次啟始介面時，如果還未用其他方法判定位址時，主機會使用此位址做為其來源位址。

::1 (迴路)
迴路設備的位址。

IPv4 相容位址

IPv6 位址是由 IPv4 位址以及由 96 個零位元組成的字首形成的。這類相容性位址用於通道 (請參閱第 21.2.3 節「IPv4 與 IPv6 的共存」[255頁])，允許 IPv4 與 IPv6 主機在純 IPv4 環境中彼此通訊。

對應到 IPv6 的 IPv4 位址

這類位址以 IPv6 標記法指定純 IPv4 位址。

本地位址

有兩種位址類型用於本地：

連結本地

這類位址僅能用於本地子網路。具有此類型來源或目標位址的封包不應該傳送到網際網路或其他子網路。這些位址包含特殊字首 (fe80::/10) 以及網路卡的介面識別碼，加上由空位元組所組成的中間部分。自動設定組態以便與屬於相同子網路中的其他主機通訊時，會使用這類位址。

網站本地

具有這種位址的封包可以傳送到其他子網路，但是不能到更寬廣的網際網路，而必須保留在組織自己的網路內。這類位址用於內部網路，而且等同於 IPv4 所定義的私人位址空間。它們包含特殊字首 (fec0::/10)、介面識別碼，以及指定子網路識別碼的 16 位元欄位。同樣地，其他則是填入空位元組。

因為引入了 IPv6 這種全新的功能，所以每個網路介面通常會取得數個 IP 位址，其優點是可透過相同介面存取數個網路。其中一個網路可以設定完全自動化 (使用 MAC 和已知的字首)，只要一啟用 IPv6 (使用連結本地位址) 即可連接區域網路上的所有主機。利用形成位址部分的 MAC，全球使用的任何 IP 位址都成為唯一的。位址的唯一變數部分，是指定網站拓撲和公用拓撲，該部分視主機目前正在操作的實際網路而定。

如果主機要在不同的網路之間往返，至少需要兩個位址。其中一個，即主位址，不僅包含了介面識別碼，也包含了其通常所屬之主網路 (及其對應字首) 的識別碼。主位址是靜態位址，因此它通常不會變更。儘管如此，預定要送到行動主機的所有封包，還是可以傳送到主位址，無論是在主網路或其他外部網路中操作。這可藉由 IPv6 全新功能來達成，如「無狀態自動設定」與「網路芳鄰探查」。除了其主位址外，行動主機也取得一或多個其他的位址，這些位址屬於

漫遊的外部網路。這些外部網路稱為 *care-of* 位址。主網路具有封包在外部漫遊時轉寄預定要送到主機的設備。在 IPv6 環境中，這個任務是由主代辦執行的，它會取得所有預定要送到主位址的封包，透過通道轉送它們。另一方面，預定送到 *care-of* 位址的封包會直接傳送到行動主機，不會特別繞行。

21.2.3 IPv4 與 IPv6 的共存

連接網際網路的所有主機從 IPv4 轉移到 IPv6 是一種漸進程序。這兩種通訊協定某些時候會共存。在一個系統上共存，可保證執行兩種通訊協定的「**雙重堆疊**」。但是仍出現一些問題，就是使用 IPv6 的主機如何與 IPv4 主機通訊，以及由 IPv4 結構主導的目前網路如何傳輸 IPv6 封包。最佳的解決方案是提供通道及相容性位址 (請參閱第 21.2.2 節「定址類型與結構」[251頁])。

IPv6 主機或多或少孤立於 (全球) IPv4 網路間，可透過通道通訊：IPv6 封包會被包成 IPv4 封包，在 IPv4 網路中移動。兩個 IPv4 主機之間的連接，稱為「**通道**」。若要完成這個目的，封包必須包含 IPv6 目的地位址 (或對應字首) 以及通道接收端上遠端主機的 IPv4 位址。基本通道可以根據主機管理員之間的協議「**手動**」設定；這也稱為「**靜態通道**」。

不過，靜態通道的組態及維護通常需要密集勞力，才能使用它們應付每天的通訊需求。因此，IPv6 提供三種不同的「**動態通道**」方法：

6over4

IPv6 封包會自動封裝成 IPv4 封包，透過能夠多重廣播的 IPv4 網路進行傳送。IPv6 的缺點是將整個網路 (網際網路) 視為一個大型的區域網路 (LAN)。如此即能自動判定 IPv4 通道的接收端。然而，這個方法不能適當的延伸，而且也因 IP 多重廣播目前在網際網路上並不普遍的事實而受到阻礙。所以，它僅能為啟用多重廣播的小型公司或機構的網路提供解決方案。這個方法的規格詳述於 RFC 2529。

6to4

利用此方法，IPv4 位址會自動從 IPv6 位址產生，使得隔離的 IPv6 主機能夠在 IPv4 網路上通訊。不過，有關這些隔離的 IPv6 主機及網際網路之間的通訊，目前已出現一些問題。該方法詳述於 RFC 3056。

IPv6 通道代理

這個方法仰賴提供 IPv6 主機專屬通道的特殊伺服器。詳述於 RFC 3053。

21.2.4 設定 IPv6

若要設定 IPv6，通常不需要在個別工作站中做任何變更。IPv6 預設會開啟這個選項。您可在第 6.16.1.3 節「網路組態」(第 6 章「使用 YaST 安裝」, ↑部署指南)所述的網路設定步驟中的安裝期間停用。若要在安裝的系統上停用或啟用 IPv6，請使用 YaST「網路設定」模組。在「全域選項」索引標籤上，根據需要核取或取消核取「啟用 IPv6」選項。如果想在下次重新開機前暫時啟用它，請以 root 身分輸入 `modprobe -i ipv6`。IPv6 模組載入之後，一般情況下無法卸載。

由於 IPv6 的自動組態概念，網路卡會在連結本地網路中指定一個位址。工作站通常不會進行路由由表格管理。工作站可使用「路由器通告通訊協定」，向網路路由器查詢應使用的前置號碼和閘道。可使用 `radvd` 程式來設定 IPv6 路由器。此程式會通知工作站該 IPv6 位址應使用的前置號碼和路由器。或者，也可使用 `zebra/quagga` 自動設定位址和路由的組態。

請參閱 `ifcfg-tunnel(5) man` 頁面，瞭解如何使用 `/etc/sysconfig/network` 檔案來設定不同類型的通道。

21.2.5 如需更多資訊

上述綜覽沒有完整地涵蓋 IPv6 主題。如需更深入的探討這種新的通訊協定，請參閱以下線上文件和書籍：

<http://www.ipv6.org/>
所有有關 IPv6 的入門資訊。

<http://www.ipv6day.org>
啟動您 IPv6 網路所需的所有資訊。

<http://www.ipv6-to-standard.org/>
啟用 IPv6 產品的清單。

<http://www.bieringer.de/linux/IPv6/>
在此處可找到 Linux IPv6-HOWTO 和許多與此主題相關的連結。

RFC 2640
有關 IPv6 的基本 RFC。

描述此主題所有重要面向的書籍，《IPv6 Essentials》由 Silivia Hagen 所著 (ISBN 0-596-00125-8)。

21.3 名稱解析

DNS 協助指定 IP 位址給一或多個名稱以及指定名稱給 IP 位址。在 Linux 中，這種轉換通常是由已知為 `bind` 的特殊類型軟體執行的。處理這個轉換的機器稱為「名稱伺服器」(name server)。所有名稱元件之間以句號分隔，它們共同組成一個階層系統。但是，名稱階層與上述的 IP 位址階層無關。

考慮使用完整名稱，如 `jupiter.example.com`，採用 `hostname.domain` 格式。完整名稱，也就是完全合格網域名稱 (*Fully Qualified Domain Name*, *FQDN*)，是由主機名稱和網域名稱 (`example.com`) 組成的。後者也包含了「最上層網域」(top level domain) 或 TLD (`com`)。

TLD 指定因為過去的緣故變得相當混淆。習慣上，美國使用三個字母的網域名稱。全世界的其他國家，則是使用兩個字母的 ISO 國際代碼為標準。除此之外，2000 年引入了較長的 TLD，代表特定活動範圍 (例如，`.info`、`.name`、`.museum`)。

在早期的網際網路 (1990 年前)，是使用檔案 `/etc/hosts` 儲存網際網路上所有機器的代表名稱。這種方式，對於連接到網際網路、快速增長的電腦數量層面而言，很快就證實是不切實際的。基於此因素，又開發出分散式的資料庫，以廣泛分散的方式來儲存主機名稱。這種資料庫與名稱伺服器類似，沒有有關網際網路上所有主機的立即可用資料，但是可以分散要求到其他名稱伺服器。

階層的最上層是由「root 名稱伺服器」(root name server) 所使用。這些 root 名稱伺服器管理最上層網域，且由「網路資訊中心」(Network Information Center, NIC) 負責管理。每個 root 名稱伺服器知道負責指定最上層網域的名稱伺服器。有關最上層網域 NIC 的資訊可從 <http://www.internic.net> 取得。

DNS 的功能不只是解析主機名稱。名稱伺服器也知道哪個主機，即「郵件交換器」(*Mail Exchanger*, *MX*)，負責接收該網域的電子郵件。

若要让您的機器能夠解析 IP 位址，它必須知道至少一個名稱伺服器及其 IP 位址。透過 YaST 的幫助可以輕鬆指定這類名稱伺服器。如果您使用數據機撥接連接，完全不需要手動設定名稱伺服器。撥號通訊協定在連線建立時會提供名

稱伺服器位址。第 21.4.1.4 節「設定主機名稱和 DNS」[267頁]中詳細描述了使用 SUSE® Linux Enterprise Server 存取名稱伺服器的組態。關於設定您自己的名稱伺服器的資訊，請參閱第 24 章「網域名稱系統」[315頁]。

whois 通訊協定與 DNS 密切相關。利用此程式，可快速找出伺服器負責哪個指定網域。

注意：MDNS 和 .local 網域名稱

.local 最上層網域將被解析程式視為連結本地網域。DNS 要求將做為多路廣播 DNS 要求予以傳送，而非通常的 DNS 要求。如果已在名稱伺服器組態中使用了 .local 網域，則必須在 /etc/host.conf 中關閉此選項。如需詳細資訊，請參閱 host.conf 手冊頁。

如果要在安裝期間關閉 MDNS，請使用 nomdns=1 做為開機參數。

如需有關多路廣播 DNS 的詳細資訊，請參閱 <http://www.multicastdns.org>。

21.4 使用 YaST 手動設定網路連線

Linux 可支援多種網路類型。大多數使用不同的設備名稱和組態檔，會分佈在檔案系統的不同位置。要更瞭解手動網路組態的綜覽，請參閱第 21.6 節「手動設定網路連線」[281頁]。

在預設會啟用 NetworkManager 的 SUSE Linux Enterprise Desktop 中，所有網路卡都已設定好。如果未啟用 NetworkManager，只會自動設定連接 (連接了網路纜線) 的第一個介面。可隨時在安裝的系統上設定其他的硬體。以下幾節將描述 SUSE Linux Enterprise Server 支援之所有網路連線類型的網路組態。

提示：IBM System z：熱插式網路卡

IBM System z 平台支援熱插式網路卡，但不支援透過 DHCP 進行的自動網路整合 (和 PC 的情況相同)。完成偵測後，接著以手動設定介面。

21.4.1 使用 YaST 設定網路卡

若要在 YaST 中設定有線或無線網路卡，請選取「*網路設備*」>「*網路設定*」。啟動模組後，YaST 將顯示「*網路設定*」對話方塊，其中包含四個索引標籤：「*全域選項*」、「*綜覽*」、「*主機名稱/DNS*」和「*路由*」。

使用「*全域選項*」索引標籤可設定一般網路選項，例如 NetworkManager、IPv6 和一般 DHCP 選項的使用方式。如需詳細資訊，請參閱第 21.4.1.1 節「設定全域網路選項的組態」[260頁]。

「*綜覽*」索引標籤包含有關已安裝網路介面與組態的資訊。此處會列出所有正確偵測到之網路卡的名稱。在此對話方塊中，您可以手動設定新網路卡、移除或變更其組態。若要手動設定未自動偵測到的卡，請參閱第 21.4.1.3 節「設定未偵測到的網路卡」[266頁]。若要變更已設定卡的組態，請參閱第 21.4.1.2 節「變更網路卡組態」[261頁]。

使用「*主機名稱/DNS*」索引標籤可設定機器的主機名稱並指定要使用的伺服器。如需詳細資訊，請參閱第 21.4.1.4 節「設定主機名稱和 DNS」[267頁]。

「*路由*」索引標籤用於設定路由組態。如需相關資訊，請參閱第 21.4.1.5 節「設定路由」[269頁]。

圖形 21.3 設定網路組態

網路設定
使用 網路管理員 會有一個桌面小程式，來管理所有介面，它十分適合在有線與多個無線網路 間... [更多](#)

全域選項 | **網路(O)** | 主機名稱/DNS | 路由

網路設定方法

☐ 使用 NetworkManager 進行使用者控制(U)

☒ 使用 ifup 的傳統方法(I)

IPv6 協定設定

☒ 啟用 IPv6

DHCP 用戶端選項

☐ 申請廣播回應(C)

DHCP 用戶端識別碼(I):

要傳送的主機名稱(H):

AUTO

☒ 透過 DHCP 變更預設路由

說明 | 取消(C) | 上一步(B) | 確定(O)

21.4.1.1 設定全域網路選項的組態

使用 YaST 「網路設定」模組的「全域選項」索引標籤，可以設定重要的全域網路選項，例如 NetworkManager、IPv6 和 DHCP 用戶端選項的使用方式。這些設定適用於所有網路介面。

在「網路設定方法」中，選擇管理網路連線的方式。若希望 NetworkManager 桌面 applet 管理所有介面的連線，請選擇「使用者以 *NetworkManager* 控制」。此選項最適合用於在多個有線和無線網路之間進行切換。如果您執行的不是桌面環境 (GNOME 或 KDE)，或者您的電腦是 Xen 伺服器、虛擬系統或者會在網路中提供 DHCP 或 DNS 等網路服務，請使用「使用 *ifup* 的傳統方法」。如果使用 NetworkManager，則應使用 nm-applet 設定網路選項，且「網路設定」模組的「綜覽」、「主機名稱/DNS」和「路由」索引標籤都會處於停用狀態。如需 NetworkManager 的詳細資訊，請參閱第 26 章「使用 *NetworkManager*」[355 頁]。

在「IPv6 通訊協定設定」中，選擇是否要使用 IPv6 通訊協定。可以同時使用 IPv6 和 IPv4。預設會啟用 IPv6。但是，在不使用 IPv6 通訊協定的網路中，停用 IPv6 通訊協定時回應較快。若要停用 IPv6，請取消核取「啟用 IPv6」選項。這會停用 IPv6 核心模組的自動載入功能。重新開機後會套用此設定。

在「DHCP 用戶端選項」中，設定 DHCP 用戶端的選項。若希望 DHCP 用戶端要求伺服器一律廣播其回應，請核取「申請廣播回應」。如果您的機器需要在不同的網路之間移動，可能會需要核取該項。在一個網路中，每個 DHCP 用戶端的「DHCP 用戶端識別碼」均不能相同。若將其留為空白，則預設會使用網路介面的硬體位址。但是，如果您要使用同一個網路介面執行多個虛擬機，因此會使用同一個硬體位址，則請在此處指定不限格式的唯一識別碼。

「要傳送的主機名稱」指定當 dhcpcd 將訊息傳送至 DHCP 伺服器時，主機名稱選項欄位使用的字串。有些 DHCP 伺服器會根據此主機名稱 (動態 DNS) 更新名稱伺服器區域 (正向或反向記錄)。此外，有些 DHCP 伺服器需要「要傳送的主機名稱」選項欄位包含用戶端傳送之 DHCP 訊息中的特定字串。如果保留「自動」，將傳送目前的主機名稱 (即 /etc/HOSTNAME 中定義的主機名稱)。將選項欄位留為空白則不會傳送主機名稱。如果您不希望根據 DHCP 的資訊變更預設路由，請取消核取「透過 DHCP 變更預設路由」。

21.4.1.2 變更網路卡組態

若要變更網路卡組態，請在 YaST 的「網路設定」>「綜覽」中偵測到的網路卡清單中選取網路卡，然後按一下「編輯」。「網路卡設定」對話方塊隨即出現，您可以使用「一般」、「位址」和「硬體」索引標籤調整網路卡的組態。如需關於無線網路卡組態的更多資訊，請參閱第 18.5 節「使用 YaST 進行設定」[211頁]。

設定 IP 位址

在「網路卡設定」對話方塊的「位址」索引標籤中，可以設定網路卡的 IP 位址或確定其 IP 位址的方式。系統支援 IPv4 和 IPv6 兩種位址。您可以為網路卡設定「無 IP 位址」(適用於 Bonding 設備)、「靜態指定的 IP 位址」(IPv4 或 IPv6)，也可以透過「DHCP」或與「Zeroconf」為其指定「動態位址」。

若要使用「動態位址」，請選擇是使用「僅限 DHCP 版本 4」(適用於 IPv4)、「僅限 DHCP 版本 6」(適用於 IPv6)，還是「DHCP 版本 4 與 6」。

若情況適合，系統會將安裝時第一個可用的已連結網路卡自動設定為使用透過 DHCP 設定的自動位址。在預設會啟用 NetworkManager 的 SUSE Linux Enterprise Desktop 中，所有網路卡都已設定好。

注意：IBM System z 和 DHCP

在 IBM System z 平台上，只有擁有 MAC 位址的網路卡才會支援 DHCP 式的位址組態。此情況只適用於 OSA 和 OSA 高速網路卡。

若您用的是 DSL 連線而非 ISP (網際網路服務提供者) 指定的靜態 IP，還應該使用 DHCP。若您決定使用 DHCP，請在 YaST 網路卡組態模組中開啟「網路設定」對話方塊，於「全域選項」索引標籤的「DHCP 用戶端選項」中設定詳細資料。在「申請廣播回應」中指定 DHCP 用戶端是否應要求伺服器一律廣播其回應。如果您的機器是需要不同網路之間移動的行動用戶端，則可能需要核取此選項。若您將虛擬主機設定為透過同一個介面與不同的主機進行通訊，則需要使用「DHCP 用戶端識別碼」來分辨它們。

DHCP 對於用戶端組態是不錯的選擇，但不適用於伺服器組態。若要設定靜態 IP 位址，請如下執行：

- 1 在 YaST 網路卡組態模組的「綜覽」索引標籤中，於偵測到的網路卡清單中選取一個網路卡，然後按一下「編輯」。
- 2 在「位址」索引標籤中，選擇「靜態指定的 IP 位址」。
- 3 輸入「IP 位址」。使用 IPv4 和 IPv6 位址都可以。在「子網路遮罩」中輸入網路遮罩。若使用 IPv6 位址，請以 /64 格式使用「子網路遮罩」做為字首長度。

您還可以選擇為此位址輸入完全合法的「主機名稱」，它將會寫入 /etc/hosts 組態檔案中。
- 4 按一下「下一步」。
- 5 若要啟用組態，請按一下「確定」。

若使用靜態位址，系統將不會自動設定名稱伺服器和預設閘道。若要設定名稱伺服器，請依第 21.4.1.4 節「設定主機名稱和 DNS」[267頁] 中的說明進行。若要設定閘道，請依第 21.4.1.5 節「設定路由」[269頁] 中的說明進行。

設定別名

一張網路卡可擁有多 IP 位址，稱為別名。

注意：別名是相容性功能

所說的這些別名或標籤僅適用於 IPv4。如果是 IPv6，則會被忽略。使用 `iproute2` 網路介面時可以使用一或多個地址。

若要使用 YaST 設定您網路卡的別名，請執行以下步驟：

- 1 在 YaST 網路卡組態模組的「綜覽」索引標籤中，於偵測到的網路卡清單中選取一個網路卡，然後按一下「編輯」。
- 2 在「位址」>「其他位址」索引標籤中，按一下「新增」。
- 3 輸入「別名」、「IP 位址」和「網路遮罩」。別名中不要包含介面名稱。
- 4 按一下「確定」。
- 5 按一下「下一步」。
- 6 若要啟用組態，請按一下「確定」。

變更設備名稱和 Udev 規則

可以在網路卡正在使用中時變更它的設備名稱。也可以決定網路卡是否應由 `udev` 透過其硬體 (MAC) 位址或透過匯流排 ID 識別。後者更適合大型伺服器，可以方便熱交換網路卡。若要使用 YaST 設定這些選項，請執行下列步驟：

- 1 在 YaST 「網路設定」模組的「綜覽」索引標籤中，於偵測到的網路卡清單中選取一個網路卡，然後按一下「編輯」。
- 2 移至「硬體」索引標籤。目前的設備名稱顯示在「Udev 規則」中。按一下「變更」。
- 3 選擇 `udev` 是應透過網路卡的「MAC 位址」還是透過「匯流排 ID」來識別網路卡。網路卡目前的 MAC 位址和匯流排 ID 將顯示在對話方塊中。
- 4 若要變更設備名稱，請選取「變更設備名稱」選項，然後編輯名稱。

- 5 按一下「確定」，然後按「下一步」。
- 6 若要啟用組態，請按一下「確定」。

變更網路卡核心驅動程式

有些網路卡可能有多個核心驅動程式可供使用。如果網路卡已設定，YaST可讓您從可用且適合的驅動程式清單中選取要使用的核心驅動程式。還可以為核心驅動程式指定選項。若要使用 YaST 設定這些選項，請執行下列步驟：

- 1 在 YaST 網路設定模組的「綜覽」索引標籤中，於偵測到的網路卡清單中選取一個網路卡，然後按一下「編輯」。
- 2 移至「硬體」索引標籤。
- 3 在「模組名稱」中選取要使用的核心驅動程式。在「選項」中以 選項=值 的格式輸入選定驅動程式的選項。若要使用多個選項，應以空格將其隔開。
- 4 按一下「確定」，然後按「下一步」。
- 5 若要啟用組態，請按一下「確定」。

啟動網路設備

若使用傳統的 ifup 方法，可以設定您的設備在開機時、連接纜線時、偵測到網路卡時啟動，或以手動方式啟動，或者永不啟動。若要變更設備啟動，請執行下列步驟：

- 1 在 YaST 的「網路設備」>「網路設定」中，於偵測到的網路卡清單中選取一個網路卡，然後按一下「編輯」。
- 2 在「一般」索引標籤中，從「設備啟用」中選擇希望的項目。

選擇「開機時」可在系統開機時啟動設備。若使用「電纜連線」，系統會監控介面，探查是否有實體的連線。若使用「Hotplug」，只要介面可用就會將其設定。它與「開機時」選項類似，唯一的區別在於如果開機時介面不存在，則不會發生錯誤。選擇「手動」可以透過 ifup 手動控制介面。選取「永不」則根本不會啟動設備。「在 NFSroot 時」與「開機時」類似，區別是使用指令 `rcnetwork stop` 不會關閉介面。若您使用的是 `nfs` 或 `iscsi` 根檔案系統，請使用此選項。

- 3 按一下「下一步」。
- 4 若要啟用組態，請按一下「確定」。

一般只有系統管理員可以啟動和取消啟動網路介面。若想讓任何使用者都能透過 KInternet 啟用此介面，請選取「允許非 *root* 使用者透過 Kinternet 控制設備」。

設定最大傳送單位大小

您可以設定介面的最大傳送單位 (MTU)。MTU 指允許的最大封包大小 (以位元組計)。MTU 越高，頻寬效率就越高。但是，大型封包可能會將慢速介面阻擋一段時間，這會加劇後續封包的延遲。

- 1 在 YaST 的「網路設備」>「網路設定」中，於偵測到的網路卡清單中選取一個網路卡，然後按一下「編輯」。
- 2 在「一般」索引標籤中，從「設定 MTU」清單中選取所需的項目。
- 3 按一下「下一步」。
- 4 若要啟用組態，請按一下「確定」。

設定防火牆

您不需輸入第 15.4.1 節「Configuring the Firewall with YaST」(第 15 章「*Masquerading and Firewalls*」, ↑*Security Guide*) 所說明的詳細防火牆資訊，僅需在設備設定時判斷基本防火牆設定即可。請執行下列步驟：

- 1 開啟 YaST 的「網路設備」>「網路設定」模組。在「綜覽」索引標籤中，於偵測到的網路卡清單中選取一個網路卡，然後按一下「編輯」。
- 2 進入「網路設定」對話方塊的「一般」索引標籤。
- 3 決定您要為介面指派的防火牆區域。可用的選項如下：

停用防火牆

只有當防火牆已停用以及防火牆根本未執行時，此選項才可用。唯有您的機器位於受外部防火牆保護的更大網路中時，才能使用此選項。

自動指定區域

只有當防火牆已啟用時，此選項才可用。防火牆會執行，並且介面會自動指定至防火牆區域。包含關鍵字 `any` 的區域或外部區域將會用於這類介面。

內部區域 (未保護)

防火牆會執行，但不強制執行任何保護此介面的規則。如果您的機器位於受外部防火牆保護的更大網路中，請使用此選項。如果機器具有多個網路介面，此選項也適用於連接到內部網路的介面。

廢除區域

廢除區域是內部網路與 (有潛在風險的) 網際網路之前的另一道防線。從內部網路與網際網路都可連接到指派至此區域的主機，但主機無法連存取內部網路。

外部區域

防火牆執行於此介面上，且會全面保護其抵禦其他危險網路流量的攻擊。此為預設選項。

4 按「下一步」。

5 按一下「確定」以啟用組態。

21.4.1.3 設定未偵測到的網路卡

您的網路卡有可能會無法正確偵測到。若發生此情況，該卡就不會出現在偵測到的網路卡清單中。若您確定您的系統具備網路卡的驅動程式，可手動設定。也可設定特殊的網路設備類型，如橋接、Bond、TUN 或 TAP。若要設定未偵測到的網路卡或特殊設備，請執行下列步驟：

- 1 在 YaST 的「網路設備」>「網路設定」>「綜覽」對話方塊中，按一下「新增」。
- 2 在「硬體」對話方塊中，從可用的選項中設定介面的「設備類型」和「組態名稱」。如果網路卡是 PCMCIA 或 USB 設備，請啟用個別的核取方塊並使用「下一步」來結束對話方塊。否則，您可以根據需要定義要用於網路卡的核心「模組名稱」以及卡的「選項」。

在「*Ethtool* 選項」中，可以設定 `ifup` 用於介面的 `ethtool` 選項。有關可用的選項，請參閱 `ethtool` 手冊頁。如果選項字串以 `-` 開頭 (例如 `-K` 介面

名稱 `rx on`)，則字串中的第二個單字會取代為目前的介面名稱。否則(例如 `autoneg off speed 10) ifup` 會在前面加上 `-s` 介面名稱。

- 3 按一下「下一步」。
- 4 在「一般」、「位址」和「硬體」索引標籤中設定介面的所有必要選項，例如 IP 位址、設備啟動或防火牆區域。如需組態選項的詳細資訊，請參閱第 21.4.1.2 節「變更網路卡組態」[261頁]。
- 5 若您介面設備類型選擇「無線」，請在下一個對話設定無線連接。關於無線設備組態的詳細資料位於第 18 章「無線區域網路」[207頁]。
- 6 按一下「下一步」。
- 7 若要啟用新網路組態，請按一下「確定」。

21.4.1.4 設定主機名稱和 DNS

若您在安裝期間未變更網路組態，且已有有線網路卡可用，則系統會自動為您的電腦產生主機名稱並啟動 DHCP。同時也會自動產生您主機要整合至網路環境所需的名稱服務資訊。若網路位址設定使用 DHCP，則網域名稱伺服器清單會自動填入適當的資料。若您希望使用靜態設定，請手動設定數值。

若要變更您電腦的名稱並調整名稱伺服器搜尋清單，請如下執行：

- 1 在 YaST 的「網路設備」模組中，移至「網路設定」>「主機名稱/DNS」索引標籤。
- 2 輸入「主機名稱」並根據需要輸入「網域名稱」。如果機器是郵件伺服器，網域就格外重要。請注意，主機名稱是全域的，會套用於所有已設定的網路介面。

若您要使用 DHCP 獲取 IP 位址，則電腦的主機名稱由 DHCP 自動設定。若要連接到其他網路，最好停用此選項，因為其他網路可能會指定其他主機名稱，而在執行時期變更主機名稱會混淆圖形桌面。若要停止使用 DHCP 獲取 IP 位址，請取消核取「透過 DHCP 變更主機名稱」。

「將主機名稱指定至迴路 IP」會將您的主機名稱與 `/etc/hosts` 中的 127.0.0.2 (迴路) IP 位址進行關聯。如果您希望主機名稱始終能得到解析(即使是沒有使用中網路的情況下)，則可以使用此選項。

- 3 在「*修改DNS組態*」中，選取修改DNS組態(名稱伺服器、搜尋清單、`/etc/resolv.conf` 檔案的內容)的方式。

若選取「*使用預設規則*」選項，則組態由 `netconfig` 程序檔來處理，這樣會將靜態定義的資料(使用 YaST 或在組態檔案中)與從 DHCP 用戶端或 NetworkManager 動態取得的資料合併。此預設規則能夠處理大部分的情況。

若選取「*僅手動*」選項，則無法使用 `netconfig` 修改 `/etc/resolv.conf` 檔案。但是可以手動編輯此檔案。

若選取「*自定規則*」選項，則應指定定義合併規則的「*自定規則*」字串。該字串包含要視為設定之有效來源的介面名稱清單(以逗號分隔)。除完整的介面名稱外，還允許使用基本萬用字元來對應多個介面。例如，`eth* ppp?` 將先找到所有 `eth`，然後找到所有 `ppp0-ppp9` 介面。以下為指定如何套用 `/etc/sysconfig/network/config` 檔案中所定義之靜態設定的兩個特定規則值：

STATIC

靜態設定必須與動態設定合併在一起。

STATIC_FALLBACK

只有動態組態不可用時才會使用靜態設定。

如需詳細資訊，請參閱 `man 8 netconfig`。

- 4 輸入「*名稱伺服器*」並填寫「*網域搜尋*」清單。名稱伺服器必須透過 IP 位址而非主機名稱指定，例如 `192.168.1.116`。在「*網域搜尋*」索引標籤中指定的名稱就是用於解析沒有指定網域之主機名稱的網域名稱。如果使用多個「*網域搜尋*」，請以逗號或空格將網域隔開。

- 5 若要啟用組態，請按一下「*確定*」。

還可以使用 YaST 透過指令行編輯主機名稱。YaST 執行的變更會立即生效(手動編輯 `/etc/HOSTNAME` 檔案的情況除外)。若要變更主機名稱，請使用下列指令：

```
yast dns edit hostname=hostname
```

若要變更名稱伺服器，請使用下列指令：

```
yast dns edit nameserver1=192.168.1.116
```

```
yast dns edit nameserver2=192.168.1.116
```

```
yast dns edit nameserver3=192.168.1.116
```

21.4.1.5 設定路由

若要讓您的電腦與其他電腦和其他網路通訊，必須提供路由資訊，以讓網路流量採取正確的路徑。若使用 **DHCP**，會自動提供此資訊。若使用靜態設定，必須手動新增此資料。

- 1 在 YaST 中，移至「**網路設定**」>「**路由**」。
- 2 輸入「**預設開道**」的 IP 位址 (必要時可以輸入 IPv4 和 IPv6)。預設開道會比對每個可能的目的地，但是如果任何其他符合所需位址的項目已經存在，就會使用該項目而非預設路由。
- 3 可以在「**路由表**」中輸入更多項目。輸入「**目的地**」網路 IP 位址、「**開道**」IP 位址和「**網路遮罩**」。選取要透過其將流量路由至所定義網路的「**設備**」(減號表示任意設備)。若要省略這些值的任何一個，請使用減號「-」。若要在表中輸入預設開道，請在「**目的地**」欄位中使用「default」。

注意

若使用了多個預設路由，則可以指定權值選項確定哪個路由的優先程度較高。要指定權值選項，請在「**選項**」中輸入 - metric 數值。權值最高的路由做為預設路由。如果該網路設備已解除連接，將會移除其路由，使用下一個路由。不過，目前的核心不會在靜態路由中使用權值，只有 **multipathd** 等路由精靈會使用。

- 4 如果系統是路由器，請在「**網路設定**」中啟用「**IP 轉遞**」選項。
- 5 若要啟用組態，請按一下「**確定**」。

21.4.2 數據機

提示：IBM System z：數據機

IBM System z 平台不支援此類型的硬體組態。

在「YaST 控制中心」中，您可透過「網路設備」>「數據機」存取數據機組態。如果無法自動偵測到您的數據機，請移至「數據機設備」索引標籤，按一下「新增」開啟對話方塊以手動組態。在「數據機設備」中輸入數據機要連接的介面。

提示：CDMA 和 GPRS 數據機

使用 YaST 「數據機」模組來設定支援的 CDMA 和 GPRS 數據機，這與您設定一般數據機使用的方式一樣。

圖形 21.4 數據機組態

**數據機參數**

輸入所有數據機組態值。「數據機裝置」指定數據機所連的埠。ttyS0、ttyS1 等是指序列埠。[更多](#)

數據機設備(U):

/dev/modem

▼

撥號前置號碼 (如果需要)(N):

撥號模式

特殊設定

☒ 撥建式撥號(D)

☒ 開啟喇叭(S)

☐ 轉盤式撥號(P)

☒ 偵測撥號聲音(E)

詳細資訊(I)

說明

取消(C)

上一步(B)

下一步(N)

如果您使用的是專用交換機(PBX)，可能需要輸入撥號前置號碼。通常為0。請參閱 PBX 隨附的說明。另外，請選擇是否使用按鍵式或轉盤式撥號、是否應開啟喇叭，以及數據機偵測撥號音前是否應等待。如果數據機連接到分機，就不能啟用最後一個選項。

在「詳細資料」下，設定傳輸速率和數據機的啟始字串。只有在無法自動偵測您的數據機或是數據機需要特殊設定來傳輸資料時，才能變更這些設定。這些設定主要適用於 ISDN 終端機介面卡。按一下「確定」來結束此對話方塊。若要將數據機控制權委託給不具備 root 許可權的一般使用者，請啟用「允許非 root 使用者透過 Kinternet 控制設備」。使用此方式，使用者即可啟用和停用介面，而不需要管理員的許可。在「撥號前置號碼正規表示式」下，指定一個正規表示式。KInternet 中的「撥號前置號碼」(一般使用者均可修改)，必須符合此正規表示式。如果此欄位為空白，則使用者必須有管理員許可才能設定不同的「撥號前置號碼」。

在下一個對話方塊中選取 ISP。如果要從國內的 ISP 預先定義清單中選擇，請選取「國家」。或者，可按一下「新增」來開啟一個對話方塊，您可以在其中輸入您的 ISP 資料。這包括撥接連接名稱、ISP 名稱以及您的 ISP 提供的登入名稱和密碼。啟用「永遠詢問密碼」，以提示您在每次連接時輸入密碼。

在最後一個對話方塊中，可以指定其他的連接選項：

「視需要撥號」

如果您啟用了「依需求撥號」，請至少設定一個名稱伺服器。因為許多程式需要定期從網際網路獲取資料，所以請僅在網路網際連線費用較低的情況下使用此功能。

「連接時修改 DNS」

此選項是依照預設啟用的，每次您連接到網際網路時，即會更新名稱伺服器位址。

「自動取回 DNS」

如果提供者沒有在連接後傳輸其網域名稱伺服器，則應停用此選項並手動輸入 DNS 資料。

「自動重新連接」

若啟用此選項，則會在連線失敗後自動重新建立連線。

「忽略提示」

此選項會停止偵測來自撥號伺服器的所有提示。如果建立的連線太慢或完全沒有作用，請嘗試此選項。

「外部防火牆介面」

選取此選項可啟動防火牆並將介面設為外部。這樣就可讓您在連接網際網路時免遭外部的攻擊。

「*閒置逾時 (秒)*」

使用此選項來指定網路靜止一段時間後即自動中斷數據機的連接。

「*IP 詳細資料*」

這會開啟位址組態對話方塊。如果您的 ISP 沒有為您的主機指定動態 IP 位址，請停用「*動態 IP 位址*」然後輸入您主機的本地 IP 位址和遠端 IP 位址。請向您的 ISP 詢問此資訊。讓「*預設路由*」保持為啟用狀態並選取「*確定*」來結束此對話方塊。

選取「*下一步*」回到原先的顯示數據機組態摘要的對話方塊。按一下「*確定*」關閉此對話方塊。

21.4.3 ISDN

提示： IBM System z：ISDN

IBM System z 平台不支援此類型的硬體組態。

使用此模組來為您的系統設定一個或多個 ISDN 卡。如果 YaST 未偵測到您的 ISDN 卡，請在「*ISDN 設備*」索引標籤中按一下「*新增*」，然後手動選取您的卡。可以有多個介面，但多個 ISP 只能設定一個介面。在接下來的對話方塊中，設定網路卡正常運作所需的 ISDN 選項。

圖形 21.5 ISDN 組態

 **contr0 的 ISDN 低階組態**
使用「開機時」，會在系統開機時載入驅動程式。若使用「手動」，驅動程式必須以 rcisdn start 指令開始。只有 root 使用... [更多](#)

ISDN 卡資訊

廠商	Abocom/Magitek
ISDN 卡	2BD1

驅動程式(V):

ISDN 協定

☒ Euro-ISDN (EDSSI)(E)
☐ ITR6(G)
☐ 租用專線(L)
☐ NII(I)

國家(C): 代碼(D):

區域號碼(A): 撥號前置號碼(O):

☒ 啟動 ISDN 記錄(I)

啟用服務(D):

[?](#) 說明 [取消](#) [上一步](#) [確定](#)

在下一個對話方塊中 (如圖形 21.5 「ISDN 組態」 [273頁] 中所示)，選取要使用的通訊協定。預設為「*Euro-ISDN (EDSSI)*」，但如果是較舊或較大型的交換機，則選取「*ITR6*」。如果您是在美國，請選取「*NII*」。在相關欄位中選取您的國家。其對應的國家代碼會顯示在旁邊的欄位。最後，提供您的「區域號碼」和「撥號前置號碼」(如有需要)。若不想記錄所有的 ISDN 流量，請取消核取「*啟動 ISDN 記錄*」選項。

「*啟動設備*」可定義 ISDN 介面的啟動方式：選取「*開機時*」會在系統每次開機時啟始化 ISDN 驅動程式。「*手動*」要求您以 root 身份使用 `rcisdn start` 指令來載入 ISDN 驅動程式。「*熱插*」用於 PCMCIA 或 USB 設備，會在插入設備後載入驅動程式。完成上述設定之後，請選取「*確定*」。

在下一個對話方塊中，指定您 ISDN 卡的介面類型，並將 ISP 新增至現有的介面。介面可能為 SyncPPP 或 RawIP 類型，但大多數 ISP 是在 SyncPPP 模式中操作，其說明如下。

圖形 21.6 ISDN 介面組態

新增 SyncPPP 介面 ippp0

我的電話號碼 -- 擁有電話號碼 (MSN) 時，如果 ISDN 卡直接對接到電話公司提供的插槽中，則請加入此... [更多](#)

連接設定

我的電話號碼(P):

啟用服務(O):

手動

☒ 允許非 root 使用者經由 KInternet 進行裝置控制(N)

☒ ChargeHUP(H)

☐ 通道連結(A)

☒ 外部防火牆介面(W)

☒ 重新啟動防火牆(W)

詳細資訊(D)...

說明 取消(C) 上一步(B) 下一步(N)

視您的特殊設定而定，在「我的電話號碼」中必須輸入的號碼會有所不同：

ISDN 卡直接連至電話插孔

標準 ISDN 連接會提供 3 組電話號碼 (稱為多重用戶號碼或 MSN)。如果訂閱者要求更多，最多可以到 10，所有的 MSN 都必須在此輸入，但不需輸入區域碼。如果您輸入錯誤的號碼，您的電話操作員會自動回復指定給您的 ISDN 連接的第一組 MSN。

連接至專用交換機的 ISDN 卡

此外，視安裝的設備而定，組態可能會有所不同：

1. 小型的專用交換機 (PBX) 大多使用 Euro-ISDN (EDSS1) 通訊協定來撥接內線電話。這些電話交換機有一個內部 S0 匯流排並在連接設備上使用內部號碼。

使用其中一組內部號碼做為您的 MSN。您至少可使用一組電話交換機的 MSN，這些 MSN 已啟用可直接對外撥號。如果無法使用，請嘗試撥 0。如需詳細資訊，請參閱您的電話交換機隨附的文件。

2. 較大型的商用電話交換機通常使用 1TR6 通訊協定來撥接內線電話。其 MSN 稱為 EAZ，通常可對應直撥號碼。如果要在 Linux 中設定組態，請輸入 EAZ 的最後一碼即可。最後一步是試著撥從 1 到 9 的每個數字。

如果想在下一個收費單位開始之前終止連接，可啟用「*ChargeHUP*」。不過，要記得並不是每個 ISP 都適用。您也可以勾選對應的選項來啟用通道合併 (多重連結 PPP)。最後，您可以選取「外部防火牆介面」和「重新啟動防火牆」來啟用連結的防火牆。要讓沒有管理員許可權的一般使用者能夠啟動或取消啟動介面，請選取「允許非 *root* 使用者透過 *Kinternet* 控制設備」。

「詳細資料」會開啟一個對話方塊，用來執行更複雜的連線配置 (一般的家庭使用者不會用到此類配置)。選取「確定」以結束「詳細資料」對話方塊。

在下一個對話方塊中設定 IP 位址設定。如果您的提供者沒有給您一個靜態 IP，請選取「動態 IP 位址」。或者，可根據您 ISP 的規格，在提供的欄位中輸入您主機的本地 IP 位址和遠端 IP 位址。如果該介面應做為網際網路的預設路由，請選取「預設路由」。每個主機只能設定一個介面做為預設路由。選取「下一步」來結束此對話方塊。

下列對話方塊中可讓您設定您的國家和選取 ISP。清單中所列的 ISP 只有撥號計費提供者。如果您的 ISP 不在清單上，請選取「新增」。會開啟「提供者參數」對話方塊，您可在其中輸入您 ISP 的所有詳細資料。輸入電話號碼時，在數字之間不能有空白或逗號。最後，請輸入您的 ISP 所提供的登入名稱和密碼。完成後，請選取「下一步」。

如果要在獨立的工作站上使用「依需求撥號」，請同時指定名稱伺服器 (DNS 伺服器)。大多數 ISP 均支援動態 DNS，即在您每次連接時 ISP 都會送出一個名稱伺服器的 IP 位址。不過，如果您使用的是單一工作站，您仍需提供一個替代位址，例如 192.168.22.99。如果您的 ISP 不支援動態 DNS，請指定 ISP 的名稱伺服器 IP 位址。如有需要，可為連接指定一個時限，即為未使用網路的時間 (以秒為單位)，之後即會自動終止連接。使用「下一步」來確認您的設定。YaST 會顯示已設定介面的摘要。若要啟用這些設定，請選取「確定」。

21.4.4 纜線數據機

提示：IBM System z：纜線數據機

IBM System z 平台不支援此類型的硬體組態。

在有些國家/地區，透過電視纜線來存取網際網路的現象相當普遍。有線電視用戶通常會有一部數據機，一邊連接到電視纜線的輸出端子，另一邊(使用10Base-TG 雙絞纜線)連接到電腦網路卡。接著纜線數據機會以固定的 IP 位址提供專用的網際網路連線。

視您的 ISP 所提供的說明而定，設定網路卡時可選取「*動態位址*」或「*靜態指定的IP 位址*」。現在大多數提供者都使用 DHCP。靜態 IP 位址通常是特殊商用帳戶的一部分。

21.4.5 DSL

提示：IBM System z：DSL

IBM System z 平台不支援此類型的硬體組態。

如果要設定您的 DSL 設備，請從 YaST 「*網路卡設備*」區段選取「*DSL*」模組。此 YaST 模組含有多個對話方塊，可根據下列其中一種通訊協定在其中設定 DSL 連接的參數：

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoATM)
- CAPI for ADSL (Fritz 網路卡)
- 點對點通道通訊協定 (PPTP)—奧地利

在「*DSL 組態綜覽*」對話方塊的「*DSL 設備*」索引標籤中，提供有已安裝 DSL 設備的清單。若要變更某個 DSL 設備的組態，請在清單中將其選定，然後按一下「*編輯*」。按一下「*新增*」可以手動設定新的 DSL 設備。

PPPoE 或 PPTP 類型的 DSL 連線組態，要求對應的網路卡必須正確設定。如果您尚未完成此步驟，請先選取「*設定網路卡*」來進行設定(請參閱 第 21.4.1 節「使用 YaST 設定網路卡」[259 頁])。若是 DSL 連結，將會自動指定位址而不是透過 DHCP 指定，因此您不可啟用「*動態位址*」選項。而是應該輸入介面的靜態虛擬位址，例如 192.168.22.1。在「*子網路遮罩*」中，輸入 255.255.255.0。如果您要設定獨立的工作站，則應保留「*預設開道*」為空白。

提示

「*IP 位址*」和「*子網路遮罩*」中的值只是預留位置。只用來啟始化網路卡，而不代表 DSL 連接等等。

在第一個 DSL 組態對話方塊 (請參閱圖形 21.7 「DSL 組態」 [277頁]) 中，選取「*PPP 模式*」和 DSL 數據機要連接的「*乙太網路卡*」(大多為 `eth0`)。然後使用「*啟動設備*」來指定是否要在開機過程中建立 DSL 連結。按一下「*允許非 root 使用者透過 KInternet 控制設備*」，以授權不具備 `root` 許可權的一般使用者透過 KInternet 啟動或取消啟動介面。

在下一個對話方塊中選取國家/地區，並從該國家/地區的多個 ISP 營運商中進行選擇。後續的 DSL 組態對話方塊詳細資料會視目前已設定的選項而定，因此下列段落只提供簡單的介紹。如需可用選項的詳細資訊，請參閱對話方塊中的詳細說明。

圖形 21.7 DSL 組態

 **DSL 組態**
在此處可以設定 DSL 連接最重要的設定。首先，請選擇 PPP 模式。這可以是 PPP over Ethernet (PPPoE)、PPP over ATM (PPPoATM)、CAPi for ADSL 或 Point-to-Point (PPPoA)。

DSL 連接設定

PPP 模式(M):

PPP 模式相關設定

VPI/VCI(V):

乙太網路卡(E):

網路卡 - DHCP 位址

何種網路模式 IP 位址(I):

設定網路卡(C)

啟用服務(O):

☒ 允許非 root 使用者藉由 KInternet 進行裝置控制(N)

如果要在獨立的工作站上使用「*視要求撥號*」，請指定名稱伺服器 (DNS 伺服器)。大部份 ISP 均支援動態 DNS，即為每次連接時，名稱伺服器送出的 IP 位址。不過，如果是單一工作站，請提供一個替代位址，例如 192.168.22.99。如果您的 ISP 不支援動態 DNS，請輸入您 ISP 提供的名稱伺服器 IP 位址。

「閒置逾時 (秒)」定義網路靜止一段時間後即自動中斷連接。合理的逾時秒數為 60 和 300 秒。如果停用「視需要撥號」，將逾時值設為零將有助於避免自動掛斷。

T-DSL 的組態與 DSL 的設定非常相似。只要選取「*T-Online*」做為您的提供者，YaST 就會開啟 T-DSL 組態對話方塊。此對話方塊提供了一些 T-DSL 要求的其他資訊，包括線路 ID、T-Online 號碼、使用者代碼以及您的密碼。在您加入 T-DSL 後，應該會收到這些資訊。

21.4.6 IBM System z：設定網路設備

適用於 IBM System z 的 SUSE Linux Enterprise Server 支援多種不同類型的網路介面。您可使用 YaST 設定所有類型。

21.4.6.1 qeth-hsi 設備

若要將 `qeth-hsi` (Hipersocket) 介面新增到已安裝的系統，請啟動 YaST 中的「網路設備」>「網路設定」模組。選取其中一個標示為「*Hipersocket*」的設備做為「讀取」設備位址，然後按一下「編輯」。輸入讀取通道、寫入通道和控制通道的設備編號(設備編號格式的範例：0.0.0600)。然後按「下一步」。在「網路位址設定」對話方塊中，指定新介面的 IP 位址和網路遮罩，然後按「下一步」和「確定」結束網路組態。

21.4.6.2 qeth-ethernet 設備

若要將 `qeth-ethernet` (IBM OSA Express 乙太網路卡) 介面新增到已安裝的系統，請啟動 YaST 中的「網路設備」>「網路設定」模組。選取其中一個標記為「*IBM OSA 高速乙太網路卡*」的設備來做為「讀取」設備位址，然後按一下「編輯」。輸入讀取通道、寫入通道和控制通道的設備編號(設備編號格式的範例：0.0.0600)。輸入所需的連接埠名稱、埠號碼(如果適用)、一些其他選項(請參閱 http://www.ibm.com/developerworks/linux/linux390/documentation_novell_suse.html 中的《*Linux for IBM System z: Device Drivers, Features, and Commands*》(適用於 IBM System z 的 Linux：設備驅動程式、功能和指令)手冊)、IP 位址和適當的網路遮罩。按「下一步」與「確定」結束網路組態。

21.4.6.3 ctc 設備

若要將 `ctc` (IBM 平行埠 CTC 介面卡) 介面新增到已安裝的系統，請啟動 YaST 中的「網路設備」>「網路設定」模組。選取一個標示為「*IBM 平行埠 CTC 介面卡*」的設備做為您的讀取通道，然後按一下「設定」。選擇適合您設備的「設備設定」(通常為「相容模式」)。指定您和遠端合作夥伴的 IP 位址。如有需要，可透過「進階」>「細節設定」來調整 MTU 的大小。按「下一步」與「確定」結束網路組態。

警告

不建議使用此介面。未來版本的 SUSE Linux Enterprise Server 將不支援此介面。

21.4.6.4 lcs 設備

若要將 `lcs` (IBM OSA-2 介面卡) 介面新增到已安裝的系統，請啟動 YaST 中的「網路設備」>「網路設定」模組。選取標示為「*IBM OSA-2 介面卡*」的設備，然後按一下「設定」。輸入所需的埠號、一些其他選項 (請參閱 http://www.ibm.com/developerworks/linux/linux390/documentation/novell_suse.html 中的《Linux for IBM System z: Device Drivers, Features, and Commands》(適用於 IBM System z 的 Linux：設備驅動程式、功能和指令) 手冊)、IP 位址和適當的網路遮罩。按「下一步」與「確定」結束網路組態。

21.4.6.5 IUCV 設備

若要將 `iucv` (IUCV) 介面新增到已安裝的系統，請啟動 YaST 中的「網路設備」>「網路設定」模組。選取標示為「*IUCV*」的設備，並按一下「編輯」。YaST 會提示您提供 IUCV 合作夥伴的名稱(「對等」)。輸入名稱(本項目區分大小寫)然後選取「下一步」。指定合作夥伴的「IP 位址」及「遠端 IP 位址」。如果需要，在「一般」索引標籤中「設定 MTU」大小。按「下一步」與「確定」結束網路組態。

警告

不建議使用此介面。未來版本的 SUSE Linux Enterprise Server 將不支援此介面。

21.5 NetworkManager

NetworkManager 是筆記型電腦與其他可攜式電腦的理想解決方案。有了 NetworkManager，您在移動中，就不必耽心網路介面的組態設定，也不必切換網路。

21.5.1 NetworkManager 和 ifup

不過，NetworkManager 解決方案並不適用於所有情況，因此您仍然可以在管理網路連線 (ifup) 的傳統方法與 NetworkManager 之間進行選擇。如果要使用 NetworkManager 管理網路連線，請依第 26.2 節「啟用或停用 NetworkManager」[356頁]中所述啟用 YaST 網路設定模組中的 NetworkManager，然後使用 NetworkManager 設定網路連線。如需使用案例的清單以及如何設定與使用 NetworkManager 的詳細說明，請參閱第 26 章「使用 NetworkManager」[355頁]。

ifup 與 NetworkManager 之間的區別包括：

root 權限

如果使用 NetworkManager 設定網路，就可以隨時使用 Applet 在您的桌面環境上輕鬆切換、停止或啟動網路連線。NetworkManager 也讓您不需要 root 權限就可以變更和設定無線網路卡連接。因此，NetworkManager 是行動工作站理想的解決方案。

傳統的 ifup 組態也提供一些切換、停止或啟動連線的方式，其中有需要使用者介入的，也有不需要的，就像使用者管理的設備。但是，使用此方法始終需要 root 權限來變更或設定網路設備。這對行動計算設備而言，往往會造成問題，因為不可能預先設定好所有可能的連線。

網路連線的類型

不論是傳統組態還是 NetworkManager，都能使用 DHCP 和靜態組態來處理無線網路 (會存取 WEP、WPA-PSK 和 WPA-Enterprise) 和有線網路的網路連線。它們也支援透過撥號、DSL 和 VPN 建立的連線。透過 NetworkManager，您還可以連接行動寬頻 (3G) 數據機，而使用傳統組態則不能做到這一點。

NetworkManager 會嘗試使用最好的連接，讓您的電腦隨時保持連接狀態。如果網路纜線突然中斷，它會嘗試重新連接。它可以從您的無線連線清單中

找到訊號最強的網路，並自動用它來連接。如果要用 ifup 達到相同的功能，必須執行很多組態工作。

21.5.2 NetworkManager 功能與組態檔案

使用 NetworkManager 建立的獨立網路連線設定儲存在組態設定檔中。使用 NetworkManager 或 YaST 設定的系統連線儲存於 `/etc/networkmanager/system-connections/*` 或 `/etc/sysconfig/network/ifcfg-*` 中。使用者定義的連線儲存在 GConf (GNOME) 或 `$HOME/.kde4/share/apps/networkmanagement/*` (KDE) 中。

如果未設定任何設定檔，NetworkManager 會自動建立一個，並將其命名為 `Auto$INTERFACE-NAME`。這是為了在未設定組態的情況下安全地處理盡可能多的案例。如果自動建立的設定檔不能滿足您的需要，請使用 KDE 或 GNOME 提供的網路連線組態對話方塊，根據需要修改這些設定檔。若需更多資訊，請參考第 26.3 節「設定網路連線」[357頁]。

21.5.3 控制與鎖定 NetworkManager 功能

在集中管理的機器上，可以使用 PolicyKit 控制或停用某些 NetworkManager 功能，例如，是否允許使用者修改管理員定義的連線，或者是否允許使用者定義自己的網路組態。若要檢視或變更各個 NetworkManager 規則，請啟動 PolicyKit 的圖形「授權」工具。這些規則位於左側網路樹中，「網路-管理員-設定」項目的下方。如需 PolicyKit 的簡介及其詳細使用方法，請參閱第 9 章「*PolicyKit*」(↑*Security Guide*)。

21.6 手動設定網路連線

網路軟體的手動組態應該永遠是最後的替代方案。建議使用 YaST。不過，這個有關網路組態的背景資訊也可協助您使用 YaST。

當核心偵測到網路卡並建立對應的網路介面時，它會根據探查到設備或載入核心模組的順序，為該設備指定名稱。只有在非常簡單或嚴密控制的硬體環境中，預設核心設備的名稱才可預測。如果系統允許在執行時期新增或移除硬體，或是支援自動設定設備組態，則無法準確預測核心在重新開機時指定的網路設備名稱。

但是，所有系統組態工具均依賴於永久的介面名稱。`udev` 解決了此問題。`udev` 永久網路產生器 (`/lib/udev/rules.d/75-persistent-net-generator.rules`) 會產生與硬體相符的規則 (預設使用其硬體位址)，並為硬體指定一個永遠唯一的介面。網路介面的 `udev` 資料庫儲存在檔案 `/etc/udev/rules.d/70-persistent-net.rules` 中。該檔案中的每一行描述一個網路介面並指定其永久名稱。系統管理員可以透過編輯 `NAME=""` 項目來變更指定的名稱。您也可以使用 `YaST` 修改永久規則。

表格 21.5 「手動網路組態程序檔」 [282頁] 總結了與網路組態相關的最重要的程序檔。

表格 21.5 手動網路組態程序檔

指令	函數
<code>ifup, ifdown, ifstatus</code>	<code>if</code> 程序檔會啟動或停止網路介面，或傳回指定介面的狀態。如需詳細資訊，請參閱 <code>ifup</code> 手冊頁。
<code>rcnetwork</code>	<code>rcnetwork</code> 程序檔可用於啟動、停止或重新啟動所有網路介面 (或指定的網路介面)。停止、啟動或重新啟動網路介面時分別使用 <code>rcnetwork stop</code> 、 <code>rcnetwork start</code> 和 <code>rcnetwork restart</code> 。若只需停止、啟動或重新啟動一個介面，請使用該命令，並在後面指定介面名稱，例如 <code>rcnetwork restart eth0</code> 。 <code>rcnetwork status</code> 指令顯示介面的狀態、IP 位址以及 DHCP 用戶端是否正在執行。使用 <code>rcnetwork stop-all-dhcp-clients</code> 和 <code>rcnetwork restart-all-dhcp-clients</code> 可以停止或重新啟動在網路介面上執行的 DHCP 用戶端。

如需 `udev` 和永久設備名稱的詳細資訊，請參閱第 14 章「使用 `udev` 進行動態核心設備管理」[167頁]。

21.6.1 組態檔案

本節提供網路組態檔的綜覽，並說明其用途和使用的格式。

21.6.1.1 `/etc/sysconfig/network/ifcfg-*`

這些檔案包含網路介面的組態。其中包含啟動模式和 IP 位址等資訊。可以使用的參數請參閱 `ifup` 的手冊頁。此外，如果一個一般設定只能用於一個介面，則檔案 `dhcp` 中的大多數變數在 `ifcfg-*` 檔案中都可以使用。但是，大多數 `/etc/sysconfig/network/config` 變數都是全域變數，在 `ifcfg` 檔案中不能將它們覆寫。例如，`NETWORKMANAGER` 或 `NETCONFIG_*` 變數就是全域變數。

如需 `ifcfg.template` 的相關資訊，請參閱第 21.6.1.2 節「`/etc/sysconfig/network/config` 和 `/etc/sysconfig/network/dhcp`」[283頁]。

► **System z:** IBM System z 不支援 USB。介面檔名稱和網路別名包含 `qeth` 等 System z 專屬元件。 ◀

21.6.1.2 `/etc/sysconfig/network/config` 和 `/etc/sysconfig/network/dhcp`

`config` 檔案包含 `ifup`、`ifdown` 和 `ifstatus` 行為的一般設定。`dhcp` 包含 DHCP 的設定。這兩個組態檔案中的變數都已被註解。`/etc/sysconfig/network/config` 中的某些變數也可以在 `ifcfg-*` 檔案中使用，而且在這些檔案中它們的優先程度更高。`/etc/sysconfig/network/ifcfg.template` 檔案列出了可在永久介面中指定的變數。但是，大多數 `/etc/sysconfig/network/config` 變數都是全域變數，在 `ifcfg` 檔案中不能將它們覆寫。例如，`NETWORKMANAGER` 或 `NETCONFIG_*` 變數就是全域變數。

21.6.1.3 /etc/sysconfig/network/routes 和 /etc/sysconfig/network/ifroute-*

TCP/IP 封包的靜態路由在此決定。您可以將各種系統任務所需的所有靜態路由都輸入 `/etc/sysconfig/network/routes` 檔案，包括主機的路由、透過閘道前往主機的路由，以及網路的路由。對於需要個別路由的介面，請定義額外的組態檔案：`/etc/sysconfig/network/ifroute-*`。以介面的名稱取代 `*`。在路由組態檔中的項目看起來就像這樣：

# Destination	Dummy/Gateway	Netmask	Device
#			
127.0.0.0	0.0.0.0	255.255.255.0	lo
204.127.235.0	0.0.0.0	255.255.255.0	eth0
default	204.127.235.41	0.0.0.0	eth0
207.68.156.51	207.68.145.45	255.255.255.255	eth1
192.168.0.0	207.68.156.51	255.255.0.0	eth1

路由的目的地是在第一個資料欄。這個資料欄可能包含網路或主機的 IP 位址，這是指「*可到達的*」名稱伺服器、完整合格的網路或主機名稱。

第二個資料欄包含預設的閘道或是可以存取主機或網路的閘道。第三個資料欄包含在閘道後面的網路或主機的網路遮罩。例如，遮罩為 255.255.255.255，供在閘道後面的主機使用。

第四欄只與連接至本地主機的網路相關，例如迴路、乙太網路、ISDN、PPP 以及虛擬設備。必須在這裏輸入設備名稱。

第五欄(可選)可指定路由的類型。不需要的欄位必須包含 - 減號，以確保解析程式可正確解譯指令。如需詳細資訊，請參閱 `routes(5) man` 頁面。

現在，IPv4 和 IPv6 的統一格式如下所示：

```
prefix/lengthgateway - [interface]
```

相應地，所謂的相容性格式則為：

```
prefixgatewaylength [interface]
```

對於 IPv4，您仍然可以使用含網路遮罩的舊格式：

```
ipv4-networkgatewayipv4-netmask [interface]
```

下列範例作用相同：

2001:db8:abba:cafe::/64	2001:db8:abba:cafe::dead	-	eth0
208.77.188.0/24	208.77.188.166	-	eth0
2001:db8:abba:cafe::	2001:db8:abba:cafe::dead	64	eth0
208.77.188.0	208.77.188.166	24	eth0
208.77.188.0	208.77.188.166	255.255.255.0	eth0

21.6.1.4 /etc/resolv.conf

主機所屬的網域指定於此檔案(關鍵字 `search`)；另外也會列出要存取的名稱伺服器位址的狀態(關鍵字 `nameserver`)。可以在檔案中指定多個網域名稱。解析不完整的名稱時，會嘗試附加個別 `search` 項目產生一個名稱。可以在多行中指定多個伺服器名稱，每個名稱均以 `nameserver` 開頭。備註前面標有 `#` 符號。範例 21.5 「`/etc/resolv.conf`」 [285頁] 顯示了 `/etc/resolv.conf` 的格式。

不過，您不可手動編輯 `/etc/resolv.conf`。它是由 `netconfig` 程序檔產生的。若不想使用 `YaST` 定義靜態 DNS 組態，請在 `/etc/sysconfig/network/config` 檔案中手動編輯適當的變數：

`NETCONFIG_DNS_STATIC_SEARCHLIST`
用於主機名稱查詢的 DNS 網域名稱清單

`NETCONFIG_DNS_STATIC_SERVERS`
用於主機名稱查詢的名稱伺服器 IP 位址清單

`NETCONFIG_DNS_FORWARDER`
定義必須設定的 DNS 轉遞者的名稱

若要使用 `netconfig` 停用 DNS 組態，請設定 `NETCONFIG_DNS_POLICY=''`。如需 `netconfig` 的詳細資訊，請參閱 `man 8 netconfig`。

範例 21.5 `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

21.6.1.5 /sbin/netconfig

`netconfig` 是一個模組化工具，用於管理其他網路組態設定。它根據預先定義的規則，將靜態定義的設定與自動組態機制 (如 DHCP 或 PPP) 提供的設定進行合併。透過呼叫負責修改組態檔案和重新啟動服務或類似動作的 `netconfig` 模組，將必要的變更套用至系統。

`netconfig` 可以辨識三個主要動作。DHCP 或 PPP 等精靈使用 `netconfig modify` 與 `netconfig remove` 指令提供或移除 `netconfig` 的設定。使用者僅可使用 `netconfig update` 指令：

`modify`

`netconfig modify` 指令會修改目前的介面和服務特定的動態設定，並更新網路組態。`Netconfig` 會從標準輸入或從 `--lease-file` 檔案名稱選項指定的檔案讀取設定，並將它們儲存於內部，直到系統重新開機 (或執行下一個修改或移除動作) 為止。系統會覆寫同一個介面與服務組合的現有設定。介面由 `-i` 介面名稱參數來指定。服務由 `-s` 服務名稱參數來指定。

`remove`

`netconfig remove` 指令會移除修改動作為指定介面和服務組合提供的動態設定，並更新網路組態。介面由 `-i` 介面名稱參數來指定。服務由 `-s` 服務名稱參數來指定。

`update`

`netconfig update` 指令會使用目前的設定更新網路組態。當規則或靜態組態變更時可以使用此指令。如果只想更新指定的服務 (dns、nis 或 ntp)，請使用 `-m` 模組類型參數。

`netconfig` 規則和靜態組態設定可透過手動方式定義，或使用 YaST 在 `/etc/sysconfig/network/config` 檔案中定義。自動組態工具 (如 DHCP 或 PPP) 提供的動態組態設定經由這些工具透過 `netconfig modify` 和 `netconfig remove` 動作直接傳送。`NetworkManager` 也可以使用 `netconfig modify` 與 `netconfig remove` 動作。`NetworkManager` 啟用時，`netconfig` (在 `auto` 規則模式中) 只會使用 `NetworkManager` 設定，忽略使用傳統 `ifup` 方法設定的任何其他介面中的設定。如果 `NetworkManager` 未提供任何設定，則使用靜態設定做為備用設定。系統不支援同時使用 `NetworkManager` 與傳統 `ifup` 方法。

如需 `netconfig` 的詳細資訊，請參閱 `man 8 netconfig`。

21.6.1.6 /etc/hosts

在此檔中(請參閱範例 21.6 「/etc/hosts」 [287頁]), IP 位址是指定給主機名稱。如果沒有執行任何名稱伺服器, 將使用此 IP 連接設定的所有主機將列示於此。對於每個主機, 分別在檔案中輸入一行包含 IP 位址、完全合法的主機名稱及主機名稱的項目。IP 位址必須在行的開頭, 然後以空格和定位點分隔這些項目。註解的前面永遠是 # 符號。

範例 21.6 /etc/hosts

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

21.6.1.7 /etc/networks

在此檔中, 網路名稱會轉換為網路位址。格式與 hosts 檔案格式相似, 但是網路名稱在位址前。請參閱範例 21.7 「/etc/networks」 [287頁]。

範例 21.7 /etc/networks

```
loopback      127.0.0.0
localnet      192.168.0.0
```

21.6.1.8 /etc/host.conf

名稱解析, 即透過解析程式庫 (Resolver Library) 翻譯主機及網路名稱, 是由此檔案控制的。該檔案僅用於與 libc4 或 libc5 連結的程式。對於目前的 glibc 程式, 請參閱 /etc/nsswitch.conf 中的設定。每個參數必須永遠是獨立一行。註解的前面是 # 符號。表格 21.6 「/etc/host.conf 的參數」 [287頁] 顯示出可用的參數。/etc/host.conf 範例是顯示在 範例 21.8 「/etc/host.conf」 [288頁]。

表格 21.6 /etc/host.conf 的參數

order hosts, bind	指定針對名稱解析存取服務的順序。可用的引數有 (以空格或逗號分隔):
	hosts: 搜尋 /etc/hosts 檔案

	<i>bind</i> : 存取名稱伺服器
	<i>nis</i> : 使用 NIS
<i>multi on/off</i>	定義在 <code>/etc/hosts</code> 中所輸入的主機是否可以有多個 IP 位址。
<i>nospoof on spoofalert on/off</i>	這些參數會影響名稱伺服器 <i>spoofing</i> ，但並不會對網路組態產生任何影響。
<i>trim domainname</i>	指定的網域名稱在主機名稱解析後會與主機名稱分隔(只要主機名稱包括網域名稱)。只有在本地網域分隔出來的名稱位於 <code>/etc/hosts</code> 檔案，但仍然使用附加的網域名稱進行辨識時，這個選項才有用。

範例 21.8 `/etc/host.conf`

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

21.6.1.9 `/etc/nsswitch.conf`

GNU C Library 2.0 的介紹隨附於名稱服務切換(NSS, Name Service Switch)的介紹。詳細資訊請參閱 `nsswitch.conf(5)` `man` 頁面和 *GNU C Library 參考手冊*。

查詢的順序定義於檔案 `/etc/nsswitch.conf`。`nsswitch.conf` 範例是顯示在範例 21.9「`/etc/nsswitch.conf`」[288頁]。備註前面標有 `#` 符號。在此範例中，`hosts` 資料庫下的項目表示要求是透過 DNS 傳送到 `/etc/hosts` (files) (請參閱第 24 章「網域名稱系統」[315頁])。

範例 21.9 `/etc/nsswitch.conf`

```
passwd:      compat
group:       compat

hosts:       files dns
```

```
networks:    files dns

services:    db files
protocols:   db files
rpc:         files
ethers:      files
netmasks:   files
netgroup:    files nis
publickey:   files

bootparams:  files
automount:   files nis
aliases:     files nis
shadow:      compat
```

NSS 上可用的「資料庫」列示於 表格 21.7 「透過 /etc/nsswitch.conf 的可用資料庫」 [289頁]。NSS 資料庫的組態選項將列於表格 21.8 「NSS 「資料庫」的組態選項」 [290頁]。

表格 21.7 透過 /etc/nsswitch.conf 的可用資料庫

aliases	sendmail 所執行的郵件別名；請參閱 man 5 aliases。
ethers	乙太網路位址。
netmasks	網路及其子網路遮罩的清單。當您使用子網路時才需要。
group	適用於 getgrent 所使用的使用者群組。請參閱 group 的 man 頁面。
hosts	gethostbyname 及類似功能所使用的主機名稱與 IP 位址。
netgroup	在網路中有效的主機與使用者清單，以利控制存取權限，請參閱 netgroup(5) man 頁面。
networks	getnetent 所使用的網路名稱與位址。

publickey	NFS 及 NIS+ 使用之 Secure_RPC 的公開金鑰和私密金鑰。
passwd	getpwent 所使用的使用者密碼；請參閱 passwd(5) man 頁面。
protocols	getprotoen 所使用的網路通訊協定；請參閱 protocols(5) man 頁面。
rpc	getrpcbyname 及類似功能所使用的遠端程序呼叫名稱與位址。
services	getservent 使用的網路服務。
shadow	getspnam 所使用的使用者遮蔽密碼；請參閱 shadow(5) man 頁面。

表格 21.8 NSS 「資料庫」的組態選項

files	直接存取檔案，例如 /etc/aliases
db	透過資料庫存取
nis、nisplus	NIS，請參閱第 3 章「 <i>Using NIS</i> 」(↑ <i>Security Guide</i>)
dns	只能做為 hosts 與 networks 的延伸
compat	只能做為 passwd、shadow 與 group 的延伸

21.6.1.10 /etc/nscd.conf

此檔案用來設定 `nscd` (名稱服務快取精靈)。請參閱 `nscd(8)` 與 `nscd.conf(5)` `man` 頁面。依預設，`passwd` 與 `groups` 的系統項目是由 `nscd` 快取。這對於目錄服務 (如 `NIS` 和 `LDAP`) 的效能而言是很重要的，否則每次存取名稱或群組時都需要使用網路連線。預設是不會快取 `hosts`，因為 `nscd` 快取主機的機制會造成本地系統無法信任轉寄以及反向查詢檢查。不要要求 `nscd` 快取名稱，而是設定快取 `DNS` 伺服器。

如果啟用 `passwd` 的快取，通常需要 15 秒，才能辨識新增的本地使用者。使用指令 `rcnscd restart` 重新啟動 `nscd`，縮短這段等待時間。

21.6.1.11 /etc/HOSTNAME

此檔案包含附加了網域名稱的完全合格的主機名稱。機器開機時數個程序檔會讀取該檔案。它只能包含一行，其中設定了主機名稱。

21.6.2 測試與組態

將組態寫入您的組態檔案之前，可先進行測試。若要設定測試組態，請使用 `ip` 指令。若要測試連接，請使用 `ping` 指令。同時也可使用較舊的組態工具，如 `ifconfig` 和 `route`。

`ip`、`ifconfig` 和 `route` 指令會直接變更網路組態，不會將其儲存到組態檔案中。除非您將組態輸入正確的組態檔案，否則重新開機之後網路組態的變更就會遺失。

21.6.2.1 使用 `ip` 設定網路介面

`ip` 是一項可顯示及設定網路設備、路由、規則路由和通道的工具。

`ip` 是非常複雜的工具。其一般語法是 `ip options object command`。您可使用下列物件：

`link`

此物件代表網路設備。

address

此物件代表設備的 IP 位址。

neighbor

此物件代表 ARP 或 NDISC 快取項目。

route

此物件代表路由表格項目。

rule

此物件代表路由原則資料庫中的規則。

maddress

此物件代表多重廣播位址。

mroute

此物件代表多重廣播路由快取項目。

tunnel

此物件表示 IP 上的通道。

若未提供指令，會使用預設指令 (通常是 `list`)。

您可使用 `ip link set device_name command` 指令變更設備狀態。例如，若要停用設備 `eth0`，請輸入 `ip link set eth0 down`。若要重新啟用，請使用 `ip link set eth0 up`。

啟用設備之後，就可加以設定。若要設定 IP 位址，請使用 `ip addr add ip_address + dev device_name`。例如，若要將介面 `eth0` 的 IP 位址以標準廣播 (選項 `brd`) 設定為 `192.168.12.154/30`，請輸入 `ip addr add 192.168.12.154/30 brd + dev eth0`。

若要具備作用中連接，必須設定預設閘道。若要為您的系統設定閘道，請輸入 `ip route add 閘道 IP 位址`。若要轉換某個 IP 位址，請使用 `nat:ip route add nat ip_address via other_ip_address`。

若要顯示所有設備，請使用 `ip link ls`。若只希望顯示運作中介面，請使用 `ip link ls up`。若要列印設備的介面統計值，請輸入 `ip -s link ls device_name`。若要檢是您設備的位址，請輸入 `ip addr`。在 `ip addr` 的輸

出中同時也可找到您設備的 MAC 位址相關資訊。若要顯示所有路由，請使用 `ip route show`。

如需有關使用 `ip` 的詳細資訊，請輸入 `iphelp` 或參閱 `ip(8) man` 頁面。`help` 選項也適用於所有 `ip` 子指令。例如，如果您需要 `ip addr` 的說明，請輸入 `ip addr help`。 `/usr/share/doc/packages/iproute2/ip-cref.pdf` 中提供了有關 `ip` 的說明。

21.6.2.2 以 ping 測試連接

`ping` 指令是測試 TCP/IP 連接運作的標準工具。其使用 ICMP 通訊協定，將小型資料封包 `ECHO_REQUEST` 傳送至目的地主機，要求立即回應。如果有作用，`ping` 會顯示訊息，指示網路連結基本上是正常的。

`ping` 不僅會測試兩台電腦之間能否連接，還會提供一些關於連線品質的基本資訊。您可在範例 21.10 「指令 `ping` 的輸出」 [293頁] 中看到 `ping` 輸出的一些範例。倒數第二行包含送出的封包數、封包遺失率以及執行 `ping` 總共花費的時間等資訊。

對於目的地，可使用主機名稱或 IP 位址，例如 `ping example.com` 或 `ping 192.168.3.100`。程式會持續傳送封包，直到您按下 `Ctrl + C` 為止。

若您只需要檢查連接功能性，您可以 `-c` 選項限定封包數目。例如，若要將 `ping` 限制於三個封包，請輸入 `ping -c 3 example.com`。

範例 21.10 指令 `ping` 的輸出

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

兩個封包之間的預設間隔為一秒。若要變更間隔，可以使用 `ping` 提供的選項 `-i`。例如，若要將 `ping` 間隔增到十秒一次，請輸入 `ping -i 10 example.com`。

在具備多網路設備的系統中，透過特定介面位址傳送 ping 非常實用。若要實現此功能，請使用 `-I` 選項並提供所選設備的名稱，例如 `ping -I wlan1 example.com`。

如需使用 ping 的選項與詳細資訊，請輸入 `ping -h` 或參閱 `ping (8) man` 頁面。

提示：Ping IPv6 位址

對於 IPv6 位址，請使用 `ping6` 指令。請注意，若要 ping 連結-本機位址，必須使用 `-I` 指定介面。如果該位址可透過 `eth1` 存取，則可以使用以下指令實現目的：

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

21.6.2.3 以 ifconfig 設定網路

`ifconfig` 是一項網路組態工具。

注意：ifconfig 和 ip

`ifconfig` 工具已過時。請改用 `ip`。與 `ip` 相反，`ifconfig` 只能用於介面組態。它將介面名稱限制為 9 個字元。

無疑，`ifconfig` 顯示的是目前作用中介面的狀態。如您在範例 21.11 「`ifconfig` 指令的輸出」[294頁]中所見，`ifconfig` 的輸出排列整齊並且內容詳盡。輸出的第一行亦包含您設備的 MAC 位址 (HWaddr 的值) 等相關資訊。

範例 21.11 ifconfig 指令的輸出

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```



```

RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1    Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
        inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
        inet6 addr: fe80::20e:2eff:fe52:3b1d/64  Scope:Link
        UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
        TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 MB)

```

如需有關使用 `ifconfig` 的選項與詳細資訊，請輸入 `ifconfig -h` 或參閱 `ifconfig (8) man` 頁面。

21.6.2.4 使用 `route` 設定路由

`route` 是操作 IP 路由表格的程式。您可使用此指令檢視您的路由組態，以及新增或移除路由。

注意：`route` 與 `ip`

`route` 這個程式已過時。請改用 `ip`。

若您需要快速又易於理解的路由組態資訊以判別路由問題，`route` 是特別實用的工具。若要檢視您目前的路由組態，請以 `root` 身分輸入 `route -n`。

範例 21.12 `route -n` 指令的輸出

```

route -n
Kernel IP routing table

```

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.20.0.0	*	255.255.248.0	U	0	0	0	eth0
link-local	*	255.255.0.0	U	0	0	0	eth0
loopback	*	255.0.0.0	U	0	0	0	lo
default	styx.exam.com	0.0.0.0	UG	0	0	0	eth0

如需使用 `route` 的選項與詳細資訊，請輸入 `route -h` 或參閱 `route (8) man` 頁面。

21.6.3 啟動程序檔

除了上述的組態檔之外，還有在機器開機時載入網路程式的各種程序檔。只要系統切換到其中一個 *multiuser runlevels*，就會啟動這些程序檔。在 表格 21.9 「網路程式的一些啟動程序檔」 [296頁] 中提供了一些程序檔的說明。

表格 21.9 網路程式的一些啟動程序檔

<code>/etc/init.d/network</code>	此程序檔會處理網路介面的組態。如果未啟動網路服務，則不會實作任何網路介面。
<code>/etc/init.d/xinetd</code>	啟動 <code>xinetd</code> 。 <code>xinetd</code> 可以用來讓伺服器服務能夠在系統上使用。例如，只要開啟 FTP 連接，它即可啟動 <code>vsftpd</code> 。
<code>/etc/init.d/rpcbind</code>	啟動可將 RPC 程式號碼轉換為通用位址的 <code>rpcbind</code> 公用程式。NFS 伺服器等 RPC 服務需要用到。
<code>/etc/init.d/nfsserver</code>	啟動 NFS 伺服器。
<code>/etc/init.d/postfix</code>	控制後置程序。
<code>/etc/init.d/ypserv</code>	啟動 NIS 伺服器。
<code>/etc/init.d/ypbind</code>	啟動 NIS 用戶端。

21.7 設定 Bonding 設備

對於某些系統而言，實作的網路連線除了需要符合一般乙太網路設備的標準資料安全性或可用性要求之外，還需要符合其他要求。在這些情況下，數個乙太網路設備可以結集成單個 Bonding 設備。

bonding 設備的組態是透過 bonding 模組選項來設定，而其行為主要受 Bonding 設備的模式影響。該模式預設為 mode=active-backup，這表示如果使用中的從屬設備失敗，另一個從屬設備將變成使用中狀態。

提示：Bonding 和 Xen

Bonding 設備僅適用於具有多個實際網路卡的機器。在大多數組態中，這表示您只應該在 Domain0 中使用 Bonding 組態。此外，只有在您將多個網路卡指定給 VM Guest 系統的情況下，才可以使用此方式在 VM Guest 中設定 Bond。

若要設定 bonding 設備，請執行以下程序：

- 1 執行「YaST」>「網路設備」>「網路設定」。
- 2 使用「新增」，然後將「設備類型」變更為「Bond」。按「下一步」繼續。

The screenshot shows the 'Network Card Settings' (網路卡設定) window in YaST. The 'Bonding' (Bonding) tab is selected. The 'Device Type' (裝置類型) is set to 'Bond'. The 'Bond Name' (組態名稱) is 'bond0'. The 'Dynamic IP' (動態位址) option is selected, with 'DHCP' (DHCP) as the method and 'DHCP version 4 and 6' (DHCP 版本 4 與 6) as the version. The 'IP Address' (IP 位址), 'Subnet Mask' (子網路遮罩), and 'Gateway' (主機名稱) fields are empty. Below these fields is a table for 'Other IP addresses' (其他位址) with columns for 'Name' (別名), 'IP Address' (IP 位址), and 'Network Device' (網路裝置). At the bottom, there are buttons for 'Add' (新增), 'Delete' (刪除), 'Apply' (套用), 'Cancel' (取消), and 'Next' (下一步).

- 3 選取為 bonding 設備指定 IP 位址的方法。有三種方法可供您選擇：
- 無 IP 位址
 - 動態位址 (透過 DHCP 或 Zeroconf)

- 靜態指定的 IP 位址

請使用適合您環境的方法。

- 4 在「*Bond* 從屬」索引標籤中，透過啟用相關的核取方塊來選取應包含在 Bond 中的乙太網路設備。
- 5 編輯「*Bond* 驅動程式選項」。可用於設定的模式顯示如下：

- balance-rr
- active-backup
- balance-xor
- 廣播
- 802.3ad
- balance-tlb
- balance-alb

- 6 確認參數 `miimon=100` 已新增至「*Bond* 驅動程式選項」。若沒有此參數，就無法定期檢查資料的完整性。

- 7 按「下一步」，然後按一下「確定」離開 YaST，以建立設備。

所有模式以及其他更多選項的詳細說明請見「*Linux* 乙太網路 *Bonding* 驅動程式 *HOWTO*」(安裝套件 `kernel-source` 之後可在 `/usr/src/linux/Documentation/networking/bonding.txt` 中找到)。

21.7.1 Bonding 從屬的熱插拔

在特定網路環境 (例如高可用性) 中，有時候您需要將 Bonding 從屬介面取代成其他介面。原因可能在於網路設備不斷發生故障。解決方案是設定 Bonding 從屬的熱插拔。

請如一般方式設定 Bond (根據 `man 5 ifcfg-bonding`)，例如：

```
ifcfg-bond0
    STARTMODE='auto' # or 'onboot'
    BOOTPROTO='static'
    IPADDR='192.168.0.1/24'
    BONDING_MASTER='yes'
    BONDING_SLAVE_0='eth0'
    BONDING_SLAVE_1='eth1'
    BONDING_MODULE_OPTS='mode=active-backup miimon=100'
```

但使用 `STARTMODE=hotplug` 和 `BOOTPROTO=none` 指定從屬：

```
ifcfg-eth0
    STARTMODE='hotplug'
    BOOTPROTO='none'

ifcfg-eth1
    STARTMODE='hotplug'
    BOOTPROTO='none'
```

`BOOTPROTO=none` 會使用 `ethtool` 選項 (若提供)，但不會使用 `ifup eth0` 設定連結。這是因為從屬介面是由 **Bond** 主要設備所控制的。

`STARTMODE=hotplug` 會導致從屬介面只要可使用便會自動加入 **Bond**。

必須變更 `/etc/udev/rules.d/70-persistent-net.rules` 中的 `udev` 規則才能按匯流排 ID (`udev` `KERNELS` 關鍵字等於 `hwinfo --netcard` 中所示的「**SysFS BusID**」) 比對設備 (而不是按 **MAC** 位址)，從而允許更換有故障的硬體 (網路卡位於相同的插槽中但具有不同的 **MAC**)，以及避免在 **Bond** 變更其所有從屬的 **MAC** 位址時引起混淆。

例如：

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
KERNELS=="0000:00:19:0", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"
```

開機時，`/etc/init.d/network` 不會等待熱插拔從屬，但會等待 **Bond** 就緒 (至少需要一個可用的從屬)。當從系統移除其中一個從屬介面 (從 **NIC** 驅動程式解除結合、**NIC** 驅動程式的 `rmmmod` 或實際 **PCI** 熱插拔移除) 時，核心會自動將它從 **Bond** 中移除。當將新卡新增至系統時 (更換插槽中的硬體)，`udev` 會使用匯流排型永久命名規則將它重新命名為從屬的名稱，然後為它呼叫 `ifup`。`ifup` 呼叫會自動將它加入 **Bond**。

21.8 smpppd 做為撥號助理

部份家庭使用者沒有連接到網際網路的專線。而是使用撥號連接。視撥號方法 (ISDN 或 DSL) 而定，連接是由 `ipppd` 或 `pppd` 來控制。基本上，連接所需做的事就是正確地啟動這些程式。

如果您有單一速率的連接，不會產生撥號連接的其他成本，請直接啟動個別的精靈。使用桌面 Applet 或指令行介面控制撥號連接。如果網際網路閘道不是您所使用的主機，您可能需要透過網路主機來控制撥號連接。

這種情況下將需要使用 `smpppd` (SUSE Meta PPP 精靈)。它會為輔助程式提供一致的介面並以兩個方向運作。首先，它會撰寫所需的 `pppd` 或 `ipppd` 程式，然後控制其撥號內容。其次，它會提供各個提供者給使用者程式，並傳輸關於連接目前狀態的資訊。因為 `smpppd` 也可以透過網路控制，所以它適合從私人子網路的工作站中，控制連至網際網路的撥號連接。

21.8.1 設定 smpppd

`smpppd` 所提供的連接會自動由 YaST 設定。實際的撥號程式 `KInternet` 與 `cinternet` 也是預先設定的。只有在設定 `smpppd` 的遠端控制等其他功能時才需要進行手動設定。

`smpppd` 的組態檔為 `/etc/smpppd.conf`。根據預設，它不會啟用遠端控制。此組態檔最重要的選項為：

`open-inet-socket = yes/no`

若要透過網路控制 `smpppd`，請將此選項設定為 `yes`。`smpppd` 會在連接埠 3185 上監聽。如果此參數設為 `yes`，則必須對 `bind-address`、`host-range` 以及 `password` 參數進行相應的設定。

`bind-address = ip address`

如果主機具有數個 IP 位址，請使用此參數以決定那個 IP 位址 `smpppd` 應該接受連接。預設為監聽所有位址。

`host-range = min ipmax ip`

`host-range` 參數會定義網路範圍。在此範圍中的 IP 位址之主機擁有 `smpppd` 的存取權。所有不在此範圍中的主機都將拒絕存取。

`password = password`

透過指定密碼，將用戶端限制為授權的主機。因為這是純文字的密碼，您不應該高估它所提供的安全性。如果沒有指定密碼，則所有的用戶端都將允許存取 `smpppd`。

`slp-register = yes/no`

使用此參數，`smpppd` 服務就可以透過 SLP 在網路中宣告。

有關 `smpppd` 的詳細資訊，請參閱 `smpppd(8)` 和 `smpppd.conf(5)` man 頁面。

21.8.2 設定 `cinternet` 以供遠端使用

`cinternet` 可用於控制本地或遠端 `smpppd`。`cinternet` 是對應於圖形 `KInternet` 的指令行工具。若要準備這些公用程式以供遠端 `smpppd` 使用，請以手動方式或使用 `cinternet` 編輯 `/etc/smpppd-c.conf` 組態檔案。此檔案只使用四個選項：

`sites = list of sites`

站台清單是指前端搜尋 `smpppd` 的站台。這些前端將會依這裏所指定的順序來測試選項。`local` 可命令建立與本地 `smpppd` 的連線。`gateway` 指向閘道上的 `smpppd`。`config-file` 指示與指定的 `smpppd` (由 `/etc/smpppd-c.conf` 中的 `server` 與 `port` 選項指定) 建立連線。`slp` 可命令前端連接至透過 SLP 找到的 `smpppd`。

`server = server`

執行 `smpppd` 的主機。

`port = port`

執行 `smpppd` 的連接埠。

`password = password`

為 `smpppd` 選取的密碼。

若 `smpppd` 正在使用，則嘗試加以存取。例如，使用 `cinternet --verbose --interface-list`。如果在此遇到問題，請參閱 `smpppd-c.conf(5)` 與 `cinternet(8)` man 頁面。

網路中的 SLP 服務

服務位置通訊協定 (SLP) 是開發用來簡化區域網路內的網路用戶端組態。若要設定網路用戶端 (包含所有必要的服務)，一般而言管理員需要對於網路中可用的伺服器有詳細的瞭解。SLP 可讓區域網路中的所有用戶端，都知道選定服務的可用性。支援 SLP 的應用程式可以使用散佈的資訊並可自動設定。

SUSE® Linux Enterprise Server 支援使用 SLP 所提供的安裝來源進行安裝，並包含許多具有 SLP 整合支援的系統服務。YaST 和 Konqueror 都包含 SLP 適當的前端介面。您可以使用 SLP 以提供主要的功能給網路上的用戶端，例如系統上的安裝伺服器、檔案伺服器或是列印伺服器。

重要：SUSE Linux Enterprise Server 中的 SLP 支援

提供 SLP 支援的服務包含 cupsd、rsyncd、ypserv、openldap2、ksysguardd、saned、kdm、vnc、login、smpppd、rpasswd、postfix 以及 sshd (透過 fish)。

22.1 安裝

預設會安裝所有必需的套件。但是，如果要透過 SLP 提供服務，請檢查是否已安裝 openslp-server 套件。

22.2 啟用 SLP

您系統必須執行 `slpd`，才能提供 SLP 服務。如果機器僅做為用戶端執行並且不提供服務，則無需執行 `slpd`。就像大部分在 SUSE Linux Enterprise Server 中的系統服務一樣，`slpd` 精靈是利用獨立的 `init` 程序檔來控制的。安裝完成後，依預設此精靈將處於非啟動狀態。若要暫時啟動，請以 `root` 身份執行 `rcslpd start` 或執行 `rcslpd stop` 將其停止。請以 `restart` 或 `status` 執行重新啟動或狀態檢查。若 `slpd` 在開機後應始終處於啟用狀態，請在「YaST」>「系統服務 (執行層級)」中啟用 `slpd`，或以 `root` 身份執行 `insserv slpd` 指令。

22.3 SUSE Linux Enterprise Server 中的 SLP 前端

若要在您的網路中尋找透過 SLP 提供的服務，請使用 SLP 前端，例如 `slptool` (`openslp` 套件) 或 YaST：

`slptool`

`slptool` 是一個指令行程式，可以宣告網路中的 SLP 查詢或宣告專用的服務。`slptool --help` 會列出所有可用的選項與功能。例如，若要在目前網路中尋找所有自我宣告的時間伺服器，請執行以下指令：

```
slptool findsrvs service:ntp
```

YaST

YaST 還提供了一個 SLP 瀏覽器。不過，在 YaST 控制中心內無法使用此瀏覽器。若要啟動此瀏覽器，請以 `root` 使用者身分執行 `yast2 slp`。按一下左側的「服務類型」，以獲取有關服務的詳細資訊。

22.4 透過 SLP 安裝

如果您的網路中提供了 SUSE Linux Enterprise Server 安裝媒體的安裝伺服器，就可以使用 SLP 註冊和提供安裝媒體。如需詳細資料，請參閱第 14.2 節「安裝保存安裝來源的伺服器」(第 14 章「遠端安裝」, ↑部署指南)。如果已選取 SLP

安裝，linuxrc 會在系統從選取的開機媒體開機後啟動 SLP 查詢，並顯示所找到的來源。

22.5 透過 SLP 提供服務

許多 SUSE Linux Enterprise Server 中的應用程式透過使用 libslp 程式庫已經具有整合的 SLP 支援。如果尚未使用 SLP 支援來編譯服務，請使用下列方式之一來透過 SLP 進行編譯：

使用 /etc/slp.reg.d 的靜態註冊

針對每個新的服務建立個別的註冊檔。以下是註冊掃描器服務的範例：

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

在此檔案中最重要的一行為 *service URL*，它是以 `service:` 開始。這包含服務類型 (`scanner.sane`) 以及位址 (可在其中找到伺服器可用的服務)。`$HOSTNAME` 會以完整的主機名稱自動取代。接著可以找到相關服務的 TCP 埠名稱，它們之間是以冒號分隔。然後輸入服務應該出現的語言以及註冊期間的秒數。這些都應該使用逗號與服務 URL 分隔。在 0 與 65535 之間設定註冊期間的值。0 會防止註冊。65535 會移除所有的限制。

註冊檔另外還包含 `watch-port-tcp` 與 `description` 兩個變數。`watch-port-tcp` 將 SLP 服務宣告連結至由 `slpd` 檢查到的服務狀態，即相關服務是否啟用。第二個變數是對顯示在適當瀏覽器中的服務，提供更為精確的描述。

提示：YaST 以及 SLP

當您在模組對話方塊中啟用 SLP 時，一些由 YaST 所仲介的服務 (例如安裝伺服器或 YOU 伺服器) 會自動執行此註冊。YaST 接著就會為這些服務建立註冊檔。

使用 `/etc/slp.reg` 的靜態註冊

此方法與使用 `/etc/slp.reg.d` 的程序的唯一區別在於所有服務都會在中心檔案內分組。

使用 `slptool` 的動態註冊

如果要動態註冊服務而不使用組態檔案，請使用 `slptool` 指令行公用程式。這一公用程式還可用於取消註冊現有服務提供而無需重新啟動 `slpd`。

22.6 如需更多資訊

RFC 2608、2609、2610

RFC 2608 一般會處理 SLP 的定義。RFC 2609 會處理更加詳細的服務 URL 語法，而 RFC 2610 則會透過 SLP 處理 DHCP。

<http://www.openslp.org>

OpenSLP 計劃的首頁。

`/usr/share/doc/packages/openslp`

此目錄包含 `openslp-server` 套件隨附的 SLP 文件，包括 `README.SuSE` (含有 SUSE Linux Enterprise Server 詳細資料)、RFC 檔案以及兩個介紹性的 HTML 文件。想要使用 SLP 功能的程式設計師可以在 `openslp-devel` 套件隨附的《*程式設計師指南*》中找到詳細資訊。

使用 NTP 進行時間同步化

NTP (網路時間協定) 機制是一種協定，用於同步化網路上的系統時間。首先，機器可以從提供可靠時間來源的伺服器取得時間。其次，機器本身在網路中可以做為其他電腦的時間來源。這個目標是雙重的，即維護絕對正確的時間，並同步化網路內所有機器的系統時間。

維護精準的系統時間對於許多情況都非重要。內建的硬體時鐘通常無法符合資料庫或叢集等應用程式的要求。手動校正系統時間有可能會造成嚴重的問題，因為，例如時間倒退將可能造成重要應用程式無法正常運作。在網路中，通常需要同步所有機器中的系統時間，而手動調整時間的做法並不可取。NTP 提供了一種用於解決這些問題的機制。NTP 服務會透過網路中可靠的時間伺服器來持續調整系統時間。它可以進一步管理本地參考的時鐘，例如收音機控制的時鐘。

23.1 使用 YaST 設定 NTP 用戶端

ntp 套件隨附的 NTP 精靈 (ntpd) 預先設定為使用本地電腦時鐘做為時間參考。不過，硬體時鐘僅供在沒有更精確的時間來源時備用。YaST 使用了 NTP 用戶端的組態。

23.1.1 基本組態

YaST NTP 用戶端組態 (「網路服務」 > 「NTP 組態」) 包含幾個索引標籤。在「一般設定」索引標籤上設定 ntpd 的啟動模式和要查詢的伺服器。

「僅手動」

如果要手動啟動 `ntpd` 精靈，請選取「僅手動」。

「現在和開機時」

選取「現在和開機時」，以便在系統開機時自動啟動 `ntpd`。強烈建議您使用此設定。然後依第 23.1.2 節「變更基本組態」[308頁] 中所述設定伺服器。

23.1.2 變更基本組態

用戶端要查詢的伺服器以及其他時間來源會列在「一般設定」索引標籤的下半部。修改清單時，可依需要使用「新增」、「編輯」以及「刪除」。「顯示記錄」可用來檢視用戶端的記錄檔。

按一下「新增」以新增時間資訊的新來源。在下列對話方塊中，選取進行時間同步化的來源類型。可用的選項如下：

圖形 23.1 *YaST : NTP 伺服器*



伺服器

在「選取」下拉式選單 (請參閱圖形 23.1 「YaST : NTP 伺服器」[308頁]) 中，指定是使用區域網路中的時間伺服器 (「本地 *NTP* 伺服器」)，還是使用可以處理您時區的網際網路時間伺服器 (「公用 *NTP* 伺服器」) 來設定時

間同步化。若需本地時間伺服器，請按一下「查詢」，開始 SLP 查詢，在網路中尋找可用的時間伺服器。從搜尋結果清單中選取最合適的時間伺服器，並按一下「確定」，結束對話方塊。若需公用時間伺服器，請選取您的國家(時區)並從「公用 NTP 伺服器」下的清單選取適當的伺服器，然後按一下「確定」，結束對話方塊。在主對話方塊中，使用「測試」來測試所選取伺服器的可用性。「選項」可讓您為 ntpd 指定其他選項。

使用「存取控制選項」，您可以限制遠端電腦可以使用電腦上執行的精靈來執行的動作。當核取「安全性設定」索引標籤(請參閱圖形 23.2「進階 NTP 組態：安全性設定」[310頁])中的「將 NTP 服務限制為僅限已設定的伺服器」後，此欄位才處於啟用狀態。這些選項對應於 /etc/ntp.conf 中的 restrict 子句。例如，nomodify notrap noquery 不允許伺服器修改電腦的 NTP 設定，並且不允許使用 NTP 精靈的設陷設備(遠端事件登入功能)。建議對超出您控制範圍(例如在網際網路上)的伺服器使用這些限制。

如需詳細資訊，請參閱 /usr/share/doc/packages/ntp-doc(ntp-doc 套件的一部份)。

點

點(peer)，是指一台建立了對稱關係的機器：它可同時做為時間伺服器與用戶端。若要在相同的網路中使用點而非伺服器，請輸入系統的位址。其餘的對話方塊與「伺服器」對話方塊相同。

收音機時鐘

若要在系統中使用收音機時鐘來進行時間同步化，請在此對話方塊中輸入時鐘類型、單位編號、設備名稱以及其他選項。按一下「驅動程式校正」，即可微調驅動程式。/usr/share/doc/packages/ntp-doc/refclock.html 中提供了關於本地無線電時鐘作業的詳細資訊。

外寄廣播

時間資訊與查詢也可以透過網路中的廣播傳輸。請在此對話方塊中輸入廣播所應傳送至的位址。除非您已經有類似收音機控制時鐘的可靠時間來源，否則請勿啟用廣播。

內送廣播

如果您想要讓用戶端透過廣播接收其資訊，請在這些欄位中輸入應該接受的個別封包位址。

圖形 23.2 進階 NTP 組態：安全性設定



進階 NTP 組態

一般設定 安全性設定

☒ 在 Chroot Jail 中執行 NTP 精靈(J)

☐ 將 NTP 服務限制為僅限已設定的伺服器(R)

防火牆設定

☐ 在防火牆中開啟埠(F) 防火牆細節(D)...

防火牆埠已關閉

說明 取消(O) 確定(O)

在「安全性設定」索引標籤 (請參閱圖形 23.2「進階 NTP 組態：安全性設定」[310頁])中，指定 `ntpd` 是否應於 `chroot jail` 中啟動。依照預設，會啟用「在 *Chroot Jail* 中執行 NTP 精靈」。由於此選項可以防止攻擊者損毀整個系統，因此在 `ntpd` 遭受攻擊時，會有較高的安全性。

「將 NTP 服務限制為僅限已設定的伺服器」可增加系統安全性，方法是禁止遠端電腦檢視並修改電腦的 NTP 設定，並且禁止使用用於遠端事件登入的設陷設備。啟用此選項後，這些限制會套用至所有遠端電腦，除非您覆寫「一般設定」索引標籤的時間來源清單中個別電腦的存取控制選項。對於所有其他遠端電腦，僅允許查詢本地時間。

如果 `SuSEfirewall2` 在作用中 (預設情況下)，請啟用「在防火牆中開啟埠」。如果您讓連接埠保持為關閉，就不可能對時間伺服器建立連接。

23.2 手動設定網路中的 NTP

在網路上使用時間伺服器的最簡單方式就是設定伺服器參數。例如，如果可以從網路存取名為 `ntp.example.com` 的時間伺服器，那麼，請新增以下行，將此伺服器的名稱新增到 `/etc/ntp.conf` 檔案：

```
server ntp.example.com
```

若要新增更多時間伺服器，請以關鍵字伺服器插入其他行。在以 `rcntp start` 指令啟始化 `ntpd` 後，系統大約會花費一個小時來穩定時間，並建立累積記錄檔案以校正本地電腦時鐘。使用累積記錄檔案，就可以在電腦一開機後立即計算硬體時鐘的系統錯誤。它會立即使用校正，使系統時間具有更高的穩定性。

有兩種方法可以將 NTP 機制做為用戶端：首先，用戶端可固定在每段間隔時間後向已知伺服器查詢時間。隨著用戶端的增加，此方法可能造成伺服器的高負載。其次，用戶端可以等待網路中的廣播時間伺服器所送出的 NTP 廣播。此方法具有伺服器品質未知的缺點，而且伺服器送出錯誤的資訊可能造成嚴重的問題。

如果時間是經由廣播取得，就不需要伺服器名稱。在這樣的情形下，請在 `/etc/ntp.conf` 組態檔中輸入 `broadcastclient`。若要完全使用一或多個已知的時間伺服器，請輸入以 `servers` 開頭的名稱。

23.3 執行時期的動態時間同步

若系統開機後並無網路連線，`ntpd` 仍會啟動，但無法解析組態檔案中設定之時間伺服器的 DNS 名稱。在加密的 WLAN 中使用網路管理員時，可能會發生這種情況。

如果您希望 `ntpd` 在執行時期解析 DNS 名稱，必須設定 `dynamic` 選項。這樣一來，當開機一段時間後連接網路時，`ntpd` 便會再次查詢名稱，並連接時間伺服器以獲取時間。

手動編輯 `/etc/ntp.conf`，並將 `dynamic` 新增至一或多個 `server` 項目：

```
server ntp.example.com dynamic
```

您也可以使用 YaST 並按以下步驟操作：

- 1 在 YaST 中，按一下「網路服務」>「NTP 組態」。
- 2 選取要設定的伺服器。然後按一下「編輯」。
- 3 啟動「選項」欄位，並新增dynamic。如果已經輸入了其他選項，請使用空格分隔。
- 4 按一下「確定」關閉編輯對話方塊。重複上述步驟以變更所有要變更的伺服器。
- 5 最後按一下「確定」儲存設定。

23.4 設定本地參考時鐘

軟體套件 ntpd 包含與本機參照時鐘連線的驅動程式。ntp-doc 套件的 /usr/share/doc/packages/ntp-doc/refclock.html 檔案中提供了受支援時鐘的清單。每個驅動程式都與數字關聯。在 NTP 中，實際組態工作是透過虛擬 IP 位址來執行。把時鐘當成在網路中一樣，將它輸入 /etc/ntp.conf 檔案中。因此，會指定特殊的 IP 位址，127.127.*t.u* 給它們。在此，*t* 代表時鐘的類型並可決定使用哪一個驅動程式，而 *u* 是代表單位，可決定使用哪一個介面。

一般而言，個別設備都具有描述組態細節的特殊參數。檔案 /usr/share/doc/packages/ntp-doc/drivers/driver*NN*.html (其中的 *NN* 為驅動程式的編號) 提供了關於特定類型之時鐘的資訊。例如，「type 8」時鐘 (透過序列介面的收音機時鐘) 需要其他可以更精確地指定時鐘的模式。例如，Conrad DCF77 接收器模組具有模式 5。若要使用此時鐘做為偏好的參考，請指定 prefer 關鍵字。Conrad DCF77 接收器模組的完整 server 行如下所示：

```
server 127.127.8.0 mode 5 prefer
```

其他的時鐘也使用相同的模式。安裝 ntp-doc 套件後，便可在 /usr/share/doc/packages/ntp-doc 目錄中找到 NTP 的文件。檔案 /usr/share/doc/packages/ntp-doc/refclock.html 提供了指向描述驅動程式參數之驅動程式頁面的連結。

23.5 將時鐘與外部時間參考 (ETR) 同步

支援將時鐘與外部時間參考 (ETR) 同步。外部時間參考每 2^{22} 百萬分之一秒 (2 的 20 次方) 傳送一次振盪器訊號與同步訊號，以將所有連結伺服器的 TOD 時鐘保持同步。

為了便利，兩個 ETR 裝置可連接到一個機器。如果時鐘偏差超出同步檢查容錯，則所有 CPU 都會收到一個機器記號，指出時鐘不同步。如果出現這種狀況，則所有啟用了 DASD I/O 到 XRC 的設備就會停止運作，直到時鐘重新同步。

ETR 支援透過兩個 `sysfs` 屬性啟動；請以 `root` 的身分執行下列指令：

```
echo 1 > /sys/devices/system/etr/etr0/online
echo 1 > /sys/devices/system/etr/etr1/online
```


網域名稱系統

必須使用 DNS (網域名稱系統) 將網域名稱和主機名稱解析為 IP 位址。例如，藉由這種方式，IP 位址 192.168.2.100 會指派給主機名稱 `jupiter`。在設定您的名稱伺服器前，請參閱第 21.3 節「名稱解析」[257頁] 中有關 DNS 的一般資訊。以下設定範例是指 BIND。

24.1 DNS 詞彙

區域

網域名稱空間細分成一個個區域。例如，如果您擁有 `example.com`，您就擁有 `com` 網域的 `example` 區段 (或區域)。

DNS 伺服器

DNS 伺服器是為網域維護名稱和 IP 資訊的伺服器。您可以擁有用於主要區域的主要 DNS 伺服器、用於從屬區域的次要伺服器、或沒有任何區域處理快取功能的從屬伺服器。

主要區域 DNS 伺服器

主要區域包含您網路上的所有主機，而且 DNS 伺服器主要區域會儲存您的網域中所有主機最新的記錄。

從屬區域 DNS 伺服器

從屬區域是主要區域的副本。從屬區域 DNS 伺服器會用區域傳輸作業從其主伺服器取得區域資料。只要從屬區域 DNS 伺服器擁有有效 (未過期) 的區域資料，它就有權代表區域回應。如果從屬無法取得區域資料的新副本，它就會停止代表區域回應。

轉遞者

轉遞者是當您的 DNS 伺服器無法答覆查詢時，它應該將其傳送至的目標 DNS 伺服器。為了在同一個組態中啟用不同的組態來源，系統使用了 `netconfig` (並請參閱 `man 8 netconfig`)。

記錄

記錄是有關名稱和 IP 位址的資訊。有關支援的記錄及其語法，請參閱 BIND 文件中的說明。一些特殊的記錄如下：

NS 記錄

NS 記錄會告訴名稱伺服器哪些機器負責管理特定網域區域。

MX 記錄

MX (郵件交換) 記錄會說明在網際網路上傳送郵件時要聯絡的機器。

SOA 記錄

SOA (授權啟動) 記錄是區域檔案中的第一筆記錄。SOA 記錄是在使用 DNS 同步化多部電腦之間的資料時使用。

24.2 安裝

若要安裝 DNS 伺服器，請啟動 YaST 並選取「軟體」>「軟體管理」。選擇「檢視」>「模式」，然後選取「*DHCP* 和 *DNS* 伺服器」。請確蓋安裝個別套件，完成此安裝程序。

24.3 使用 YaST 進行設定

使用 YaST DNS 模組可以設定區域網路的 DNS 伺服器。當您第一次啟動模組時，一個精靈會啟動，提示您指定有關伺服器管理的一些設定。完成此初步設定，即會產生基本的伺服器組態。使用進階模式可以處理更進階的組態任務，如設定 ACL、記錄、TSIG 金鑰和其他選項。

24.3.1 精靈組態

精靈包含三個步驟或對話方塊。在對話方塊中適當的地方，能夠讓您進入進階組態模式。

- 1 第一次啟動模組時，會開啟圖形 24.1「DNS 伺服器安裝：轉遞者設定」[317頁]中所示的「轉遞者設定」對話方塊。「*Netconfig DNS 規則*」決定哪些設備應提供轉遞者，或者您是否要提供自己的「轉遞者清單」。如需 `netconfig` 的詳細資訊，請參閱 `man 8 netconfig`。

圖形 24.1 DNS 伺服器安裝：轉遞者設定

轉遞者是指當您的 DNS 伺服器無法答覆查詢時，將查詢傳送至的目標 DNS 伺服器。請輸入它們的 IP 位址，然後按一下「新增」。

- 2 「DNS 區域」對話方塊包含數個部分，負責管理區域檔案，如第 24.6 節「區域檔案」[330頁]所述。對於新區域，請在「名稱」中提供其名稱。若要新增反向區域，名稱的結尾必須是 `.in-addr.arpa`。最後，選取「類型」(主要、從屬或轉遞)。請參閱圖形 24.2「DNS 伺服器安裝：DNS 區域」[318頁]。按一下「編輯」可設定現有區域的其他設定值。若要移除區域，按一下「刪除」。

圖形 24.2 DNS 伺服器安裝：DNS 區域



DNS 伺服器安裝: DNS 區域

新增區域

名稱: example.com 類型: 主要 [新增(A)]

設定時 DNS 區域

區域	類型
example.com	主要

[刪除(D)] [新增(N)]

[說明] [中止(B)] [上一步(B)] [下一步(N)]

- 3 在最後的對話方塊中，可按一下「在防火牆中開啟埠」，在防火牆中開啟 DNS 連接埠。然後決定是否在開機時啟動 DNS 伺服器(「開啟」或「關閉」)。您亦可啟用 LDAP 支援。請參閱圖形 24.3 「DNS 伺服器安裝：完成精靈」 [318頁]。

圖形 24.3 DNS 伺服器安裝：完成精靈



DNS 伺服器安裝: 完成精靈

☐ 在防火牆中開啟埠(F) [防火牆埠已關閉]

防火牆埠已關閉

☐ LDAP 主動支援(L)

啟動動作

☐ 開啟(N)：現在和開機時啟動

☒ 關閉(F)：僅手動啟動

- 轉送者: 192.168.27.1
- 領域: ., localhost, 0.0.127.in-addr.arpa, example.com

[DNS 伺服器連接埠(E)...]

[說明] [中止(B)] [上一步(B)] [完成(F)]

24.3.2 進階組態

啟動模組後，YaST 會開啟顯示數個組態選項的視窗。完成該視窗可讓 DNS 伺服器組態的基本功能就位運作：

24.3.2.1 啟動

在「**啟動**」下，定義是應在系統開機時啟動 DNS 伺服器還是手動啟動。若要立即啟動 DNS 伺服器，請按一下「**立即啟動 DNS 伺服器**」。若要停止 DNS 伺服器，請按一下「**立即停止 DNS 伺服器**」。若要儲存目前的設定，請選取「**立即儲存設定並重新載入 DNS 伺服器**」。您可以使用「**在防火牆中開啟埠**」開啟防火牆中的 DNS 埠，並使用「**防火牆詳細資訊**」修改防火牆設定。

若選取「**LDAP 主動支援**」，區域檔案將由 LDAP 資料庫來管理。只要 DNS 伺服器重新啟動或提示重新載入其組態時，就會抓取寫入到 LDAP 資料庫中區域資料的變更。

24.3.2.2 轉遞者

如果您的本地 DNS 伺服器無法答覆要求，它會嘗試將要求轉遞至「**轉遞者**」(若做此設定)。可手動將此轉遞者新增至「**轉遞者清單**」。如果轉遞者與撥號連線同樣不是靜態的，則「**netconfig**」會處理組態。如需 **netconfig** 的詳細資訊，請參閱 `man 8 netconfig`。

24.3.2.3 基本選項

在此區段中，可設定基本伺服器選項。從「**選項**」功能表中，選取所需項目，然後在對應的項目欄位中指定值。選取「**新增**」以包含新項目。

24.3.2.4 記錄

若要設定 DNS 伺服器應記錄的內容和記錄方式，請選取「**記錄**」。在「**記錄類型**」下，指定 DNS 伺服器應該寫入記錄資料的位置。選取「**系統記錄**」來使用全系統的記錄檔「`/var/log/messages`」或選取「**檔案**」指定不同的檔案。如果使用後一種方式，還需另行指定名稱、最大檔案大小(以 MB 為單位)以及要儲存的記錄檔案版本數。

進一步選項可從「其他記錄」下存取。啟用「記錄所有 DNS 查詢」會記錄每個查詢，此選項會讓記錄檔變得非常大。所以，除了偵錯用途外，啟用此選項並不是理想的作法。若要記錄 DHCP 與 DNS 伺服器之間在區域更新期間的資料流量，請啟用「記錄區域更新」。若要記錄從主伺服器到從屬伺服器在區域傳輸期間的資料流量，請啟用「記錄區域轉送」。請參閱圖形 24.4「DNS 伺服器：記錄」[320頁]。

圖形 24.4 DNS 伺服器：記錄



24.3.2.5 ACL

使用此對話方塊可定義 ACL (存取控制清單) 以強制執行存取限制。在「名稱」下提供獨特名稱後，在「值」下指定 IP 位址 (有或沒有網路遮罩)，格式如下：

```
{ 192.168.1/24; }
```

組態檔的語法要求位址以分號結尾，而且放置在大括號之間。

24.3.2.6 TSIG 金鑰

TSIG (交易簽章) 的主要目的是保護 DHCP 與 DNS 伺服器之間的通訊。在第 24.8 節「安全交易」[334頁]中有所描述。

若要產生 TSIG 金鑰，請在標籤為「金鑰 ID」的欄位中輸入特別的名稱，並指定用來儲存金鑰的檔案（「檔案名稱」）。按一下「產生」確認您的選擇。

若要使用之前建立的金鑰，請將「金鑰 ID」欄位保留空白，並在「檔案名稱」下選取儲存金鑰的檔案。接著，以「新增」確認您的選項。

24.3.2.7 DNS 區域 (新增從屬區域)

若要新增從屬區域，請選取「DNS 區域」，選擇「從屬」區域類型，指定新區域的名稱，並按一下「新增」。

在「區域編輯器」子對話方塊中，於「主 DNS 伺服器 IP」下指定從屬伺服器應從中提取資料的主伺服器。若要限制對伺服器的存取，可以從清單選取其中一個 ACL。

24.3.2.8 DNS 區域 (新增主要區域)

若要新增主要區域，請選取「DNS 區域」，選擇「主要」區域類型，寫入新區域的名稱，然後按一下「新增」。新增主要區域時，也需要新增反向區域。例如，如果新增指向子網路 192.168.1.0/24 中主機的例子.com 區域，則也應該新增涵蓋該 IP 位址範圍的反向區域。根據定義，該區域應該命名為 1.168.192.in-addr.arpa。

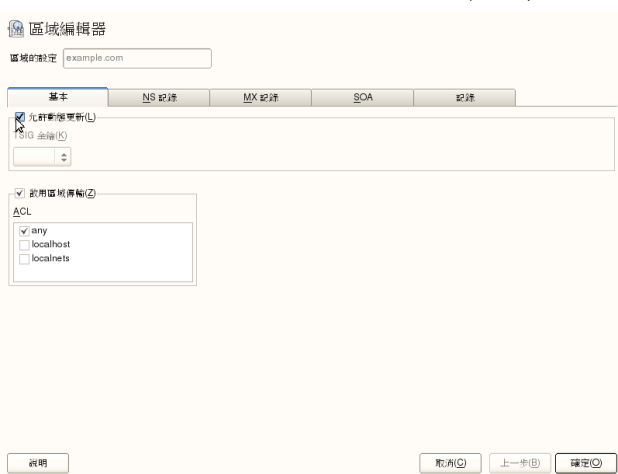
24.3.2.9 DNS 區域 (編輯主要區域)

若要編輯主要區域，請選取「DNS 區域」，然後從表中選取主要區域，並按一下「編輯」。對話方塊由幾個頁面組成：「基本」（第一個開啟的頁面）、「NS 記錄」、「MX 記錄」、「SOA」以及「記錄」。

基本對話方塊 (如圖形 24.5 「DNS 伺服器：區域編輯器 (基本)」 [322 頁] 所示)，可讓您定義動態 DNS 的設定以及到用戶端及從屬名稱伺服器之區域傳輸的存取選項。若要允許動態更新區域，請選取「允許動態更新」以及對應的 TSIG 金鑰。更新動作開始前，必須先定義金鑰。若要啟用區域傳輸，請選取對應的 ACL。必須先行定義 ACL。

在「基本」對話方塊中，選擇是否要啟用區域傳輸。使用列出的 ACL 來定義可以下載區域的人員。

圖形 24.5 DNS 伺服器：區域編輯器 (基本)



區域編輯器 (NS 記錄)

「*NS 記錄*」對話方塊可讓您為指定的區域定義替代名稱伺服器。請確定您的名稱伺服器包含於清單中。若要新增記錄，請在「*要新增的名稱伺服器*」下輸入其名稱，然後使用「*新增*」確認動作。請參閱圖形 24.6 「DNS 伺服器：區域編輯器 (NS 記錄)」[322頁]。

圖形 24.6 DNS 伺服器：區域編輯器 (*NS 記錄*)



區域編輯器 (MX 記錄)

若要新增目前區域的郵件伺服器到現有清單，請輸入對應的位址及優先順序值。完成後，選取「新增」確認該動作。請參閱圖形 24.7 「DNS 伺服器：區域編輯器 (MX 記錄)」[323頁]。

圖形 24.7 DNS 伺服器：區域編輯器 (MX 記錄)

區域編輯器 (SOA)

此頁允許您建立 SOA (授權啟動) 記錄。如需個別選項的說明，請參閱範例 24.6 「/var/lib/named/example.com.zone 檔案」[330頁]。透過 LDAP 管理的動態區域，並不支援變更 SOA 記錄。

圖形 24.8 DNS 伺服器：區域編輯器 (SOA)

區域編輯器 (記錄)

此對話方塊可管理名稱解析。在「記錄金鑰」中，輸入主機名稱，然後選取其類型。「*A-Record*」代表主項目。此項目的值應為 IP 位址。「*CNAME*」是別名。使用「*NS*」與「*MX*」類型，可取得「*NS 記錄*」與「*MX 記錄*」標籤提供之資訊的詳細或部分擴充記錄。這三個類型都可以解析成現有的 A 記錄。「*PTR*」是供反向區域所使用。它的內容與 A 記錄相反，例如：

```
hostname.example.com. IN A 192.168.0.1
1.0.168.192.in-addr.arpa IN PTR hostname.example.com.
```

注意：編輯反向區域

新增正向區域後，返回到主功能表，然後選取要編輯的反向區域。在「基本」索引標籤中，啟用「自動產生以下區域的記錄」核取方塊，然後選取正向區域。這樣，反向區域中會自動更新正向區域的所有變更。

24.4 啟動 BIND 名稱伺服器

在 SUSE® Linux Enterprise Server 系統上，名稱伺服器 BIND (*Berkeley Internet Name Domain*，柏克萊網際網路名稱網域) 已經預先設定，因此安裝後即可啟動，不會有任何問題。如果您已具有可以運作的網際網路連線，而且在 `/etc/`

resolv.conf 中輸入了 127.0.0.1 做為 localhost 的名稱伺服器位址，則通常表示您已經具有可以運作的名稱解析，因而無需瞭解提供者的 DNS。BIND 透過根名稱伺服器執行名稱解析，顯見處理程序較慢。一般而言，應該在 forwarders 下的組態檔 /etc/named.conf 中輸入提供者的 DNS 及其 IP 位址，以確保有效及安全的名稱解析。如果目前此辦法可行，名稱伺服器會當成純粹的「僅快取」名稱伺服器執行。只有在您設定了名稱伺服器自己的區域後，它才會成為真正的 DNS。/usr/share/doc/packages/bind/config 中提供了一個簡單範例。

提示：自動使用名稱伺服器資訊

在某些類型的網際網路連線或網路連線下，名稱伺服器資訊可自動根據目前的情況進行調整。若要這麼做，請將 /etc/sysconfig/network/config 檔案中的 NETCONFIG_DNS_POLICY 變數設為 auto。

不過，在相關機構為您指派正式的網域之前，切勿設定網域。即使您有自己的網域而且是由提供者管理，最好也不要使用，否則 BIND 不會轉遞此網域的要求。例如，此網域將無法存取提供者的網頁伺服器。

若要啟動名稱伺服器，請以 root 的身分輸入指令 `rcnamed start`。如果右邊出現綠色的「done」，即表示已成功啟動稱為 `named` 的名稱伺服器程序。使用 `host` 或 `dig` 程式立即測試本地系統上的名稱伺服器，應該會傳回 localhost 做為預設伺服器，位址為 127.0.0.1。如果出現的不是這種情況，則可能是 /etc/resolv.conf 包含不正確的名稱伺服器項目，或是檔案根本不存在。如果是第一次測試，請輸入 `host 127.0.0.1`，這通常都能成功。如果看到錯誤訊息，請使用 `rcnamed status`，檢查伺服器是否真的執行。如果名稱伺服器沒有啟動或是未以預期的方式運作，通常在 /var/log/messages 記錄檔中可以找到原因。

若要使用提供者的名稱伺服器或網路上正在執行的名稱伺服器做為轉遞者，請在 forwarders 下的 options 區段中輸入對應的 IP 位址。範例 24.1 「named.conf 中的轉寄選項」[325頁]中包含的位址只是範例。請根據您自己的設定調整這些項目。

範例 24.1 named.conf 中的轉寄選項

```
options {
    directory "/var/lib/named";
    forwarders { 10.11.12.13; 10.11.12.14; };
    listen-on { 127.0.0.1; 192.168.1.116; };
    allow-query { 127/8; 192.168/16; };
```

```
notify no;
};
```

options 項目後面跟著區域的項目：localhost 以及 0.0.127.in-addr.arpa。在「.」之下的 type hint 項目應該永遠是存在的。對應的檔案無需修改，而且應該依其原狀運作。另外也請確定每個項目的末尾都有「;」，且大括號在正確的位置。變更組態檔 /etc/named.conf 或區域檔後，使用 `rndc reload` 可要求 BIND 重新讀取這些檔案。使用 `rndc restart` 停止並重新啟動名稱伺服器會達成相同的結果。任何時候，輸入 `rndc stop` 都可停止伺服器。

24.5 /etc/named.conf 組態檔案

BIND 名稱伺服器本身的所有設定都儲存於檔案 /etc/named.conf 中。不過，要處理之網域的區域資料(包括主機名稱、IP 位址等)儲存於 /var/lib/named 目錄中的各個檔案中。詳細資訊會在稍後說明。

/etc/named.conf 粗略分為兩個部分。其中一個是一般設定的 options 區段，另一個則是由個別網域的 zone 項目組成。logging 區段和 acl (存取控制清單) 項目是選擇性的。註解行的開頭是 # 符號或 //。在範例 24.2 「基本的 /etc/named.conf」 [326頁] 中顯示了最基本的 /etc/named.conf。

範例 24.2 基本的 /etc/named.conf

```
options {
    directory "/var/lib/named";
    forwarders { 10.0.0.1; };
    notify no;
};

zone "localhost" in {
    type master;
    file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};

zone "." in {
    type hint;
    file "root.hint";
};
```


24.5.1 重要組態選項

`directory "filename";`

指定 BIND 可以在其中找尋包含區域資料之檔案的目錄。通常是 `/var/lib/named`。

`forwarders { ip-address; };`

指定無法直接解析 DNS 要求時應該將其轉遞至哪個名稱伺服器 (一般屬於提供者)。以 192.168.1.116 之類的 IP 位址取代 *IP 位址*。

`forward first;`

將會在嘗試透過根名稱伺服器解析 DNS 要求之前先加以轉遞。除了 `forward first`，可以寫入 `forward only` 以轉遞所有要求，且不會有任何要求傳送到根名稱伺服器。這對於防火牆組態是可以理解的。

`listen-on port 53 { 127.0.0.1; ip 位址; };`

告訴 BIND 哪個網路介面和哪個連接埠要接受用戶端查詢。`port 53` 不需要明確指定，因為 53 是預設連接埠。輸入 127.0.0.1 將允許來自本地主機的要求。如果完全省略此項目，預設會使用所有介面。

`listen-on-v6 port 53 { any; };`

告訴 BIND 哪個連接埠應該傾聽 IPv6 用戶端要求。除了 `any` 外只能使用 `none`。就 IPv6 而言，伺服器僅接受萬用字元位址。

`query-source address * port 53;`

如果防火牆封鎖 DNS 要求外送，則需要這個項目。這樣會告訴 BIND 從外部的連接埠 53 張貼要求，而不是從任何高於 1024 的連接埠張貼。

`query-source-v6 address * port 53;`

告訴 BIND 哪個連接埠用於 IPv6 查詢。

`allow-query { 127.0.0.1; net; };`

定義用戶端可以張貼 DNS 要求的網路。使用如 192.168.2.0/24 的位址資訊取代 *網路*。尾部的 /24 是網路遮罩的縮寫表示式，在此例中為 255.255.255.0。

`allow-transfer ! *;;`

控制哪些主機可以要求區域傳輸。在範例中，這類要求是使用 `! *`。如果沒有這個項目，就可以從任一處要求區域傳輸，沒有限制。

`statistics-interval 0;`

如果沒有這個項目，BIND 每小時都會在 `/var/log/messages` 中產生數行統計資訊。指定 `0` 則完全不會顯示這些統計數字，或設定以分鐘為單位的間隔時間。

`cleaning-interval 720;`

此選項定義 BIND 清除其快取記憶體的時間間隔。這樣每次清除時會觸發 `/var/log/messages` 中的項目。時間規格單位為分鐘。預設值是 60 分鐘。

`interface-interval 0;`

BIND 會定期搜尋網路介面，尋找新的或不存在的介面。如果此值設定為 `0`，就不會執行這個動作，且 BIND 僅會傾聽啟動時偵測到的介面。如果不想出現這種情況，請以分鐘為單位定義間隔時間。預設值是 60 分鐘。

`notify no;`

當變更區域資料或重新啟動名稱伺服器時，`no` 會防止通知其他名稱伺服器。

如需可用選項的清單，請參閱 `man 5 named.conf` 的手冊頁。

24.5.2 記錄

記錄的內容、方式及位置皆可在 BIND 中詳細設定。一般而言，預設設定應該足夠。範例 24.3「關閉記錄的項目」[328頁]顯示了這類項目的最簡單格式，而且完全停用了記錄。

範例 24.3 關閉記錄的項目

```
logging {  
    category default { null; };  
};
```

24.5.3 區域項目

範例 24.4 *example.com* 的區域項目

```
zone "example.com" in {  
    type master;  
    file "example.com.zone";  
    notify no;  
};
```

在 `zone` 之後，指定要管理的網域名稱 (`example.com`)，後面跟上 `in` 以及大括號括住的相關選項區塊，如範例 24.4 「`example.com` 的區域項目」[328頁] 中所示。若要定義 *slave zone*，切換 `type` 為 `slave` 並指定管理此區域的名稱伺服器為 `master` (也可能成為另一個主要的從屬)，如 範例 24.5 「`example.net` 的區域項目」[329頁] 中所示。

範例 24.5 `example.net` 的區域項目

```
zone "example.net" in {  
    type slave;  
    file "slave/example.net.zone";  
    masters { 10.0.0.1; };  
};
```

區域選項：

`type master;`

藉由指定 `master`，可以告訴 BIND 區域由本地名稱伺服器處理。這假設區域檔案已經以正確格式建立。

`type slave;`

此區域傳輸自另一部名稱伺服器。必須與 `masters` 一起使用。

`type hint;`

區域屬於 `hint` 類型，可用來設定根名稱伺服器。此區域定義可以維持原狀。

檔案 `example.com.zone` 或檔案 `slave/example.net.zone`;

此項目可指定網域之區域資料所在的檔案。從屬區域不需要此檔案，因為此資料是從另一個名稱伺服器提取。若要分別主要和從屬檔案，請為從屬檔案使用目錄 `slave`。

`masters { server-ip-address; };`

僅從屬區域需要此項目。它指定應該傳輸區域檔案的名稱伺服器。

`allow-update {! *};`

此選項可控制外部寫入存取，將允許用戶端產生 DNS 項目——出於安全性考量，通常不應使用此項目。如果沒有此項目，將禁止區域更新。以下項目會產生相同的結果，因為 `! *` 可有效地禁止任何這類活動。

24.6 區域檔案

需要兩種類型的區域檔案。一個會指派 IP 位址給主機名稱，另一個的作用恰恰相反：為 IP 位址提供主機名稱。

提示：在區域檔案中使用點號 (英文句號)

每則訊息前的 `.` 在區域檔案中具有重要意義。如果主機名稱最後不用 `.` 結尾，則會附加區域。與完整網域名稱一同指定的完整主機名稱必須以 `.` 結尾，才能避免再次附加網域。缺少 `.` 或其位置錯誤往往是造成名稱伺服器組態錯誤的原因所在。

第一個要考慮的情況是負責網域 `example.com` 的區域檔案 `example.com.zone`，如範例 24.6 「`/var/lib/named/example.com.zone` 檔案」[330頁] 中所示。

範例 24.6 `/var/lib/named/example.com.zone` 檔案

```
1. $TTL 2D
2. example.com. IN SOA      dns root.example.com. (
3.                     2003072441 ; serial
4.                     1D         ; refresh
5.                     2H         ; retry
6.                     1W         ; expiry
7.                     2D )       ; minimum
8.
9.                     IN NS      dns
10.                    IN MX      10 mail
11.
12. gate           IN A          192.168.5.1
13.               IN A          10.0.0.1
14. dns            IN A          192.168.1.116
15. mail           IN A          192.168.3.108
16. jupiter        IN A          192.168.2.100
17. venus          IN A          192.168.2.101
18. saturn         IN A          192.168.2.102
19. mercury        IN A          192.168.2.103
20. ntp            IN CNAME     dns
21. dns6           IN A6        0 2002:c0a8:174::
```

行 1:

`$TTL` 定義應該套用到此檔案中所有項目的預設有效時間。在此範例中，項目的有效時間是兩天 (2 D)。

行 2:

這是 SOA (授權開始) 控制記錄開始的地方：

- 最前面的位置中的 `example.com` 是要管理的網域名稱。名稱以 `.` 結尾，否則將再次附加區域。或者，可以在此輸入 `@`，這樣會從 `/etc/named.conf` 中的對應項目擷取區域。
- 在 `IN SOA` 之後是名稱伺服器的名稱，做為此區域的主伺服器。名稱會從 `dns` 擴充為 `dns.example.com`，因為它沒有以 `.` 結尾。
- 後面跟著此名稱伺服器之負責人的電子郵件地址。因為 `@` 符號本身具有特殊意義，所以在此輸入 `.` 來代替。對於 `root@example.com`，項目必須寫成 `root.example.com.`。每則訊息前的 `.`，以防止新增區域。
- (將所有到) 的行都包含在 `SOA` 記錄中。

行 3:

`serial number` 是任意號碼，每次此檔案變更時就會增加。通知次要名稱伺服器 (從屬伺服器) 發生變更，這是必要的。對於這種情形，十個數字的日期及執行號碼，寫法是 `YYYYMMDDNN`，已成為習慣格式。

行 4:

`refresh rate` 指定次要名稱伺服器確認區域 `serial number` 的時間間隔。在此例中，是一天。

行 5:

`retry rate` 指定在發生錯誤時次要名稱伺服器嘗試再次聯絡主要伺服器的時間間隔。在此例中，是兩小時。

行 6:

`expiration time` 指定次要名稱伺服器無法重新取得與主要伺服器的聯絡時，在此時間範圍後丟棄快取資料。此例中為一週。

行 7:

`SOA` 記錄中的最後一個項目，指定 `negative caching TTL` — 亦即可在此時間內快取其他伺服器無法解析之 `DNS` 查詢的結果。

行 9:

`IN NS` 指定負責此網域的名稱伺服器。`dns` 會擴充為 `dns.example.com`，因為它沒有以 `.` 結尾。可能有數行與此類似 — 主要名稱伺服器佔用一行，每部次要名稱伺服器也各自佔用一行。如果 `/etc/named.conf` 中的

notify 不是設定為 no，此處列出的所有名稱伺服器會收到區域資料變更的通知。

行 10:

MX 記錄指定用於接收、處理和轉遞網域 example.com 之電子郵件的郵件伺服器。在此範例中，郵件伺服器為主機 mail.example.com。主機名稱前的號碼是偏好設定值。如果有多個 **MX** 項目，會先優先使用具有最小值的郵件伺服器，而如果郵件無法送到此伺服器，就會嘗試使用下一個較高的值。

行 12-19 :

這些是指派給主機名稱的一或多個 IP 位址的實際位址記錄。此處列出的名稱不含 .，因為它們不包含其網域，所以會將 example.com 新增到所有名稱。系統會將兩個 IP 位址指定給主機 gate，因為它有兩張網路卡。若主機位址是傳統位址 (**IPv4**)，記錄會使用 **A** 標示。如果位址是 **IPv6** 位址，則會使用 **AAAA** 標示該項。

注意：IPv6 語法

IPv6 記錄與 **IPv4** 的語法稍有不同。因為可以分段，所以必須在位址前提供有關遺漏位元的資訊。若要只用所需的數字「0」填寫 **IPv6** 位址，則在位址的正確位置新增兩個冒號。

```
pluto      AAAA 2345:00C1:CA11::1234:5678:9ABC:DEF0
pluto      AAAA 2345:00D2:DA11::1234:5678:9ABC:DEF0
```

行 20:

別名 ntp 可用於定址 dns (**CNAME** 表示 正式名稱)。

虛擬網域 in-addr.arpa 用來反向查詢 IP 位址到主機名稱。它會以反向標記法附加到位址的網路部分。因此 192.168 會解析為 168.192.in-addr.arpa。請參閱範例 24.7 「反向查詢」 [332頁]。

範例 24.7 反向查詢

```
1. $TTL 2D
2. 168.192.in-addr.arpa.    IN SOA dns.example.com. root.example.com. (
3.                          2003072441          ; serial
4.                          1D                  ; refresh
5.                          2H                  ; retry
6.                          1W                  ; expiry
7.                          2D )                ; minimum
8.
```

```
9.                               IN NS           dns.example.com.
10.
11. 1.5                           IN PTR         gate.example.com.
12. 100.3                         IN PTR       www.example.com.
13. 253.2                         IN PTR       cups.example.com.
```

行 1:

\$TTL 定義套用到此處所有項目的標準 TTL。

行 2:

組態檔應該為網路 192.168 啟用反向查詢。假設 區域稱為 168.192.in-addr.arpa，則不應新增到主機名稱。因此輸入的主機名稱都使用完整格式 — 附帶網域並以 . 做為結尾。其餘的項目與之前 example.com 範例中所述的項目對應。

行 3–7:

請參閱之前的 example.com 範例。

行 9:

同樣地，此行指定負責此區域的名稱伺服器。不過，這一次是以完整格式輸入名稱，即包含網域以及結尾的 .。

行 11–13:

這些是相關主機上 IP 位址的指標記錄提示。行的開頭僅輸入了 IP 位址的最後一部分，結尾沒有 .。對此附加區域(不加上 .in-addr.arpa)會造成完整 IP 位址變成反向順序。

一般情況下，不同 BIND 版本之間的區域傳輸應該可以順利進行。

24.7 區域資料的動態更新

「動態更新」這個詞是指新增、變更或刪除主伺服器的區域檔案項目的作業。此機制於 RFC 2136 中有詳細描述。利用新增選擇性的 allow-update 或 update-policy 規則，可為每個區域項目個別設定動態更新。動態更新的區域不應該手動修改。

使用指令 nsupdate 將要更新的项目傳送到伺服器。如需此指令的完整語法，請查閱 nsupdate 的手冊頁 (man 8 nsupdate)。為了安全性的緣故，這類更新應該使用 TSIG 金鑰加以執行，如第 24.8 節「安全交易」[334頁] 所述。

24.8 安全交易

透過採用共享秘密金鑰 (也稱為 TSIG 金鑰) 的交易簽章 (TSIG)，可以實現安全交易。本節說明如何產生及使用這類金鑰。

不同伺服器之間的通訊，以及區域資料的動態更新，都需要安全交易。讓存取控制依靠金鑰比單純依靠 IP 位址要來得安全許多。

使用以下指令可產生 TSIG 金鑰 (有關詳細資訊，請參閱 `mandnssec-keygen`):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

這樣會建立兩個檔案，名稱類似如下：

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

金鑰本身 (如 `ejIkuCyyGJwwuN3xAteKgg==` 的字串) 在兩個檔案中都可找到。如果要用於交易，第二個檔案 (`Khost1-host2.+157+34265.key`) 必須傳輸到遠端主機，最好是以安全的方式傳輸 (例如，使用 `scp`)。在遠端伺服器上，金鑰必須包含於檔案 `/etc/named.conf` 內，才能開啟 `host1` 與 `host2` 之間的安全通訊：

```
key host1-host2 {  
    algorithm hmac-md5;  
    secret "ejIkuCyyGJwwuN3xAteKgg=";  
};
```

警告： `/etc/named.conf` 的檔案權限

請確定 `/etc/named.conf` 的許可權受到適當的限制。此檔案的預設值是 0640，擁有者為 `root` 及群組 `named`。另一種方法是，將金鑰移到具有特別限定許可權的其他檔案，然後將檔案從 `/etc/named.conf` 包含進來。若要包含外部檔案，請使用：

```
include "filename"
```

將檔案名稱取代為金鑰所在檔案的絕對路徑。

若要讓伺服器 `host1` 能夠使用 `host2` (在此範例中位址為 10.1.2.3) 的金鑰，伺服器的 `/etc/named.conf` 必須包含以下規則：

```
server 10.1.2.3 {  
    keys { host1-host2. };  
};
```


類比項目必須包含於 `host2` 的組態檔中。

針對為 IP 位址和位址範圍定義的任何 ACL (存取控制清單，切勿與檔案系統 ACL 混淆) 新增 TSIG 金鑰，以確保交易安全性。對應項目應該看起來如下：

```
allow-update { key host1-host2. ;};
```

此主題在 `update-policy` 下的 *BIND Administrator Reference Manual* 中有詳細討論。

24.9 DNS 安全性

DNSSEC 或 DNS 安全性細述於 RFC 2535。DNSSEC 的可用工具在 BIND 手冊中有詳加討論。

與一或多個區域金鑰關聯的區域才是安全區域。與主機金鑰一樣，這些金鑰也是使用 `dnssec-keygen` 產生。目前是使用 DSA 加密演算法產生這些金鑰。產生的公用金鑰應該包含於套用 `$INCLUDE` 規則的對應區域檔案中。

使用 `dnssec-signzone` 指令，可以建立產生的金鑰集 (`keyset-` 檔案)，將金鑰集安全地傳送至父區域，並對其簽名。這樣便會在 `/etc/named.conf` 中產生每個區域要包含的檔案。

24.10 如需更多資訊

如需其他資訊，請參閱 `bind-doc` 套件的 *BIND Administrator Reference Manual* (安裝於 `/usr/share/doc/packages/bind/` 下)。另外也請參閱手冊參考的 RFC 以及 BIND 隨附的手冊頁。如需 SUSE Linux Enterprise Server 之 BIND 的最新資訊，請參閱 `/usr/share/doc/packages/bind/README.SuSE`。

DHCP

動態主機組態通訊協定 (Dynamic Host Configuration Protocol, DHCP) 的用途是從伺服器集中指定網路設定，這樣就不必在每一個工作站本地分別設定。設定要使用 DHCP 的主機對於自己的靜態位址並沒有控制權。它可以根據伺服器的指示完全且自動地設定自己本身。如果您在用戶端使用 NetworkManager，就完全不必設定用戶端。這在環境多變、而且一次只使用一個介面的情況下非常有用。絕對不要在執行 DHCP 伺服器的機器上使用 NetworkManager。

提示：IBM System z：DHCP 支援

在 IBM System z 平台上，DHCP 僅能用於使用 OSA 和 OSA Express 網路卡的介面。這些網路卡是唯一使用 MAC 的網路卡，是 DHCP 自動組態功能的必要元件。

DHCP 伺服器的一種設定方式是識別每個使用網路卡硬體位址 (大部分的情況下是固定的) 的用戶端，以後每次用戶端連接伺服器時，將提供相同的設定值給用戶端。或者，也可以將 DHCP 設定成從專門設定的位址池，動態指派位址給每個相關用戶端。在後者的情形中，DHCP 伺服器在每次接到請求時會指派相同的位址給用戶端，即使經過較長的時間也是一樣。這只適用於網路用戶端數少於網路位址數的情況。

DHCP 可簡化系統管理員的工作。任何與位址及一般網路組態相關的變更 (包括較大的變更) 都可集中執行，只要編輯伺服器的組態檔。與重新設定眾多的工作站相比，這種方法要便利許多。此外，由於這些機器可以從位址池獲取 IP 位址，因此將機器 (特別是新機器) 整合到網路中也要容易得多。從 DHCP 伺服器擷取適當的網路設定這種方式，對於經常需要在不同網路中使用筆記型電腦的情況特別有用。

在本章中，DHCP 伺服器將在使用 192.168.2.1 做為閘道的工作站 192.168.2.0/24 所在的子網路中執行。它有固定的 IP 位址 192.168.2.254，並處理兩個位址範圍：192.168.2.10 到 192.168.2.20 以及 192.168.2.100 到 192.168.2.200。

DHCP 伺服器不僅提供 IP 位址和網路遮罩，也提供主機名稱、網域名稱、閘道和名稱伺服器位址供用戶端使用。除此之外，DHCP 也允許集中設定一些其他的參數，例如，用戶端可以輪詢目前時間的時間伺服器或甚至是列印伺服器。

25.1 使用 YaST 設定 DHCP 伺服器

若要安裝 DNS 伺服器，請啟動 YaST 並選取「軟體」>「軟體管理」。選擇「過濾器」>「模式」，然後選取「DHCP 及 DNS 伺服器」。請確蓋安裝個別套件，完成此安裝程序。

重要：LDAP 支援

YaST DHCP 模組可以設定成將伺服器組態儲存在本地（即執行 DHCP 伺服器的主機上），或是由 LDAP 伺服器來管理其組態資料。如果要使用 LDAP，應在設定 DHCP 伺服器之前先設定您的 LDAP 環境。

如需 LDAP 的詳細資訊，請參閱第 4 章「*LDAP—A Directory Service*」（↑*Security Guide*）。

YaST DHCP 模組 (`yast2-dhcp-server`) 可讓您為區域網路設定您自己的 DHCP 伺服器。該模組能夠以精靈模式或是進階組態模式執行。

25.1.1 初始組態（精靈）

首次啟動模組時，會啟動精靈，提示您對伺服器管理進行一些基本設定。完成此初始設定程序後會產生一個非常基本的伺服器組態，能夠發揮其基本功能。進階模式可以處理更多進階設定任務。請執行下列步驟：

- 1 請從清單中選取 DHCP 伺服器應監聽的介面，然後按一下「選取」。接著選取「開啟選取介面的防火牆」，以開啟此介面的防火牆，然後按「下一步」。請參閱圖形 25.1「DHCP 伺服器：介面卡選項」[339頁]。

圖形 25.1 DHCP 伺服器：介面卡選項

 DHCP 伺服器精靈 (1/4): 介面卡選項

DHCP 伺服器的網路卡

已選取

介面名稱	設備名稱	IP
br0	DHCP 位址	
br1	DHCP 位址	
ib1	DHCP 位址	

選取(S)

取消選取(U)

☒ 開啟選取介面的防火牆(F)

說明

中止(B)

上一步(B)

下一步(N)

2 使用核取方塊決定您的 DHCP 設定是否要由 LDAP 伺服器自動儲存。在輸入欄位中提供 DHCP 伺服器應管理的所有用戶端的網路細節。這些細節包括網域名稱、時間伺服器的位址、主要及次要名稱伺服器的位址、列印和 WINS 伺服器的位址 (供同時具有 Windows 與 Linux 用戶端的混和網路使用)、閘道位址以及租用時間。請參閱圖形 25.2「DHCP 伺服器：全域設定」[340 頁]。

圖形 25.2 DHCP 伺服器：全域設定

 DHCP 伺服器精靈 (2/4): 全域設定

☐ LDAP 支援

DHCP 伺服器名稱 (選擇性)

網域名稱(D)

主要名稱伺服器 IP

次要名稱伺服器 IP(S)

預設網速 (除由圖)(G)

NTP 時間伺服器(T)

列印伺服器(P)

WINS 伺服器(W)

預設租用時間(L)
 單位(U)
小時

說明

中止(B)

上一步(B)

下一步(N)

- 3 設定應該如何將動態 IP 位址指定給用戶端。若要這樣做，指定伺服器可以指派位址給 DHCP 用戶端的 IP 範圍。所有這些位址應該涵蓋在相同的網路遮罩下。另外也指定租用時間，在此時間段內用戶端可以保留其 IP 位址，無需要求延續租用。或者，指定最長租用時間，也就是伺服器保留特定用戶端之 IP 位址的時間。請參閱圖形 25.3 「DHCP 伺服器：動態 DHCP」 [341 頁]。

圖形 25.3 DHCP 伺服器精靈 (3/4): 動態 DHCP

 DHCP 伺服器精靈 (3/4): 動態 DHCP

子網路資訊

目前網路 (N)

172.22.0.0

目前網路 遮罩 (M)

255.255.0.0

網路 遮罩 位元 (I)

16

最小 IP 位址 (I)

172.22.0.1

最大 IP 位址 (X)

172.22.255.254

IP 位址範圍

第一個 IP 位址 (F)

192.168.2.100

最後一個 IP 位址 (L)

192.168.2.128

☐ 允許動態 BOOTP (B)

租用時間

預設 (D)

4

單位 (U)

小時

最大 (M)

2

單位 (T)

日

同步化 DNS 伺服器 (S)...

說明

中止 (B)

上一步 (B)

下一步 (N)

4 定義應該如何啟動 DHCP 伺服器。指定您希望系統開機時自動啟動 DHCP 伺服器，還是在需要時手動啟動 (例如，用於測試目的)。按一下「完成」完成伺服器的組態。請參閱圖形 25.4 「DHCP 伺服器：啟動」 [342頁]。

圖形 25.4 DHCP 伺服器：啟動



- 5 除了以先前步驟描述的方式使用動態 DHCP 外，您也可以設定伺服器以準靜態方式指定位址。使用下半部所提供的輸入欄位，指定用戶端清單以這種方式進行管理。具體而言，就是提供要指定給這類用戶端的「名稱」和「IP 位址」，另外還要提供「硬體位址」和「網路類型」（記號環或乙太網路）。使用「新增」、「編輯」和「從清單中刪除」修改顯示於螢幕上半部分的用戶端清單。請參閱圖形 25.5 「DHCP 伺服器：主機管理」 [343頁]。

圖形 25.5 DHCP 伺服器：主機管理

啟動
介面卡選擇
全域設定
對能: DHCP
主機管理
進階設定

DHCP 伺服器：主機管理

註冊的主機

名稱	IP	硬體位址	類型
----	----	------	----

清單設定

名稱(I): IP 位址(I): 硬體位址(H):

☒ 乙太網路(E) ☐ 記錄對象(T)

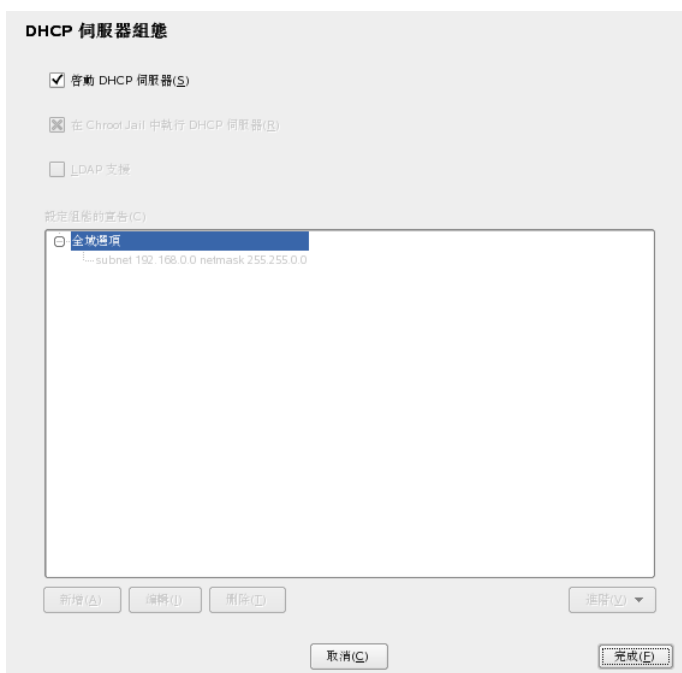
25.1.2 DHCP 伺服器組態 (進階)

除了稍早討論的組態方法外，還有進階組態模式，可讓您變更 DHCP 伺服器設定的每個細節。啟動進階組態，方法是在「啟動」對話方塊中按一下「*DHCP 伺服器進階組態*」(請參閱圖形 25.4「DHCP 伺服器：啟動」[342頁])。

Chroot 環境與宣告

在此第一個對話方塊中，選取「*啟動DHCP 伺服器*」讓現有組態可以編輯。DHCP 伺服器行為的一個重要特點是，它能夠在 chroot 環境或 chroot jail 中執行，以確保伺服器主機的安全。如果 DHCP 伺服器會遭受外部攻擊，駭客將會被阻絕於 chroot jail 的保護之外，防止其染指系統的其他部分。對話方塊的下半部顯示已經定義之宣告的樹狀檢視。使用「新增」、「刪除」和「編輯」修改這些宣告。選取「進階」將帶您到其他的進階對話方塊。請參閱圖形 25.6「DHCP 伺服器：Chroot Jail 和宣告」[344頁]。選取「新增」後，定義要新增的宣告類型。使用「進階」，檢視伺服器的記錄檔、設定 TSIG 金鑰管理，並根據 DHCP 伺服器的設定調整防火牆的組態。

圖形 25.6 *DHCP 伺服器：Chroot Jail 和宣告*



選取宣告類型

DHCP 伺服器的「全域選項」由數個宣告組成。此對話方塊可讓您設定宣告類型：「子網路」、「主機」、「共享網路」、「群組」、「位址池」和「類別」。此範例顯示新子網路的選項 (請參閱 圖形 25.7 「DHCP 伺服器：選取宣告類型」 [345 頁])。

圖形 25.7 DHCP 伺服器：選取宣告類型

宣告類型

☒ 子網路(S)

☐ 主機(H)

☐ 共用網路(N)

☐ 群組(G)

☐ 位址池(P)

☐ 類別(C)

中止(B)

下一步(N)

子網路組態

此對話方塊可讓您使用 IP 位址及網路遮罩來指定新的子網路。在對話方塊的中間部分，使用「新增」、「編輯」和「刪除」修改所選子網路的 DHCP 伺服器啟動選項。若要設定子網路的動態 DNS，選取「動態 DNS」。

圖形 25.8 DHCP 伺服器：設定子網路

子網路組態

網路位址(N) 網路遮罩(M)

選項	值
default-lease-time	14400
max-lease-time	172800

新增(A) 編輯(I) 刪除(D) 動態 DNS(D)

中止(B) 確定(O)

TSIG 金鑰管理

如果在上一個對話方塊中選擇設定動態 DNS，現在可以針對安全區域傳輸設定金鑰管理。選取「確定」會帶您到另一個對話方塊，讓您設定動態 DNS 的介面 (請參閱 圖形 25.10 「DHCP 伺服器：動態 DNS 的介面組態」 [348頁])。

圖形 25.9 DHCP 伺服器：TSIG 組態

TSIG 金鑰管理

新增現有的 TSIG 金鑰

檔案名稱(F):

建立新的 TSIG 金鑰

金鑰 ID(K): 檔案名稱(F):

目前的 TSIG 金鑰

金鑰 ID	檔案名稱
-------	------

動態 DNS：介面組態

選取「*啟用此子網路的動態 DNS*」，即可啟用子網路的動態 DNS。完成此操作後，使用下拉式清單選擇正向與反向區域的 TSIG 金鑰，確定為 DNS 和 DHCP 伺服器選擇的金鑰相同。使用「*更新全域動態 DNS 設定*」，來依據動態 DNS 環境自動更新及調整全域 DHCP 伺服器設定。最後，定義每個動態 DNS 的哪些轉遞和反向區域需要更新，為兩個區域都指定主要名稱伺服器的名稱。選取「*確定*」返回子網路組態對話方塊 (請參閱圖形 25.8

「DHCP 伺服器：設定子網路」[346頁])。再次選取「*確定*」返回最初的進階組態對話方塊。

圖形 25.10 DHCP 伺服器：動態 DNS 的介面組態

The screenshot shows the 'Dynamic DNS' configuration window for a DHCP server. The window has a title bar with a document icon and the text '介面組態'. Inside, there is a section for enabling dynamic DNS with a checked checkbox labeled '啟用此子網路的動態 DNS(E)'. Below this are two dropdown menus: '正向區域 TSIG 金鑰(K)' and '反向區域 TSIG 金鑰(K)', both set to 'example'. A checkbox for '更新全域動態 DNS 設定(U)' is unchecked. At the bottom, there are four text input fields arranged in two rows: '區域(Z)' and '主要 DNS 伺服器(P)' in the first row, and '反向區域(V)' and '主要 DNS 伺服器(I)' in the second row. The bottom of the window features three buttons: '上一步(B)' (Previous), '中止(R)' (Cancel), and '確定(O)' (OK).

網路介面組態

若要定義 DHCP 伺服器應該監聽的介面以及調整防火牆組態，請從進階組態對話方塊中選取「進階」>「介面組態」。從顯示的介面清單中，選取一或多個要由 DHCP 伺服器處理的介面。如果所有子網路中的用戶端都必須能與伺服器通訊，並且伺服器主機還要執行防火牆，請對防火牆進行相應的調整。若要這樣做，請選取「調整防火牆設定」。接著，YaST 會將 SuSEfirewall2 的規則調整為新的條件 (請參閱圖形 25.11 「DHCP 伺服器：網路介面和防火牆」[349頁])，之後您即可選取「確定」返回最初的對話方塊。

圖形 25.11 DHCP 伺服器：網路介面和防火牆

介面組態

可用的介面

☒ eth-id-00 0c: 29:73: 6f:f5

☒ 開啓選取介面的防火牆(F)

上一步(B) 中止(B) 確定(O)

完成所有組態步驟後，按一下「確定」關閉對話方塊。伺服器現在會以新的組態啟動。

25.2 DHCP 軟體套件

產品可以使用 DHCP 伺服器，也可以使用 DHCP 用戶端。可用的 DHCP 伺服器是 `dhcpcd` (由 Internet Systems Consortium 發佈)。對於用戶端，可於兩個不同的 DHCP 用戶端程式間做出選擇：`dhcpc-client` (也來自 ISC) 以及 `dhcpcd` 套件中的 DHCP 用戶端精靈。

預設會安裝 `dhcpcd`。該程式易於使用，而且會在每次系統開機時自動啟動，尋找 DHCP 伺服器。它不需要組態檔來執行其工作，而且大部分的標準設定可以直接使用。如果情況較為複雜，請使用 `ISC dhcpc-client`，此程式可透過組態檔案 `/etc/dhclient.conf` 來控制。

25.3 DHCP 伺服器 dhcpd

任何 DHCP 系統的核心都是動態主機組態通訊協定精靈。這個伺服器會依照組態檔 `/etc/dhcpd.conf` 中定義的設定，租用位址並監看其使用情形。藉由變更此檔案中的參數及值，系統管理員可以透過數種方式影響程式的行為。請參閱 範例 25.1 「組態檔 `/etc/dhcpd.conf`」 [350頁] 中的 `/etc/dhcpd.conf` 基本範例檔案。

範例 25.1 組態檔 `/etc/dhcpd.conf`

```
default-lease-time 600;          # 10 minutes
max-lease-time 7200;             # 2  hours

option domain-name "example.com";
option domain-name-servers 192.168.1.116;
option broadcast-address 192.168.2.255;
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0
{
    range 192.168.2.10 192.168.2.20;
    range 192.168.2.100 192.168.2.200;
}
```

這個簡單的組態檔應足以讓 DHCP 伺服器在網路中指派 IP 位址。請確定每行結尾都插入分號，否則不會啟動 `dhcpd`。

範例檔可以分為三個部分。第一個部分定義要求用戶端預設可租用 IP 位址的秒數(`default-lease-time`)，此時間過後將需要申請續約。其中還包含機器可以保留 DHCP 伺服器指派之 IP 位址、不申請續約的最長期限的陳述式(`max-lease-time`)。

在第二部份中，一些基本網路參數定義於全域層級：

- 行 `option domain-name` 定義了您網路的預設網域。
- 利用 `option domain-name-servers` 項目，最多可指定三個 DNS 伺服器值，用來將 IP 位址解析為主機名稱，或將主機名稱解析為 IP 位址。最好在設定 DHCP 前先設定機器上或網路上其他位置的名稱伺服器。該名稱伺服器也應為每個動態位址定義主機名稱，或為每個主機名稱定義動態位址。若要瞭解如何設定您自己的名稱伺服器，請參閱第 24 章「網域名稱系統」 [315頁]。

- `option broadcast-address` 這一行定義要求用戶端應使用的廣播位址。
- 利用 `option routers`，可設定伺服器要將無法傳送至區域網路上之主機的资料封包傳送到什麼地方 (依據提供的來源和目的主機位址及子網路遮罩)。在大多數的情況中，特別是較小的網路，此路由與網際網路閘道是完全一樣的。
- 利用 `option subnet-mask`，指定指定給用戶端的網路遮罩。

檔案的最後一個部分定義網路，包括子網路遮罩。若要完成設定，請指定 DHCP 精靈用來指派 IP 位址給相關用戶端的位址範圍。在範例 25.1「組態檔 `/etc/dhcpd.conf`」[350頁] 中，用戶端的指定位址可介於 192.168.2.10 與 192.168.2.20 之間以及 192.168.2.100 與 192.168.2.200 之間。

編輯這幾行後，就能夠使用指令 `rcdhcpd start` 啟用 DHCP 精靈。該精靈可以立即使用。使用指令 `rcdhcpd check-syntax` 執行簡短的語法檢查。如果在組態上遇到任何未預期的問題，例如同伺服器因出現錯誤而中止或在啟動時沒有傳回 done，可以查詢主系統記錄 `/var/log/messages` 或主控台 10 (Ctrl + Alt + F10) 上的資訊，找出問題所在。

在預設的 SUSE Linux Enterprise Server 系統上，出於安全性考量，DHCP 精靈會在 `chroot` 環境中啟動。組態檔必須複製到 `chroot` 環境，如此精靈才可以找到這些檔案。通常情況下不需要擔心發生這種情形，因為指令 `rcdhcpd start` 會自動複製檔案。

25.3.1 使用固定 IP 位址的用戶端

DHCP 也可以用來指派預先定義的靜態位址給特定用戶端。明確指派的位址永遠比集區的動態位址優先。當可用位址不足，伺服器必須在用戶端之間重新分配位址時 (舉例而言)，動態位址便會過期，靜態位址則不同，它永遠不會過期。

為了識別使用靜態位址設定的用戶端，`dhcpd` 會使用硬體位址 (全域唯一的固定數字代碼，由六對八位元組組成) 來識別所有網路設備 (例如，00:30:6E:08:EC:80)。如果相對的行 (如 範例 25.2「組態檔的增加部分」[352頁] 中所示) 新增到 範例 25.1「組態檔 `/etc/dhcpd.conf`」[350頁] 的組態檔，DHCP 精靈始終會指定相同的資料集給對應的用戶端。

範例 25.2 組態檔的增加部分

```
host jupiter {  
    hardware ethernet 00:30:6E:08:EC:80;  
    fixed-address 192.168.2.100;  
}
```

在第一行輸入對應用戶端的名稱 (host 主機名稱，範例中為 jupiter)，在第二行輸入 MAC 位址。在 Linux 主機上，使用指令 `ip link show` 並在後面接上網路設備 (例如，eth0) 可尋找 MAC 位址。輸出應該包含如下內容

```
link/ether 00:30:6E:08:EC:80
```

在上述範例中，具有網路卡、且 MAC 位址為 00:30:6E:08:EC:80 的用戶端會自動分配到 IP 位址 192.168.2.100 及主機名稱 jupiter。幾乎所有情況中輸入的硬體類型會是 ethernet，儘管通常在 IBM 系統上找到的是 token-ring，也是可以支援的。

25.3.2 SUSE Linux Enterprise Server 版本

為了改善安全性，SUSE Linux Enterprise Server 版 ISC DHCP 伺服器在出貨時即套用了 Ari Edelkind 的 non-root/chroot 修補程式。這樣可讓 dhcpd 利用使用者 ID nobody 執行，而且也能在 chroot 環境下 (/var/lib/dhcp) 執行 dhcpd。若要這樣做，組態檔 dhcpd.conf 必須位於 /var/lib/dhcp/etc。init 程序檔啟動時會自動複製檔案到此目錄。

透過檔案 /etc/sysconfig/dhcpd 中的項目，可控制伺服器與此功能相關的行為。若是不要在 chroot 環境下執行 dhcpd，請將 /etc/sysconfig/dhcpd 中的 DHCPD_RUN_CHROOTED 變數設定為「no」。

若要讓 dhcpd 從 chroot 環境內解析主機名稱，必須也要複製以下其他組態檔案：

- /etc/localtime
- /etc/host.conf
- /etc/hosts
- /etc/resolv.conf

啟動 `init` 程序檔時，這些檔案會複製到 `/var/lib/dhcp/etc/`。如果 `/etc/ppp/ip-up` 之類的程序檔動態修改了這些檔案，則進行所需變更時，也要考量到這些副本。不過，如果組態檔僅指定 IP 位址 (而不是指定主機名稱) 時，則不需要擔心。

如果組態包含要複製到 `chroot` 環境的其他檔案，請在檔案 `/etc/sysconfig/dhcpd` 中的變數 `DHCPD_CONF_INCLUDE_FILES` 下設定這些檔案。為了確保重新啟動 `syslog-ng` 精靈後，DHCP 記錄設備仍然能夠持續運作，`/etc/sysconfig/syslog` 檔案中還有另一個項目 `SYSLOGD_ADDITIONAL_SOCKET_DHCP`。

25.4 如需更多資訊

如需有關 DHCP 的詳細資訊，請參閱 *Internet Systems Consortium* 的網站 <http://www.isc.org/products/DHCP/>。在 `dhcpd`、`dhcpd.conf`、`dhcpd.leases` 和 `dhcp-options` `man` 頁面中也可以找到資訊。

使用 NetworkManager

NetworkManager 是筆記型電腦與其他可攜式電腦的理想解決方案。它允許對網路連線使用一流的加密類型和標準，包括連至 802.1X 保護網路的連線。802.1X 是「區域網路和都會區網路的 IEEE 標準 - 基於連接埠的網路存取控制」。有了 NetworkManager，您身處不同的環境中就不必顧慮網路介面的組態設定，也不必考慮如何在有線網路或無線網路之間進行切換。NetworkManager 可自動連接已知的無線網路，或是同時管理多個網路連線，然後按預設使用速度最快的連線。此外，您還可以手動在可用網路之間切換，並使用系統匣中的 Applet 管理網路連線。

同一時間有多個連線處於使用中狀態，而不僅僅是一個。因此，您可以在將筆記型電腦從乙太網路中斷開後，繼續透過無線網路保持連線狀態。

26.1 NetworkManager 的使用案例

NetworkManager 提供了精巧且直觀的使用者介面，可以讓使用者輕鬆切換網路環境。但是 NetworkManager 解決方案不適用於下列情況：

- 您的電腦會為網路的其他電腦提供網路服務，例如，它是 DHCP 或 DNS 伺服器。
- 您的電腦為 Xen 伺服器，或您的系統是 Xen 之中的虛擬系統。

26.2 啟用或停用 NetworkManager

對於筆記型電腦，NetworkManager 預設處於啟用狀態。但是您也可以 YaST 網路設定模組中隨時將其啟用或停用。

- 1 執行 YaST，然後前往「網路設備」>「網路設定」。
 - 2 此時將開啟「網路設定」對話方塊。前往「全域選項」索引標籤。
 - 3 若要使用 NetworkManager 設定和管理網路連線：
 - 3a 在「網路設定方法」欄位中，選取「使用 *NetworkManager* 進行使用者控制」。
 - 3b 按一下「確定」，然後關閉 YaST。
 - 3c 依第 26.3 節「設定網路連線」[357頁]中所述使用 NetworkManager 設定您的網路連線。
 - 4 若要停用 NetworkManager 並以傳統方式控制網路：
 - 4a 在「網路設定方法」欄位中，選擇「使用 *ifup* 的傳統方法」。
 - 4b 按一下「確定」。
 - 4c 透過 YaST 使用 DHCP 的自動組態或靜態 IP 位址來設定您的網路卡。或者，使用 YaST 設定數據機：
 - 對於撥號連線，請使用「網路設備」>「數據機」。
 - 若要設定內部或 USB ISDN 數據機，請選取「網路設備」>「*ISDN*」。
 - 若要設定內部或 USB DSL 數據機，請選取「網路設備」>「*DSL*」。
- 如需使用 YaST 設定網路組態的詳細資訊，請參閱第 21.4 節「使用 YaST 手動設定網路連線」[258頁]和第 18 章「無線區域網路」[207頁]。

26.3 設定網路連線

在 YaST 中啟用 NetworkManager 之後，使用 KDE 和 GNOME 中提供的 NetworkManager 前端設定網路連線。兩者的前端所顯示的網路組態對話方塊很相似。它們都會顯示所有類型網路連線的索引標籤，如有線、無線、行動寬頻、DSL 及 VPN 連線。您可以在每個索引標籤上新增、編輯或刪除相應類別的連線。在 KDE 組態對話方塊中，僅有系統提供的連線類型（視硬體和軟體而定），其索引標籤才會處於使用中狀態。依預設，KNetworkManager 還會顯示每個索引標籤上各個輸入欄位和選項的完整工具提示。

注意：藍芽連線

目前無法使用 NetworkManager 設定藍芽連線。

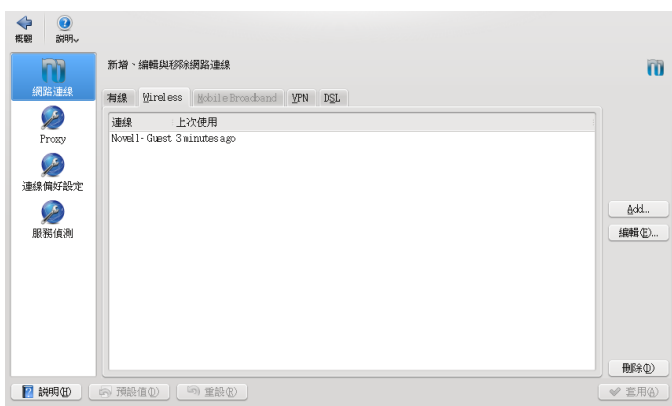
若要開啟 GNOME 中的網路組態對話方塊，請開啟主功能表，然後按一下右側的「網路」項目。也可以按 **Alt+F2**，然後輸入 `nm-connection-editor`，或者在 GNOME 控制中心內選取「系統」>「網路連線」。

圖形 26.1 GNOME 網路連線對話方塊



如果使用 KDE，則開啟主功能表，然後按一下「設定桌面」。在「個人設定」中，選取「一般」索引標籤上的「網路設定」，開啟網路組態對話方塊。

圖形 26.2 KDE 網路組態對話方塊



或者，也可以透過系統匣中的 NetworkManager Applet 開啟組態對話方塊。在 KDE 中，按一下該圖示，然後選取「管理連線」。在 GNOME 中，用滑鼠右鍵按一下該圖示，然後選取「編輯連線」。

注意：選項的可用性

在某些系統設定下，您可能無法設定連線。在安全環境中，某些選項可能會被鎖定，或者需要 `root` 許可權。請向您的系統管理員洽詢詳細資料。

過程 26.1 新增或編輯連線

借助 NetworkManager 設定網路連線後，還可以定義所有使用者可共享的系統連線。與使用者連線相比，系統連線在啟動 NetworkManager 之後便可立即使用，不必等到使用者登入之後。如需兩種連線類型的詳細資訊，請參閱第 26.7.1 節「使用者和系統連線」[368頁]。

目前，KDE 中不提供系統連線選項。因此，若要設定系統連線，需使用 YaST。

注意：隱藏的網路

若要連接至「隱藏」網路（一種不廣播其服務的網路），則您必須知道該網路的服務設定識別碼 (SSID) 或延伸服務設定識別碼 (ESSID)。系統無法自動偵測到隱藏的網路。

- 1 在網路組態對話方塊中，按一下要使用之連線類型對應的索引標籤。

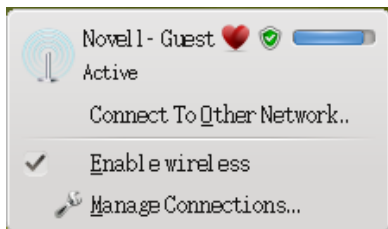
- 2 按一下「新增」以建立新的連線，也可以選取現有連線，然後按一下「編輯」。
- 3 輸入「連線名稱」以及連線詳細資料。
- 4 如果是隱藏網路，請輸入 ESSID 及加密參數。
- 5 如果一種連線類型對應多個實體設備(例如，您的機器配有兩個乙太網路卡或兩個無線介面卡)，可以將此連線關聯到特定的設備。

如果使用的是 KDE，請透過「限制介面」選項達成上述目的。如果使用的是 GNOME，請輸入連線要關聯之設備的「MAC 位址」，並確認設定。

- 6 為了讓 NetworkManager 自動使用特定連線，請為此連線啟動下列選項：「自動連接」(KDE) 或「儘可能保持連接」(GNOME)。
- 7 若要將連線轉變為系統連線，請啟動「所有使用者皆可用」(GNOME)。要建立並編輯系統連線，需要 root 許可權。

確認變更後按一下 NetworkManager Applet，所顯示的可用網路清單中便會出現新設定的網路連線。

圖形 26.3 KNetworkManager — 已設定的可用連線



26.4 使用 KNetworkManager

NetworkManager 的 KDE 前端是 KNetworkManager Applet。為 NetworkManager 控制設定網路之後，Applet 通常會於桌面環境啟動時自動啟動，並顯示為系統匣中的一個圖示。

如果系統匣未顯示任何網路連線圖示，則可能是 Applet 未啟動。按 Alt + F2 並輸入 `knetworkmanager` 可手動將其啟動。

KNetworkManager 只會顯示已設定連線的無線網路。如果您不在無線網路的覆蓋範圍內，或是網路線斷開連線，這些連線便會隱藏，因此可以使用的連線始終一目了然。

26.4.1 管理有線網路連線

如果電腦已藉由網路線連接至現有網路，請使用 KNetworkManager 來選擇網路連線。

- 1 在 applet 圖示上按一下滑鼠左鍵，以顯示可用網路的功能表。功能表中處於選中狀態的便是目前使用的連線，此連線標示為「使用中」。
- 2 如果要使用另一種有線網路組態，請按一下「管理連線」，然後新增另一種有線連線，如過程 26.1, “新增或編輯連線” [358頁] 中所述。
- 3 按一下 KNetworkManager 圖示，然後選取新設定的連線將其啟動。

26.4.2 管理無線網路連線

依預設，KNetworkManager 只會顯示已設定連線的無線網路，前提是這些無線網路既可以連接又未隱藏。第一次連接無線網路時，請執行下列步驟：

過程 26.2 連接至無線網路

- 1 按一下 Applet 圖示，然後選取「建立網路連線」。KNetworkManager 會顯示未隱藏並可連接的無線網路清單，還提供訊號強度和安全性的詳細資料。
- 2 若要連接至某個未隱藏的網路，請從清單中選取該網路，然後按一下「連接」。如果該網路已加密，則會開啓一個對話方塊。請選擇網路使用的「安全性」類型，然後輸入相應的身分證明。
- 3 若要連接到因不廣播服務設定識別碼 (SSID 或 ESSID) 而無法自動偵測到的網路，請選取「使用 WLAN 介面連接至其他網路」。
- 4 在開啟的對話方塊中，輸入 SSID 或 ESSID，並根據需要設定加密參數。
- 5 按一下「確定」確認您的變更。此時，NetworkManager 會啟動新連線。

- 6 若要終止連線並停用無線網路，請按一下 Applet 圖示，然後取消核取「啟用無線」。在飛機上或者在其他任何不允許使用無線網路的環境中，此方法很有用。

明確指定的無線網路會儘可能長久地保持連線狀態。如果在此期間插入網路線，則會連接已設定為「自動連接」的連線，而無線連線仍將延續。

26.4.3 將無線網路卡設定成存取點

如果您的無線網路卡支援存取點模式，您可以使用 NetworkManager 來設定組態。

注意：選項的可用性

在某些系統設定下，您可能無法設定連線。在安全環境中，某些選項可能會被鎖定，或者需要 `root` 許可權。請向您的系統管理員洽詢詳細資料。

- 1 按一下 NetworkManager Applet，然後選取「建立網路連線」>「新增 Ad-Hoc 網路」。
- 2 在隨後顯示的組態對話方塊中，於「SSID」欄位內輸入網路的名稱。

連線名稱(N): 新的無線網路連線

☐ 自動連線(A)

☐ 系統連線(S)

無線(W) | 無線安全性(E) | IP 位址(I)

SSID(D): 掃描(C)

模式(C): 臨時操作

BSSID(B):

限制介面(R): 任何

MTU(U): 自動

確定(O) 取消(C)

- 3 在「無線安全性」索引標籤中設定加密。

重要：不保護無線網路會帶來安全風險

如果將「安全性」設定為「無」，則所有人都可以連接到您的網路、重複使用您的連線並攔截您的網路連線。若要限制存取點的存取，並保全您的連線，請使用加密。您可以在各種 WEP 與基於 WPA 加密之間加以選擇。如果不確定哪一種技術最適合您，請參閱第 18.3 節「驗證」[209頁]。

- 4 在「IP 位址」索引標籤中，確定已將「設定」選項設為「分享」(ad-hoc 網路的預設選項)。
- 5 按一下「確定」確認您的組態。

26.4.4 自定 KNetworkManager

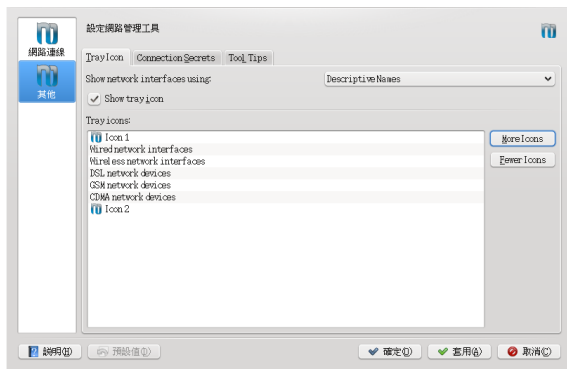
您可以自定 KNetworkManager 的某些設定，包括在系統匣中顯示的圖示數量、顯示的工具提示以及如何儲存網路連線的密碼和身分證明。如需最後一項設定的詳細資訊，請參閱第 26.7.2 節「儲存密碼與身份證明」[368頁]。

若要瞭解可用的選項，請在 NetworkManager 系統匣圖示上按一下滑鼠右鍵，選取「管理連線」，然後按一下組態對話方塊左側的「其他」。

過程 26.3 為 KNetworkManager 設定多個系統匣圖示

由於 KNetworkManager 可以同時讓多個連線處於使用中狀態，因此您可能需要快速瞭解多個連線的連線狀態。若是如此，您可以在系統匣中使用多個 NetworkManager 圖示，每個圖示都代表一組連線類型 (例如，一個圖示代表有線連線，另一個圖示代表無線連線)。

- 1 在組態對話方塊中，切換至「系統匣圖示」索引標籤。
- 2 按一下「更多圖示」。清單中即會顯示一個新圖示。
- 3 選取此圖示要代表的網路連線類型，然後將各種連線類型分組於對應的圖示下。



- 4 確認您的變更。

現在，系統匣中便會顯示多個 NetworkManager 圖示，透過圖示可以存取其關聯的連線類型。

設定網路連線 (如過程 26.1, “新增或編輯連線” [358頁] 中所述) 時, KNetworkManager 也可讓您自定為此連線顯示的圖示。若要變更圖示, 請按一下「**連線名稱**」旁邊的圖示按鈕, 並在隨後顯示的對話方塊中選取心儀的圖示。確認變更後按一下系統匣中的 KNetworkManager 圖示, 所顯示的可用連線清單中便會出現新的圖示。

26.5 使用 GNOME NetworkManager Applet

在 GNOME 中, 可以使用 GNOME NetworkManager Applet 控制 NetworkManager。如果已為 NetworkManager 控制設定了網路, 則 Applet 通常會於桌面環境啟動時自動啟動, 並會在系統匣中顯示一個圖示。

如果系統匣未顯示任何網路連線圖示, 則可能是 Applet 未啟動。按 Alt + F2 並輸入 nm-applet 可手動啟動。

26.5.1 管理有線網路連線

如果電腦已藉由網路纜線連接至現有網路, 請使用 NetworkManager applet 來選擇網路連接。

- 1 在 applet 圖示上按一下滑鼠左鍵, 以顯示可用網路的功能表。功能表中已選取的就是目前使用的連接。
- 2 若要切換到其他網路, 請先在清單中選擇該網路。
- 3 若要關閉所有網路連接 (無論是有線還是無線), 請在 applet 圖示上按一下滑鼠右鍵, 然後取消勾選「**啟用網路**」。

26.5.2 管理無線網路連線

可用的可見無線網路均列在「**無線網路**」下的 GNOME NetworkManager Applet 功能表中。每個網路的訊號強度也會顯示在功能表中。加密的無線網路以盾牌圖示標明。

過程 26.4 連接至無線網路

- 1 若要連接至某個無線網路，請按一下 Applet 圖示，然後從可用無線網路清單中選擇一項。
- 2 如果該網路已加密，則會開啓一個對話方塊。它會顯示網路使用的加密類型（「無線安全性」），並包含各種加密和驗證設定對應的多個輸入欄位。請輸入適當的身分證明。
- 3 若要連接到因不廣播服務設定識別碼 (SSID 或 ESSID) 而無法自動偵測到的網路，請在 NetworkManager 圖示上按一下滑鼠左鍵，然後選擇「*連接到隱藏的無線網路*」。
- 4 在開啟的對話方塊中，於「網路名稱」內輸入 SSID 或 ESSID，並根據需要設定加密參數。
- 5 若要停用無線網路，請在 Applet 圖示上按一下滑鼠右鍵，取消勾選「*啟用無線*」。在飛機上或者在其他任何不允許使用無線網路的環境中，此方法很有用。

明確指定的無線網路會儘可能長久地保持連線狀態。如果在此期間插入網路線，則會連接已設定為「*儘可能保持連接*」的連線，而無線連線仍將延續。

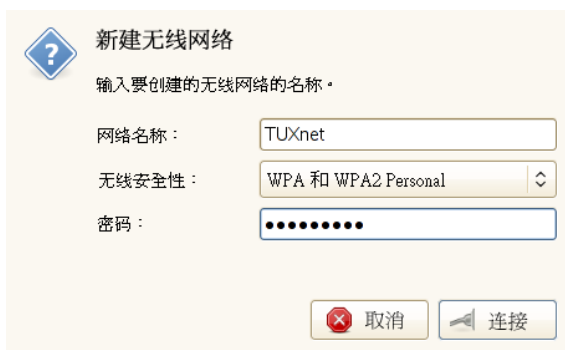
26.5.3 將無線網路卡設定成存取點

如果您的無線網路卡支援存取點模式，您可以使用 NetworkManager 來設定組態。

注意：選項的可用性

在某些系統設定下，您可能無法設定連線。在安全環境中，某些選項可能會被鎖定，或者需要 root 許可權。請向您的系統管理員洽詢詳細資料。

- 1 按一下 NetworkManager Applet，然後選取「*建立新的無線網路*」。



新建无线网络

输入要创建的无线网络的名称。

网络名称： TUXnet

无线安全性： WPA 和 WPA2 Personal

密码：

取消 连接

- 2 輸入「網路名稱」，然後透過「無線安全性」下拉式清單設定要使用的加密方式。

重要：不保護無線網路會帶來安全風險

如果將「無線安全性」設定為「無」，則所有人都可以連接到您的網路、重複使用您的連線並攔截您的網路連線。若要限制存取點的存取，並保全您的連線，請使用加密。您可以在各種 WEP 與基於 WPA 加密之間加以選擇。如果不確定哪一種技術最適合您，請參閱第 18.3 節「驗證」[209頁]。

26.6 NetworkManager 與 VPN

NetworkManager 支援多項虛擬私人網路 (VPN) 技術。對於每種技術，SUSE Linux Enterprise Server 都附帶了可為 NetworkManager 提供一般支援的基礎套件。除此之外，您還需要為 Applet 安裝相應的桌面專屬套件。

NovellVPN

若要使用此 VPN 技術，請安裝

- NetworkManager-novellvpn 與
- NetworkManager-novellvpn-kde4 或
NetworkManager-novellvpn-gnome。

目前尚不提供對 KDE 的 NovellVPN 支援，但研發人員正在努力。

OpenVPN

若要使用此 VPN 技術，請安裝

- NetworkManager-openvpn 與
- NetworkManager-openvpn-kde4 或 NetworkManager-openvpn-gnome。

vpnc (Cisco)

若要使用此 VPN 技術，請安裝

- NetworkManager-vpnc 與
- NetworkManager-vpnc-kde4 或 NetworkManager-vpnc-gnome。

PPTP (點對點通道通訊協定)

若要使用此 VPN 技術，請安裝

- NetworkManager-pptp 與
- NetworkManager-pptp-kde4 或 NetworkManager-pptp-gnome。

安裝完套件後，請依第 26.3 節「設定網路連線」[357頁]中所述設定 VPN 連線。

26.7 NetworkManager 和安全性

NetworkManager 將無線連線分為受信任和不受信任兩種。受信任的連線是過去您明確選取過的任何網路，除此以外的連線都屬於不受信任。受信任的連線以存取點的名稱和 MAC 位址來識別。使用 MAC 位址可確保別的存取點不能使用受信任連線的名稱。

NetworkManager 會定期掃描是否有可用的無線網路。如果找到多個受信任的網路，便自動選取最近使用的那個網路。如果所有網路都不受信任，NetworkManager 會等待您做出選擇。

如果加密設定變更，但名稱和 MAC 位址未變，NetworkManager 會嘗試進行連接，但它會先要求您確認新的加密設定並提供所有更新，例如新的金鑰。

如果從使用無線連線切換成離線模式，NetworkManager 會將 SSID 或 ESSID 設為空白。以確保該網路卡斷開連線。

26.7.1 使用者和系統連線

NetworkManager 可識別兩種類型的連線：使用者連線與系統連線。使用者連線是第一位使用者登入時 NetworkManager 可使用的連線，要求使用者提供所有必要的身份證明。使用者登出後，連線即會斷開，並從 NetworkManager 中移除。任何使用者登入之前，定義為系統連線的連線可由所有使用者共享，並且在 NetworkManager 啟動後即可使用。對於系統連線，必須在連線建立時提供所有身份證明。此類系統連線可用於自動連接要求驗證的網路。如需使用 NetworkManager 設定使用者連線或系統連線的相關資訊，請參閱第 26.3 節「設定網路連線」[357頁]。

對於 KDE，目前還不支援使用 NetworkManager 來設定系統連線，請使用 YaST。

26.7.2 儲存密碼與身份證明

如果您不希望每次連接加密網路時都要重新輸入身分證明，可以使用桌面專屬工具 GNOME 鑰匙圈管理員或 KWalletManager，將加密的身分證明儲存在磁碟中，並以主密碼加以保護。

NetworkManager 也可從憑證儲存區取回安全連線 (例如，加密的有線、無線或 VPN 連線) 的憑證。如需詳細資訊，請參閱第 12 章「*Certificate Store*」(↑*Security Guide*)。

26.8 常見問題解答

以下提供了有關使用 NetworkManager 設定特殊網路選項的常見問題。

如何將連線關聯到特定設備？

依預設，NetworkManager 中的連線是特定於設備類型的：它們適用於相同類型的所有實體設備。如果一種連線類型對應多個實體設備 (例如，您的機器配有兩個乙太網路卡)，可以將連線關聯到特定的設備。

若要在 GNOME 中執行此動作，請先使用 Applet 中的「連線資訊」，或使用指令行工具 (如 nm-tool 或 ifconfig) 的輸出，來查詢設備的 MAC 位

址。然後開啟用於設定網路連線的對話方塊，並選擇要修改的連線。在「有線」或「無線」索引標籤中輸入設備的「*MAC 位址*」，並確認您的變更。

如果使用的是 **KDE**，則啟動用於設定網路連線的對話方塊，然後選擇要修改的連線。在「乙太網路」或「無線」索引標籤中，使用「*限制介面*」選項，選取連線要關聯的網路介面。

在偵測到多個存取點具有相同 **ESSID** 的情況下，如何指定特定的存取點？

如果有具有不同無線頻段 (a/b/g/n) 的多個存取點可用，系統預設會自動選擇訊號最強的存取點。要置換此存取點，請在設定無線連線時使用「*BSSID*」欄位。

基本服務組識別碼 (**BSSID**) 可唯一識別每個基本服務組。在基礎結構基本服務組中，**BSSID** 是無線存取點的 *MAC 位址*。在獨立的 (臨機操作) 基本服務組中，**BSSID** 是由 46 位元隨機數字產生的本地管理的 *MAC 位址*。

依照第 26.3 節「設定網路連線」[357頁] 中所述啟動用於設定網路連線的對話方塊。選擇要修改的無線連線，然後按一下「*編輯*」。在「無線」索引標籤中，輸入 **BSSID**。

如何與其他電腦共享網路連線？

主要設備 (連接至網際網路的設備) 不需要任何特殊組態。不過，您需要以如下方式設定連接至本地 **Hub** 或機器的設備：

1. 依照第 26.3 節「設定網路連線」[357頁] 中所述啟動用於設定網路連線的對話方塊。選擇要修改的連線，然後按一下「*編輯*」。如果使用的是 **GNOME**，則切換到「*IPv4 設定*」索引標籤，然後從「方法」下拉式清單中，選擇「*分享給其他電腦*」。如果使用的是 **KDE**，則切換到「*IP 位址*」索引標籤，然後從「設定」下拉式清單中，選擇「*分享*」。這樣可讓 IP 流量轉遞並會執行設備上的 **DHCP** 伺服器。確認您在 **NetworkManager** 中所做的變更。
2. 由於 **DCHP** 伺服器使用連接埠 67，請確定防火牆未封鎖此連接埠：在共享連線的機器上啟動 **YaST**，然後選取「*安全性與使用者*」>「*防火牆*」。切換到「*允許的服務*」類別。如果「*DCHP 伺服器*」尚未顯示為「*允許的服務*」，則從「*要允許的服務*」中選取「*DCHP 伺服器*」，然後按一下「*新增*」。確認您在 **YaST** 中所做的變更。

如何使用動態位址 (**DHCP**、**PPP** 與 **VPN**) 提供靜態 **DNS** 資訊？

如果 **DHCP** 伺服器提供的 **DNS** 資訊 (與/或路由) 無效，則可將其置換。依照第 26.3 節「設定網路連線」[357頁] 中所述啟動用於設定網路連線的對話

方塊。選擇要修改的連線，然後按一下「編輯」。如果使用的是GNOME，則切換到「IPv4 設定」索引標籤，然後從「方法」下拉式清單中，選擇「只用自動 (DHCP) 位址」。如果使用的是KDE，則切換到「IP 位址」索引標籤，然後從「設定」下拉式清單中，選擇「只有自動 (DHCP) 位址」。在「DNS 伺服器」與「搜尋網域」欄位中輸入DNS資訊。若要「忽略自動取得的路由設定」，請按一下「路由」(GNOME) 並啟動對應的核取方塊，或從索引標籤 (KDE) 底部的下拉式選單中選取「路由」並啟動對應的核取方塊。確認您的變更。

如何在使用者登入之前將 NetworkManager 連接到受密碼保護的網路？
定義用於此目的的系統連線。如需詳細資訊，請參閱第 26.7 節「NetworkManager 和安全性」[367頁]。

26.9 疑難排解

可能發生連線問題。與 NetworkManager 相關的一些常見問題有：Applet 未啟動或缺少 VPN 選項。解析和預防這些問題的方法會視使用的工具而定。

NetworkManager Desktop Applet 不啟動

為 NetworkManager 控制設定網路之後，GNOME 和 KDE NetworkManager Applet 會自動啟動。如果不啟動，請如第 26.2 節「啟用或停用 NetworkManager」[356頁]中所述，檢查 YaST 中的 NetworkManager 是否已啟用。然後確定針對桌面環境的相應套件是否也已安裝。如果使用的是KDE 4，則套件為 NetworkManager-kde4。針對 GNOME 使用者的套件為 NetworkManager-gnome。

如果桌面 Applet 已安裝，但因為某些原因而不執行，您可以用手動方式啟動。如果安裝了桌面 Applet，但其由於某些原因並未執行，請使用 nm-applet (GNOME) 或 knetworkmanager (KDE) 指令手動將其啟動。

NetworkManager Applet 不包含 vpn 選項

針對 NetworkManager 的支援、Applet 與適用於 NetworkManager 的 VPN 均在各自獨立套件中發佈。如果您的 NetworkManager Applet 不包含 VPN 選項，請檢查是否安裝了為VPN技術提供NetworkManager支援的套件。如需詳細資訊，請參閱第 26.6 節「NetworkManager 與 VPN」[366頁]。

無可用的網路連線

如果已正確設定網路連線，且網路連線的所有其他元件 (路由器等) 也均已設定並正在執行中，有時需要重新啟動電腦的網路介面。若要執行此操作，請以 root 身份登入指令行並執行 `rcnetwork restart`。

26.10 如需更多資訊

您可以在下列網站和目錄中找到更多有關 NetworkManager 的資訊：

NetworkManager 專案頁面

<http://projects.gnome.org/NetworkManager/>

KDE NetworkManager 前端

<http://userbase.kde.org/NetworkManagement>

套件文件

另請參閱下列目錄中有關 NetworkManager、GNOME 與 KDE NetworkManager Applet 的最新資訊：

- `/usr/share/doc/packages/NetworkManager/`,
- `/usr/share/doc/packages/NetworkManager-kde4/` 和
- `/usr/share/doc/packages/NetworkManager-gnome/`。

Samba

使用 Samba 可以將 Unix 機器設定為 Mac OS X、Windows 以及 OS/2 機器的檔案與列印伺服器。Samba 已經是一個開發至完全成熟且相當複雜的產品。使用 YaST、SWAT (一種 Web 介面)，或透過手動編輯組態檔的方式設定 Samba。

27.1 術語

下列為 Samba 文件和 YaST 模組中常用的詞彙。

SMB 通訊協定

Samba 使用基於 NetBIOS 服務的 SMB (伺服器訊息區塊) 通訊協定。由於 Microsoft 發行了此通訊協定，因此其他的軟體製造商可以建立連接至 Microsoft 網域網路的連線。使用 Samba，SMB 通訊協定就可以在 TCP/IP 通訊協定上運作，因此 TCP/IP 通訊協定必須安裝在所有的用戶端上。

提示：IBM System z：NetBIOS 支援

IBM System z 僅支援 TCP/IP 上的 SMB。在這些系統上不提供 NetBIOS 支援。

CIFS 通訊協定

CIFS (一般網際網路檔案系統) 通訊協定是 Samba 所支援的另一種通訊協定。CIFS 定義用於網路上的標準遠端檔案系統存取通訊協定，讓使用者群組可以透過網路分工合作和共享文件。

NetBIOS

NetBIOS 是用來在提供名稱服務的機器之間進行通訊的軟體介面 (API)。它允許連接至網路的機器保留自己的名稱。在保留後，就可以使用名稱來定址這些機器。在此沒有檢查名稱的中央程序。在網路上的任何機器都可以保留它所需的任何數量名稱，只要這些名稱尚未使用。可以針對不同的網路結構實作 NetBIOS 介面。有一個與網路硬體一起緊密運作的執行程序，稱為 NetBEUI，不過這通常稱為 NetBIOS。與 NetBIOS 一起執行的網路通訊協定是 Novell 的 IPX (經由 TCP/IP 的 NetBIOS) 與 TCP/IP。

經由 TCP/IP 所傳送的 NetBIOS 名稱，與 `/etc/hosts` 中所使用的名稱，或由 DNS 所定義的名稱完全不相同。NetBIOS 使用自己完全獨立的命名慣例。不過，一般建議使用與 DNS 主機名稱相對應的名稱，如此可使管理較為輕鬆，或者可本地使用 DNS。Samba 預設是使用此對應名稱。

Samba 伺服器

Samba 伺服器可為用戶端提供 SMB/CIFS 服務和 NetBIOS over IP 命名服務。對於 Linux 系統，Samba 伺服器有三種精靈可用：`smbd` (用於 SMB/CIFS 服務)、`nmbd` (用於命名服務) 及 `winbind` (用於驗證)。

Samba 用戶端

Samba 用戶端是透過 SMB 通訊協定，使用 Samba 伺服器所提供之 Samba 服務的系統。所有一般的作業系統 (例如 Mac OS X、Windows 以及 OS/2) 都支援 SMB 通訊協定。TCP/IP 通訊協定必須安裝在所有的電腦上。Samba 提供適用於不同 UNIX 類別的用戶端。就 Linux 而言，有一個 SMB 的核心模組，允許在 Linux 系統層級上整合 SMB 資源。您不必為 Samba 用戶端執行任何精靈。

共享

SMB 伺服器透過共享方式向用戶端提供資源。共享是指印表機和位在伺服器上的目錄及其子目錄。它是利用名稱來輸出，並且可藉由其名稱來存取。共享名稱可以設成任何名稱——它並不需是輸出目錄的名稱。也會指定一個名稱給印表機。用戶端可以透過其名稱存取印表機。

DC

領域控制器 (DC) 是處理網域中帳戶的伺服器。進行資料複製時，可在一個網域中使用其他領域控制器。

27.2 啟動和停止 Samba

您可以在開機時自動啟動 Samba 伺服器，也可以手動啟動或停止。啟動和停止原則是 YaST Samba 伺服器組態的一部分 (如第 27.3.1 節「使用 YaST 設定 Samba 伺服器」[375頁] 所述)。

若要使用 YaST 停止或啟動執行中的 Samba 伺服器，請使用「系統」>「系統服務 (執行層級)」，然後檢查 winbind、smb 與 nmb。在指令行中使用 `rcsmb stop && rcnmb stop` 可停止 Samba 所需的服務，使用 `rcnmb start && rcsmb start` 可啟動這些服務；必要時，rcsmb 會參考 winbind 的結果。

27.3 設定 Samba 伺服器

SUSE® Linux Enterprise Server 中的 Samba 伺服器可以兩種方式設定：使用 YaST 設定或手動設定。手動設定組態可以提供較詳細的設定，但是缺乏 YaST GUI 提供的方便性。

27.3.1 使用 YaST 設定 Samba 伺服器

若要設定 Samba 伺服器，請啟動 YaST 並選取「網路服務」>「*Samba 伺服器*」。

27.3.1.1 初始的 Samba 組態

第一次啟動模組時，系統會啟動「*Samba 安裝*」對話方塊，提示您對伺服器管理進行一些基本設定。組態設定結束時，系統會提示您輸入 Samba 管理員密碼 (「*Samba root 使用者密碼*」)。之後再啟動該模組時，會顯示「*Samba 組態*」對話方塊。

「*Samba 安裝*」對話方塊包含兩個步驟與一些選擇性的詳細設定：

工作群組或網域名稱

在「工作群組或網域名稱」中選取現有的名稱，或輸入新的名稱，並按一下「下一步」。

Samba 伺服器類型

在下一步中，指定伺服器是應該做為主要網域控制器 (PDC)、備份網域控制器 (BDC) 還是根本不做為網域控制器。按「**下一步**」繼續。

如果不想繼續設定伺服器的詳細組態，請按一下「**確定**」確認。然後，在最後一個快顯方塊中設定「*Samba root 使用者密碼*」。

之後可在「*Samba 組態*」對話方塊的「**啟動**」、「**共享**」、「**身分**」、「**信任的網域**」與「**LDAP 設定**」索引標籤中變更所有設定。

27.3.1.2 進階 Samba 組態

第一次啟動 Samba 伺服器模組時，執行第 27.3.1.1 節「**初始的 Samba 組態**」[375頁]中所述的兩個初始步驟後，「*Samba 組態*」對話方塊會直接顯示。用此調整您的 Samba 伺服器組態。

編輯組態後，按一下「**確定**」儲存設定。

啟動伺服器

在「**啟動**」索引標籤中，設定 Samba 伺服器的啟動。若每次系統開機時都要啟動服務，請選取「**開機時**」。若要啟用手動啟動，請選擇「**手動**」。如需有關啟動 Samba 伺服器的詳細資訊，請參閱第 27.2 節「**啟動和停止 Samba**」[375頁]。

在此索引標籤中，您也可以開啟您的防火牆中的連接埠。若要執行此動作，請選取「**在防火牆中開啟埠**」。如果您有多個網路介面，請按一下「**防火牆詳細資訊**」，選取介面，並按一下「**確定**」來選取 Samba 服務的網路介面。

共享

在「**共享**」索引標籤中，決定要啟用的 Samba 共享。標籤中有一些預先定義的共同，如 **home** 和 **printer**。使用「**切換狀態**」以切換「**作用中**」與「**非作用中**」。按一下「**新增**」可新增新的共享，按一下「**刪除**」可刪除選取的共享。

「**允許使用者共享自己的目錄**」讓「**許可的群組**」中的群組成員能與其他使用者共享自己的目錄。例如：**users** 針對本地範圍，**DOMAIN\Users** 針對網域範圍。使用者還必須確定檔案系統的許可權允許存取。請使用「**最多共享數**」限制可建立的共享總數。若要允許在沒有驗證的情況下存取使用者共享，請啟用「**允許訪客存取**」。

識別

在「身分」索引標籤中，您可以決定主機關聯的網域（「基本設定」），以及是否要在網路中使用替代的主機名稱（「*NetBIOS* 主機名稱」）。也可以使用 Microsoft Windows 網際網路名稱服務 (WINS) 進行名稱解析。在這種情況下，請啟用「使用 *WINS* 解析主機名稱」，並決定是否「透過 *DHCP* 取回 *WINS* 伺服器」。若要設定進階全域設定或使用者驗證來源（例如 LDAP 而非 TDB 資料庫），請按一下「進階設定」。

信任的網域

若要讓其他網域的使用者存取您的網域，請在「信任的網域」索引標籤中進行適當的設定。若要新增網域，請按一下「新增」。若要移除所選網域，請按一下「移除」。

LDAP 設定

在索引標籤「*LDAP* 設定」中，您可決定 LDAP 伺服器是否使用驗證。若要測試 LDAP 伺服器的連線，請按一下「測試連線」。若要查看進階 LDAP 設定或使用者預設值，請按一下「進階設定」。

如需 LDAP 組態的詳細資訊，請參閱第 4 章「*LDAP—A Directory Service*」(†*Security Guide*)。

27.3.2 使用 SWAT 管理網頁

另一種管理 Samba 伺服器的工具是 SWAT (Samba Web Administration Tool, Samba 網頁管理工具)。它提供簡單的網頁介面，以用於設定 Samba 伺服器。若要使用 SWAT，請在網頁瀏覽器中開啟 <http://localhost:901>，並以 root 使用者的身分登入。如果您沒有特殊的 Samba root 帳戶，請使用系統的 root 帳戶。

注意：啟用 SWAT

安裝 Samba 伺服器後，並不會啟用 SWAT。若要啟用 SWAT，請在 YaST 中開啟「網路服務」>「網路服務 (*xinetd*)」，啟用網路服務組態，選取表格中的「*swat*」，並按一下「切換狀態 (開啟或關閉)」。

27.3.3 手動設定伺服器

如果您想要使用 Samba 做為伺服器，請安裝 `samba`。Samba 的主要組態檔為 `/etc/samba/smb.conf`。這個檔案可以分成兩個邏輯部份。`[global]` 區段包含中央與全域設定值。`[share]` 區段包含個別檔案與印表機共享。利用此方法，就可以在 `[global]` 區段中以不同的方式或以全域方式設定關於共享的細節，它可以加強組態檔的結構透明化。

27.3.3.1 全域區段

下列 `[global]` 區段的參數需要做一些調整，以符合網路設定的需求，讓其他機器可以透過 Windows 環境中的 SMB 存取 Samba 伺服器。

```
workgroup = TUX-NET
```

這一行是將 Samba 伺服器指定給工作群組。以網路環境中適當的工作群組取代 TUX-NET。Samba 伺服器會以其 DNS 名稱顯示，除非此名稱已指定給網路中的其他機器。如果沒有可用的 DNS 名稱，請使用

`netbiosname=MYNAME` 設定伺服器名稱。如需更多有關此參數的詳細資料，請參閱 `smb.conf` **man** 頁面。

```
os level = 20
```

此參數會觸發 Samba 伺服器是否嘗試變成其工作群組的 LMB (本地主要的瀏覽器)。對於 Samba 3 版本系列，通常不需要覆寫預設設定 (20)。選擇一個極小值 (例如 2) 可以讓現有的 Windows 網路免受因 Samba 伺服器設定不當而造成的任何干擾。有關此重要主題的詳細資訊，可參閱《Samba 3 Howto》中的「Network Browsing」(網路瀏覽) 一章；如需有關《Samba 3 Howto》的詳細資訊，請參閱第 27.7 節「如需更多資訊」[385頁]。

如果網路中沒有其他的 SMB 伺服器 (例如，Windows 2000 伺服器)，而且您希望 Samba 伺服器保留本地環境中存在的所有系統的清單，請將 `os level` 設成更高的值 (例如，65)。接著就會將 Samba 伺服器選擇成本地網路的 LMB。

當變更此設定值時，請小心地考慮這個值將會如何影響現有的 Windows 網路環境。首先請在獨立的網路中或在一天中非重要的時間測試變更。

wins support 與 wins server

若要將 Samba 伺服器整合至含有主動 WINS 伺服器的現有 Windows 網路中，請啟用 wins server 選項，並將其值設為該 WINS 伺服器的 IP 位址。

如果您的數台 Windows 機器連接至不同的子網路，但仍然需要看到彼此，則您需要設定 WINS 伺服器。若要將 Samba 伺服器變成像這樣的 WINS 伺服器，請設定 wins support = Yes 選項。請確定網路中只有一個 Samba 伺服器啟用了這個設定值。wins server 與 wins support 選項絕不能在 smb.conf 檔案中同時啟用。

27.3.3.2 共享

下列範例說明如何將 CD-ROM 光碟機與使用者目錄 (homes) 開放給 SMB 用戶端使用。

[cdrom]

若要避免不小心將 CD-ROM 光碟機開放成共享，請以備註符號停用這些行 (在此例中為分號)。請在第一個資料欄中移除分號，以便和 Samba 共享 CD-ROM 光碟機。

範例 27.1 CD-ROM 共享(已停用)

```
[cdrom]
;      comment = Linux CD-ROM
;      path = /media/cdrom
;      locking = No
```

[cdrom] and comment

[cdrom] 區段項目是網路上所有 SMB 用戶端都可以看到之共享的名稱。可以另外再加入一個 comment，以進一步描述共享。

```
path = /media/cdrom
path 會輸出 /media/cdrom 目錄。
```

利用限制非常嚴格的預設組態，就可以將這種共享只開放給出現在此系統上的使用者共享。如果這個共享應該開放每個人使用，請將 guest ok = yes 加入組態。這個設定值可以將讀取權限開放給網路上的每個人使用。建議您處理此參數時必須極為小心。這將會在 [global] 區段中套用更多此參數的使用。

[homes]

[homes] 共享在這裡特別重要。如果使用者擁有 Linux 檔案伺服器以及其自己主目錄的有效帳戶與密碼，就可以連接到主目錄。

範例 27.2 [homes] 共享

```
[homes]
comment = Home Directories
valid users = %S
browseable = No
read only = No
create mask = 0640
directory mask = 0750
```

[homes]

只要沒有其他的共享，使用共享的使用者名稱連接至 SMB 伺服器，就會使用 [homes] 共享指示來動態產生共享。共享的產生名稱是使用者名稱。

```
valid users = %S
```

只要成功地建立連接，就會以共享的具體名稱取代 %S。[homes] 共享，永遠為使用者名稱。因此，對使用者共享的存取權限僅限於該使用者。

```
browseable = No
```

這個設定值讓共享在網路環境變成無形的。

```
read only = No
```

根據預設，Samba 會利用 read only = Yes 參數，以禁止寫入任何輸出共享的權限。若要開放共享為可寫入的，請設定 read only = No 的值，這與 writable = Yes 同義。

```
create mask = 0640
```

以 MS Windows NT 為基礎的系統將無法理解 UNIX 權限的概念，因此在建立檔案時，它們將無法指定權限。create mask 參數可以定義指定給新建立檔案的存取權限。這只會套用至可寫入的共享。實際上，這個設定值表示擁有者具有讀取與寫入權限，而擁有者的主要群組成員則具有讀取權限。valid users = %S 可以在即使群組具有讀取權限時禁止讀取權限。若想要使群組具有讀取或寫入權限，請停用 valid users = %S 一行。

27.3.3.3 安全性層級

為了提高安全性，每個共享存取權都以密碼保護。SMB 提供下列幾種權限檢查方式：

共享層級安全性 (安全性 = 共享)

每個共享都必須指定密碼。每個知道此密碼的人員都具有該共享的存取權。

使用者層級安全性 (安全性 = 使用者)

此變體在 SMB 中引入了使用者概念。每個使用者都必須以自己的密碼註冊伺服器。在註冊後，伺服器可以視使用者名稱將存取權授予個別輸出的共享。

伺服器層級安全性 (安全性 = 伺服器)

對其用戶端而言，Samba 會模擬在使用者層級模式中工作。不過，它會將所有的密碼查詢傳遞給另一個將會處理驗證的使用者層級模式伺服器。此設定需要用到另一個密碼伺服器參數。

ADS 層級安全性 (安全性 = ADS)

在這種模式下，Samba 在 Active Directory 環境中以網域成員的身分執行。要以此模式作業，執行 Samba 的機器需要安裝與設定 Kerberos。您必須讓使用 Samba 的機器加入 ADS 領域。可使用 YaST 的「Windows 網域成員」模組完成此操作。

網域層級安全性 (安全性 = 網域)

僅在機器已加入到 Windows NT 網域時，此模式才會正常工作。Samba 將嘗試驗證使用者名稱與密碼，方法是將其傳送至 Windows NT 主網域或備份網域控制器。這與 Windows NT 伺服器用來驗證的方法相同。需要將加密密碼參數設定為 yes。

共享、使用者、伺服器或網域層級安全性的選項會套用至整部伺服器。因為無法針對伺服器組態的個別共享提供共享層級的安全性，並針對其他的共享提供使用者層級的安全性。然而，您可以針對系統上每個設定的 IP 位址執行個別的 Samba 伺服器。

在《Samba 3 HOWTO》中可以找到關於此主題的詳細資訊。至於在一個系統上的多個伺服器，請注意 interfaces 與 bind interfaces only 選項。

27.4 設定用戶端

用戶端只能透過 TCP/IP 存取 Samba 伺服器。NetBEUI 與透過 IPX 的 NetBIOS 無法與 Samba 一起使用。

27.4.1 使用 YaST 設定 Samba 用戶端

設定 Samba 用戶端以存取 Samba 或 Windows 伺服器上的資源 (檔案或印表機)。在「網路服務」>「Windows 網域成員」對話方塊中輸入 NT 或 Active Directory 網域或工作群組。如果您啟用了「Linux 驗證也使用 SMB 資訊」，則使用者驗證將會在 Samba、NT 或 Kerberos 伺服器上執行。

按一下「進階設定」可以指定進階組態選項。例如，使用「安裝伺服器目錄」表格可設定在驗證時自動掛接伺服器主目錄。這樣，當使用者的主目錄在 CIFS 上託管時，他們便可以存取這些目錄。如需詳細資料，請參閱 `pam_mount` man 頁面。

完成所有設定之後，在對話方塊中進行確認以完成組態設定。

27.5 做為登入伺服器的 Samba

在以 Windows 用戶端為主的網路中，通常會建議使用者只註冊一個有效的帳戶與密碼。在以 Windows 為基礎的網路中，這個任務是由主要網域控制器 (PDC) 來處理。您可以使用已設定為 PDC 的 Windows NT 伺服器，但也可借助 Samba 伺服器完成此任務。在 `smb.conf` 的 `[global]` 區段中必須編輯的項目如範例 27.3 「在 `smb.conf` 中的全域區段」[382頁] 所示。

範例 27.3 在 `smb.conf` 中的全域區段

```
[global]
    workgroup = TUX-NET
    domain logons = Yes
    domain master = Yes
```

如果使用加密密碼進行驗證，則 Samba 伺服器必須能夠處理這些密碼。在 `[global]` 區段中的 `encrypt passwords = yes` 項目可以啟用此功能 (加上 Samba 版本 3，現在這個是預設值)。除此之外，必須準備符合 Windows 加密

格式的使用者帳戶與密碼。此操作可使用指令 `smbpasswd -a name` 來完成。使用下列指令為電腦建立網域帳戶 (Windows 網域概念所需)：

```
useradd hostname\$\n  
smbpasswd -a -m hostname
```

使用 `useradd` 指令，就會加上貨幣符號。當使用 `-m` 參數時，`smbpasswd` 指令就會自動插入這個符號。加備註的組態範例 (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) 包含一些設定，可讓此任務自動執行。

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \n  
-s /bin/false %m\$\n
```

為確保 Samba 可正確執行此程序檔，請選擇擁有所需之管理員權限的 Samba 使用者，並將其新增至 `ntadmin` 群組。這樣就可以透過下列指令將 `Domain Admin` 狀態指定給此 Linux 群組內的所有使用者：

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

如需有關此主題的詳細資訊，請參閱《Samba 3 HOWTO》(`/usr/share/doc/packages/samba/Samba3-HOWTO.pdf`) 的第 12 章。

27.6 含 Active Directory 的網路中之 Samba 伺服器

若您同時執行 Linux 伺服器與 Windows 伺服器，您可建立兩個獨立的驗證系統與網路，或將兩部伺服器透過一個中央驗證系統連接到一個網路。由於 Samba 可與 active directory 網域共同運作，因此您可將 SUSE Linux Enterprise Server 加入 Active Directory (AD) 中。

加入現有 AD 網域的動作可以在安裝期間進行，也可以後來藉由在安裝好的系統中使用 YaST 啟動 SMB 使用者驗證來進行。安裝時加入網域的說明可在第 6.16.1.7 節「使用者驗證方式」(第 6 章「使用 YaST 安裝」, ↑部署指南) 中找到。

若要在運作中的系統加入 AD 網域，請執行下列步驟：

- 1 以 `root` 身分登入並啟動 YaST。
- 2 啟動「網路服務」>「Windows 網域成員」。

3 在「*Windows 領域成員*」畫面的「*領域或工作群組*」中輸入要加入的領域。

圖形 27.1 決定 *Windows 網域成員*

4 勾選「*Linux 驗證也使用 SMB 資訊*」，以在 SUSE Linux Enterprise Server 上使用 SMB 來源進行 Linux 驗證。

5 按一下「*確定*」，並在出現提示時確認要加入網域。

6 為 Windows 管理員提供 AD 伺服器上的密碼，並按一下「*確定*」。

您的伺服器現在已可使用 Active Directory 網域控制器上的所有驗證資料。

27.7 如需更多資訊

可在數位文件中取得更多有關 Samba 的資訊。如果已安裝 Samba 文件，若要取得更多的線上文件與範例，請在指令行輸入 `apropossamba` 以顯示一些手冊頁或直接瀏覽 `/usr/share/doc/packages/samba` 目錄。在 `examples` 子目錄中尋找加有備註的範例組態 (`smb.conf.SuSE`)。

《Samba 3 HOWTO》由 Samba 團隊提供，包含疑難排解一節。除此之外，文件的第五部份提供檢查組態的逐步指南。安裝 `samba-doc` 套件後，可以在 `/usr/share/doc/packages/samba/Samba3-HOWTO.pdf` 中找到《Samba 3 HOWTO》。

使用 NFS 共享檔案系統

透過網路配送和共享檔案系統在公司環境中極為常見。這種成熟的網路檔案系統 (NFS) 可與 NIS (黃頁通訊協定) 搭配使用。如需可與 LDAP 搭配使用並且還要使用 Kerberos 的更安全通訊協定，請選擇 NFSv4。若與 pNFS 結合使用，可以消除效能瓶頸。

NFS 與 NIS 攜手能讓使用者對網路有清楚的瞭解。可以使用 NFS 透過網路配送任意檔案系統。如果安裝妥當，使用者將會發現，不論他們目前使用的是哪個終端機，他們始終處於同一個環境中。

重要：DNS 所需

原則上，可以只使用 IP 位址來進行所有的輸出。為了避免逾時，您需要有正常運作的 DNS 系統。即使為了記錄目的，DNS 也必不可少，因為掛接的精靈執行的是反向查詢。

28.1 術語

YaST 模組中使用了下列詞彙。

輸出

由 NFS 伺服器輸出的目錄，用戶端可將該目錄整合到其系統中。

NFS 用戶端

NFS 用戶端是指透過「網路檔案系統」通訊協定使用 NFS 伺服器提供之 NFS 服務的系統。TCP/IP 通訊協定已整合到 Linux 核心中；不需要安裝任何其他軟體。

NFS 伺服器

NFS 伺服器向用戶端提供 NFS 服務。執行中的伺服器依賴於下列精靈運作：nfsd (工作者)、idmapd (使用者及群組名稱至 ID 的映射，反之亦然)、statd (檔案鎖定) 及 mountd (掛接要求)。

pNFS

平行 NFS，NFSv4 的通訊協定延伸。所有 pNFS 用戶端都可以直接存取 NFS 伺服器上的資料。

28.2 安裝 NFS 伺服器

在進行預設安裝時並不會安裝 NFS 伺服器軟體。如果依第 28.3 節「設定 NFS 伺服器」[388頁] 中所示設定 NFS 伺服器，系統會自動提示您安裝必要的套件。或者，使用 YaST 或 zypper 安裝套件 `nfs-kernel-server`。

NFS 與 NIS 一樣，都是主從式系統。但一台機器可同時扮演這兩種角色——它可透過網路提供檔案系統 (輸出)，也可以從其他主機掛接檔案系統 (輸入)。

28.3 設定 NFS 伺服器

NFS 伺服器可透過 YaST 來設定，也可以手動設定。若要進行驗證，還可以將 NFS 與 Kerberos 結合使用。

28.3.1 以 YaST 輸出檔案系統

使用 YaST，將您網路中的主機轉變為 NFS 伺服器，此類伺服器可將目錄和檔案輸出到所有擁有存取權的主機。該伺服器還可為群組的所有成員提供應用程式，這樣就不必逐個在每部主機本地安裝這些應用程式。

若要設定這樣的伺服器，請執行下列步驟：

過程 28.1 設定 NFSv3 伺服器

- 1 啟動 YaST 並選取「網路服務」>「NFS 伺服器」；請參閱圖形 28.1 「NFS 伺服器組態工具」[389頁]。系統可能會提示您安裝其他軟體。

圖形 28.1 NFS 伺服器組態工具

NFS 伺服器組態

NFS 伺服器

☒ 啟動(S)

☐ 不要啟動(N)

防火牆

☐ 在防火牆中開啟埠(F) 防火牆組態(O)...

防火牆埠已關閉

啟用 NFSv4

☒ 啟用 NFSv4(Y)

輸入 NFSv4 相連名稱(N):

localdomain

☐ 啟用 GSS 安全性(G)

說明 取消(C) 上一步(B) 下一步(N)

- 2 啟用「開始」選項圓鈕。
- 3 如果系統上的防火牆 (SuSEfirewall2) 處於使用中狀態，請核取「在防火牆中開啟連接埠」。YaST 會啟用 `nfs` 服務來調整其組態以適用於 NFS 伺服器。
- 4 保持「啟用 NFSv4」核取方塊處於停用狀態。
- 5 若您需要安全存取伺服器，請按一下「啟用 GSS 安全性」。先決條件是您的網域中安裝有 Kerberos，且伺服器和用戶端都可進行 Kerberos 驗證。按一下「下一步」。
- 6 按一下對話方塊上半部分中的「新增目錄」以輸出目錄。
- 7 如果您尚未設定允許的主機，系統會自動彈出另一個對話方塊，可讓您輸入用戶端資訊及選項。輸入主機萬用字元 (通常您可以保留預設設定不變)。

有四種主機萬用字元類型可讓您針對各主機進行設定：單一主機 (名稱或 IP 位址)、網路群組、萬用字元 (例如 * 標是所有機器都可存取伺服器) 以及 IP 網路。

8 按一下「完成」以完成組態。

28.3.1.1 NFSv4 用戶端的輸出

對於固定的 NFSv4 用戶端集合來說，能輸出的目錄有兩種類型—做為虛擬根檔案系統的目錄，以及結合至虛擬檔案系統之某些子目錄的目錄。虛擬檔案系統可做為基礎點，底下所有為這些用戶端集合而輸出的檔案系統都有其位置。對於用戶端或用戶端集合來說，伺服器上只有一個目錄可以設定為虛擬根部來進行輸出。針對此用戶端，可將多個目錄結合至虛擬根中某些現有子目錄來輸出它們。

舉例來說，假設目錄 `/exports` 被選為所有可存取伺服器之用戶端的虛擬根部目錄。然後請將其加入輸出目錄的清單，並確定針對此目錄所輸入的選項包含了 `fsid=0`。如果另一個目錄 (`/data`) 也需要使用 NFSv4 輸出，請將該目錄也新增至清單中。針對此狀況輸入選項時，請確定 `bind=/exports/data` 位於清單中，而且 `/exports/data` 是 `/exports` 的現有子目錄。
`bind=/target/path` 選項中的任何變更 (不論是新增、刪除還是變更值) 都會反映在「結合掛接目標」中。

若要設定伺服器以輸出 NFSv4 用戶端的目錄，請使用過程 28.1, “設定 NFSv3 伺服器” [389頁] 中的一般指南，但要變更下列步驟：

- 1 在第一個對話方塊中核取「啟用 NFSv4」。
- 2 在第一個對話方塊中輸入適當的 NFSv4 網域名稱。

請確定該名稱與存取此特定伺服器的 NFSv4 用戶端之 `/etc/idmapd.conf` 檔案中的一個名稱相同。此參數適用於 `idmapd` 精靈，而此精靈在支援 (伺服器和用戶端二者的) NFSv4 時是必要的。如果您沒有任何特殊需求，則請讓它維持為 `localdomain` (預設)。

按「下一步」後出現的對話方塊有兩個區段。上半部有兩欄，分別稱為「目錄」和「結合掛接目標」。該服務將立即可用。

3 按一下對話方塊上半部分中的「**新增目錄**」以輸出目錄，然後按一下「**確定**」進行確認。

4 在「**主機萬用字元**」文字欄位和選項中輸入您的主機名稱。

在「**選項**」文字欄位中，將 `fsid=0` 加入逗號分隔的選項清單，以將目錄設為虛擬根目錄。如果此目錄需要繫結至某個已設定之虛擬根部下的目錄，請確定已使用 `bind=/target/path` 在選項清單中提供目標繫結路徑。

「**結合掛接目標**」欄無法直接編輯，只是列出目錄及其屬性。

5 按一下「**完成**」以完成組態。

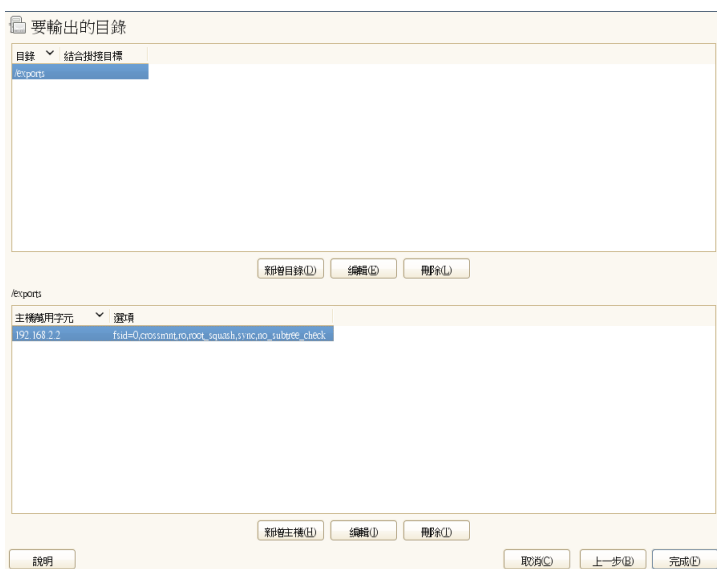
28.3.1.2 NFSv3 和 NFSv2 的輸出

請在按一下「**下一步**」之前先確定起始對話方塊中的「**啟用NFSv4**」並未勾選。

下一個對話方塊包括兩個部分。在上方的文字欄位中，鍵入要輸入的目錄。在下方，輸入可以存取它們的主機。有四種主機萬用字元類型可讓您針對各主機進行設定：單一主機 (名稱或 ip 位址)、網路群組、萬用字元 (例如 * 標是所有機器都可存取伺服器) 以及 IP 網路。

在圖形 28.2 「以 NFSv2 和 v3 輸出目錄」[392頁] 中顯示了此對話方塊。如需這些選項的詳細說明，請參閱 `man exports`。按一下「**完成**」以完成組態。

圖形 28.2 以 NFSv2 和 v3 輸出目錄



28.3.1.3 共存的 v3 和 v4 輸出

NFSv3 和 NFSv4 的輸出可共存於同一個伺服器上。在起始組態對話方塊啟用了對 NFSv4 的支援之後，對於選項清單中沒有納入 `fsid=0` 和 `bind=/target/path` 的輸出，v3 的輸出作業會予以考慮。

請參閱第 28.3.1.1 節「NFSv4 用戶端的輸出」[390 頁]中的範例。如果您使用「新增目錄」來加入其他目錄(例如 `/data2`)，而對應的選項清單並未列出 `fsid=0` 或 `bind=/target/path`，則此輸出即屬於 v3 的輸出作業。

重要

自動防火牆組態

如果您的系統上啟用了 `SuSEfirewall2`，YaST 會在選取「在防火牆中開啟埠」時，啟用 `nfs` 服務以調整其 NFS 伺服器組態。

28.3.2 手動輸出檔案系統

NFS 輸出服務的組態檔案為 `/etc/exports` 和 `/etc/sysconfig/nfs`。除了這些檔案之外，NFSv4 伺服器組態還需要 `/etc/idmapd.conf`。若要啟動或重新啟動服務，請執行 `rcnfsserver restart` 指令。如果已在 `/etc/sysconfig/nfs` 中設定 NFSv4，還會啟動 `rpc.idmapd`。NFS 伺服器需依賴執行的 RPC 埠對應程式。因此，也請以 `rcrpcbind restart` 啟動或重新啟動埠對應程式服務。

28.3.2.1 以 NFSv4 輸出檔案系統

NFSv4 是 SUSE Linux Enterprise Server 上最新版的 NFS 通訊協定。若要設定以 NFSv4 輸出的目錄，其程序和之前的 NFS 版本會有些許不同。

`/etc/exports`

`/etc/exports` 檔案包含一份項目清單。每一個項目都指出一個共享的目錄，並記錄它的共享方式。`/etc/exports` 中的典型項目會包含：

```
/shared/directory host(option_list)
```

例如：

```
/export 192.168.1.2(rw,fsid=0,sync,crossmnt)
/export/data 192.168.1.2(rw,bind=/data,sync)
```

這裡使用了 IP 位址 192.168.1.2，以識別允許的用戶端。您也可以使用主機的名稱以及指向一組主機 (*.abc.com、* 等) 或網路群組 (@my-hosts) 的萬用字元。

指定 `fsid=0` 的目錄是一個特殊的目錄。它是所輸出檔案系統的根目錄，有時稱為虛擬根檔案系統。此目錄還必須包含 `crossmnt`，以便使用 NFSv4 進行正確操作。透過 NFSv4 輸出的所有其他目錄必須掛接在此掛接點下面。如果要輸出的目錄不在此輸出根目錄下，則需要將該目錄繫結至輸出網路樹。可使用 `bind=` 語法完成此操作。

在上面的範例中，`/data` 並不位於 `/export` 之下，因此我們輸出 `/export/data`，並指定 `/data` 目錄應繫結至該名稱。目錄 `/export/data` 必須存在，並且通常應為空白。

用戶端從此伺服器進行掛接時，掛接的只是 `servername:/`，而不是 `servername:/export`。`servername:/data` 不必掛接，因為該目錄會在 `servername:/` 掛接後自動顯示在其下方。

/etc/sysconfig/nfs

`/etc/sysconfig/nfs` 檔案包含一些決定 NFSv4 伺服器精靈行為的參數。`NFS4_SUPPORT` 參數必須設定為 `yes`。`NFS4_SUPPORT` 決定 NFS 伺服器是否支援 NFSv4 輸出和用戶端。

/etc/idmapd.conf

Linux 機器的所有使用者都有名稱和 ID。`idmapd` 會針對伺服器接收的 NFSv4 要求進行名稱和 ID 的對應，然後對用戶端發出回覆。此動作必須同時在 NFSv4 的伺服器和用戶端上執行，因為 NFSv4 的通訊中只使用名稱。

對於可能使用 NFS 來共享檔案系統的機器，請確定有一個統一的方式來對各機器之間的使用者指定使用者名稱和 ID (uid)。您可以透過 NIS、LDAP 或您網域中的任何統一網域驗證機制來達成這個目的。

在用戶端和伺服器兩端的 `/etc/idmapd.conf` 檔案中，`Domain` 參數必須設定為相同的值。如果您不確定，請讓伺服器和用戶端檔案中的網域保持為 `localdomain`。我們在此提出一個組態檔案的例子，如下所示：

```
[General]

Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]

Nobody-User = nobody
Nobody-Group = nobody
```

如需更多參考，請參閱 `idmapd` 和 `idmapd.conf`; `man idmapd`, `man idmapd.conf` 的 `man` 頁面。

啟動和停止服務

對 `/etc/exports` 或 `/etc/sysconfig/nfs` 進行變更後，請以 `rcnfsserver restart` 啟動或重新啟動 NFS 伺服器服務。對 `/etc/idmapd.conf` 進行變更後，請使用指令 `killall -HUP rpc.idmapd` 重新載入組態檔案。

如果 NFS 服務需要在開機時啟動，請執行指令 `chkconfig nfsserver on`。

28.3.2.2 以 NFSv2 和 NFSv3 輸出檔案系統

本節僅適用於 NFSv3 和 NFSv2 的輸出作業。如需以 NFSv4 輸出的詳細資訊，請參閱第 28.3.1.1 節「NFSv4 用戶端的輸出」[390頁]。

以 NFS 輸出檔案系統時需要兩個組態檔案：`/etc/exports` 和 `/etc/sysconfig/nfs`。典型 `/etc/exports` 檔案項目的格式如下：

```
/shared/directory    host(list_of_options)
```

例如：

```
/export    192.168.1.2(rw, sync)
```

這裡的 `/export` 目錄與主機 192.168.1.2 共享，選項清單為 `rw, sync`。此 IP 位址可使用萬用字元以用戶端名稱或用戶端集合取代(例如 `*.abc.com`)，甚至也可以 `netgroup` 取代。

如需所有選項及其意義的詳細說明，請參閱 `man` 頁面 `exports` (`man exports`)。

變更了 `/etc/exports` 或 `/etc/sysconfig/nfs` 以後，請以 `rcnfsserver restart` 指令啟動或重新啟動 NFS 伺服器。

28.3.3 NFS 搭配使用 Kerberos

若要為 NFS 使用 Kerberos 驗證，則 GSS 安全性必須啟用。在初始 &YaST NFS 伺服器對話方塊中選取「啟用 GSS 安全性」。您必須有一個工作中的 Kerberos 伺服器才能使用此功能。YaST 不會設定該伺服器，只會使用所提供的功能。如果除了 YaST 組態之外，您還要使用 Kerberos 驗證，請在執行 NFS 組態之前至少完成以下步驟：

- 1 請確定伺服器 and 用戶端位於相同的 Kerberos 領域中。它們必須存取相同的 KDC (金鑰配送中心) 伺服器，並共享它們的 `krb5.keytab` 檔案 (所有機器上的預設位置都是 `/etc/krb5.keytab`)。如需有關 Kerberos 的詳細資訊，請參閱第 6 章「*Network Authentication with Kerberos*」(↑*Security Guide*)
- 2 請以 `rcgssd start` 來啟動用戶端上的 `gssd` 服務。
- 3 請以 `rcsvcgssd start` 來啟動伺服器上的 `svcgssd` 服務。

如需有關設定啟用 Kerberos 之 NFS 的詳細資訊，請參閱第 28.5 節「如需更多資訊」[399頁] 中的連結所提供的內容。

28.4 設定用戶端

您不需安裝其他軟體就能將您的主機設定為 NFS 用戶端。所有需要的套件預設都會安裝。

28.4.1 以 YaST 輸入檔案系統

授權使用者可以使用 YaST NFS 用戶端模組將 NFS 目錄從 NFS 伺服器掛接到本地檔案樹。請執行下列步驟：

過程 28.2 輸入 NFS 目錄

- 1 啟動 YaST NFS 用戶端模組。
- 2 在「*NFS 共用*」索引標籤中按一下「*新增*」。輸入 NFS 伺服器的主機名稱、要輸入的目錄和在本地掛接此目錄的掛接點。
- 3 如果您要使用防火牆並希望允許遠端電腦存取服務，請啟用「*NFS 設定*」索引標籤中的「*在防火牆中開啟埠*」。防火牆的狀態顯示於核取方塊旁。
- 4 使用 NFSv4 時，請確定選取了「*啟用 NFSv4*」核取方塊，並且「*NFSv4 網域名稱*」中的值與 NFSv4 伺服器使用的值相同。預設網域為 `localdomain`。
- 5 按一下「*確定*」，儲存變更。

組態將會寫入 `/etc/fstab` 中，並會掛接指定的檔案系統。當您稍後啟動 YaST 組態用戶端時，它也會從這個檔案讀取現有組態。

28.4.2 手動輸入檔案系統

從 NFS 伺服器手動輸入檔案系統的先決條件是有 RPC 埠對應程式正在執行。若要啟動該程式，請以 `root` 身分輸入 `rcrpcbind start`。接著，可以像處理本地分割區一樣，使用 `mount` 指令在檔案系統中掛接遠端檔案系統：

```
mount host:remote-pathlocal-path
```

例如，若要從 `nfs.example.com` 機器輸入使用者目錄，可以使用：

```
mount nfs.example.com:/home /home
```

28.4.2.1 使用自動裝載服務

`autofs` 精靈可用於自動掛接遠端檔案系統。請將下列項目加入您的 `/etc/auto.master` 檔案：

```
/nfsmounts /etc/auto.nfs
```

如果能正確填入 `auto.nfs` 檔案，`/nfsmounts` 目錄此後便會成為用戶端上所有 NFS 掛接作業的根部。選擇 `auto.nfs` 這個名稱是以方便為考量，您可以自行選擇任何名稱。使用以下指令在 `auto.nfs` 中為所有 NFS 掛接作業新增項目：

```
localdata -fstype=nfs server1:/data  
nfs4mount -fstype=nfs4 server2:/
```

以 `root` 身分使用 `rcautofs start` 啟動設定。在此範例中，`server1` 的 `/data` 目錄 `/nfsmounts/localdata` 會掛接 NFS，而 `server2` 的 `/nfsmounts/nfs4mount` 會掛接 NFSv4。

如果 `/etc/auto.master` 檔案在 `autofs` 服務的執行過程中被編輯，則必須使用 `rcautofs restart` 重新啟動自動掛載器，才能使變更生效。

28.4.2.2 手動編輯 `/etc/fstab`

`/etc/fstab` 中典型的 NFSv3 掛接項目如下：

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

NFSv4掛接也可以新增至 `/etc/fstab` 檔案。對於這些掛接項目，請在第三欄中使用 `nfs4` (而非使用 `nfs`)，並確定遠端檔案系統在第一欄中的 `nfs.example.com:` 之後以 `/` 提供。`/etc/fstab` 中的 NFSv4 掛接範例行如下：

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

`noauto` 選項可防止在啟動時自動掛載檔案系統。如果要手動掛接各檔案系統，可以縮短掛接指令的長度，僅指定掛接點：

```
mount /local/path
```

請注意，如果未輸入 `noauto` 選項，系統的啟始化程序檔會在啟動時處理這些檔案系統的掛接。

28.4.3 平行 NFS (pNFS)

NFS 是最舊的通訊協定之一，開發於八十年代。雖然如此，NFS 對於共用小型檔案還是綽綽有餘的。但是，如果您要傳輸大型檔案或大量用戶端想要存取資料，NFS 伺服器將會成為瓶頸，並對系統效能造成明顯影響。出現這種情況的原因是檔案大小快速變大，而乙太網路的相對速度未能緊隨其後。

當您申請「一般」NFS 伺服器中的檔案時，該伺服器會尋找檔案中繼資料、收集所有資料並透過網路將其傳輸至您的用戶端。但是，不論檔案的大小，效能瓶頸都會變得很明顯：

- 對於小型檔案，大部分時間都用在收集中繼資料上
- 對於大型檔案，大部分時間則用在將資料從伺服器傳輸至用戶端上

pNFS (或平行 NFS) 克服了這個局限性，因為它將檔案系統中繼資料與資料位置分隔開來。因此，pNFS 需要兩種類型的伺服器：

- 中繼資料或控制伺服器，用於處理所有非資料流量
- 一或多個儲存伺服器，用於存放資料

中繼資料與儲存伺服器構成了一個邏輯 NFS 伺服器。當用戶端想要讀取或寫入時，中繼資料伺服器會告知 NFSv4 用戶端使用哪個儲存伺服器來存取檔案區塊。用戶端可以直接存取伺服器上的資料。

SUSE Linux Enterprise 僅對用戶端支援 pNFS。

28.4.3.1 使用 YaST 設定 pNFS 用戶端

依過程 28.2, “輸入 NFS 目錄” [396頁] 中所示繼續操作，但要按一下「*pNFS (v4.1)*」核取方塊並選擇性地按一下「*NFSv4 共享*」。YaST 將會執行所有必要的步驟，並將所有需要的選項寫入檔案 `/etc/exports` 中。

28.4.3.2 手動設定 pNFS 用戶端

請參閱第 28.4.2 節「手動輸入檔案系統」 [397頁] 開始設定。大部分組態均由 NFSv4 伺服器執行。對於 pNFS，唯一的差異是將 `minorversion` 選項和中繼資料伺服器 *MDS 伺服器* 新增至 `mount` 指令：

```
mount -t nfs4 -o minorversion=1 MDS_SERVER MOUNTPOINT
```

為了協助進行除錯，請在 `/proc` 檔案系統中變更該值：

```
echo 32767 > /proc/sys/sunrpc/nfsd_debug  
echo 32767 > /proc/sys/sunrpc/nfs_debug
```

28.5 如需更多資訊

除了 `exports`、`nfs` 和 `mount` 的 `man` 頁面以外，`/usr/share/doc/packages/nfsidmap/README` 中也提供了有關設定 NFS 伺服器和用戶端的資訊。如需更多線上文件，請參閱下列網站：

- 如需詳細的線上技術文件，請造訪 SourceForge [<http://nfs.sourceforge.net/>]。
- 如需設定已監督之 NFS 的指示，請參閱 NFS 第 4 版開放原始碼實作參考 [<http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html>]。
- 如果您有任何關於 NFSv4 的問題，請參閱 Linux NFSv4 常見問答集 [<http://www.citi.umich.edu/projects/nfsv4/linux/faq/>]。

檔案同步化

現在，許多人都使用多台電腦——家裡一台、辦公室一台或數台，出門在外還使用筆記型電腦、平板電腦或智慧型手機。許多檔案都需要各存一份在所有這些電腦上。您可能希望所有電腦能一起工作、修改檔案，這樣就能讓所有電腦都擁有最新的資料。

29.1 可用的資料同步化軟體

對於永久以快速網路連結的電腦而言，資料同步化不是問題。在此狀況下，使用 NFS 之類的網路檔案系統，並將檔案儲存在伺服器上，所有主機就可以透過網路來存取相同的資料。但如果網路連線品質很差或不是永久的，就無法使用此方法。當您出門在外使用筆記型電腦時，所有需要的檔案複本都必須在本地硬碟上。不過之後需要將修改過的檔案同步化。當您在某一台電腦上修改檔案時，請確定也更新了所有其他電腦上的同一檔案。至於一些零散的複本，則可以使用 `scp` 或 `rsync` 手動更新它。然而，如果有許多檔案需要處理，則該程序有可能變得很複雜，而且需要更小心才能避免類似以舊檔案覆寫新檔案的錯誤。

警告：資料遺失的風險

在您開始使用同步化系統管理資料之前，應該先好好的認識要使用的程式並測試其功能。對於重要檔案而言，備份是不可或缺的動作。

手動同步化資料非常耗時，而且是一種容易發生錯誤的任務，要避免這些缺點，可以使用一種以多種方法將此工作自動化的程式。下列摘要讓您概略瞭解這些程式的運作方式和使用方法。如果您打算使用它們，請詳閱程式文件。

29.1.1 CVS

CVS 主要用來管理程式來源版本，它能在多台電腦上保留檔案副本。因此，它也適用於資料同步化。CVS 負責維護伺服器上的中央儲存庫，檔案及檔案的變更都儲存在此。在本地執行的變更會交付至儲存庫，並且可以利用更新從其他電腦擷取。兩個程序都必須由使用者起始。

CVS 對於錯誤有非常大的彈性與包容性，所以可以應付多台電腦同時進行變更的情況。所有變更會合併，如果同一行發生多種變更，系統還會報告衝突。衝突發生時，資料庫會維持一致的狀態。只有在用戶端主機上才能看到衝突，並加以解決。

29.1.2 rsync

當不需要版本控制，但是大型目錄結構需要透過緩慢的網路連線進行同步化時，rsync 工具針對僅傳送檔案中的變更可提供已開發成熟的機制。這不只適用於文字檔，也適用於二進位檔。為了偵測檔案之間的不同，rsync 會將檔案分為區塊並計算它們的檢查總數。

偵測變更將需要付出相當大的成本。要同步化的系統應該要具有相當的硬體配備，才能使用 rsync。RAM 尤其重要。

29.2 選取程式時所要考慮的決定性因素

在決定要使用哪個程式時，必須考慮一些重要的因素。

29.2.1 用戶端對伺服器與點對點

配送資料時常使用的模式有兩種。第一個模式是，所有的用戶端都以中央伺服器為準，將其檔案同步化。伺服器至少必須偶爾可以讓所有的用戶端存取。CVS 使用此模式。

另一種可能性就是，讓網路上所有主機都以點對點的方式將彼此間的資料同步化。rsync 實際作用於用戶端模式，但任何用戶端都可以當作伺服器使用。

29.2.2 可攜式

在許多其他的作業系統上也可以使用 CVS 以及 rsync，包含各種 Unix 與 Windows 系統。

29.2.3 互動式與自動化

在 CVS 中，資料同步化是由使用者以手動方式啟動。這讓使用者對於要同步化的資料進行良好的控制，並可輕鬆地處理衝突。然而，如果同步化間隔太長，就比較可能發生衝突。

29.2.4 衝突：發生與解決

即使有數個人員同時在某個大型的程式專案上一起工作，在 CVS 中發生衝突的機率還是相當地少。這是因為文件是在個別的行列上進行合併。當發生衝突時，只有一個用戶端會受到影響。CVS 中的衝突通常都可以輕易解決。

rsync 中則無衝突處理功能。使用者必須小心不要覆寫檔案，並手動解決所有可能的衝突。為確保安全，另外還可使用版本設定系統 (如 RCS)。

29.2.5 選取和新增檔案

在 CVS 中，必須分別使用 `cvs` 或 `add` 指令，明確地新增目錄與檔案。這讓使用者對於要同步化的檔案擁有更大的控制權。另一方面，新檔案時常會被忽略，特別是在處理大量的檔案而忽略了 `cvs` 以及 `update` 輸出中的問號時。

29.2.6 歷程

CVS 還有另一項功能，那就是可以重新建構舊的檔案版本。每個變更都可以插入簡短的編輯符號，而且之後可以根據其內容與符號輕易地追蹤檔案的發展。這對論文與程式文字而言，是一種很珍貴的助力。

29.2.7 資料量與硬碟需求

所有相關主機的硬碟都需要有足夠的可用空間來儲存所有分散式的資料。CVS 在伺服器上還需要額外的空間，供儲存庫資料庫使用。檔案歷程記錄也會儲存在伺服器上，因此需要更多的空間。當文字格式的檔案變更時，只需儲存修改過的那幾行。每當變更檔案時，二進位檔案就會需要與該檔案大小相同的額外空間。

29.2.8 GUI

有經驗的使用者通常會從指令行執行 CVS。然而，在 *cervisia* 之類的 Linux 系統中，以及 *wincvs* 之類的其他作業系統中，都有圖形使用者介面。此外，許多開發工具 (像是 *kdevelop*) 以及文字編輯器 (像是 *Emacs*) 都支援 CVS。使用這些前端程式的話，衝突的解決方案通常會更容易執行。

29.2.9 使用者親切性

rsync 較易於使用且適合新進人員。CVS 某種程度上較難操作。使用者必須瞭解儲存庫與本地資料之間的互動。對資料的變更應該先在本地與儲存庫合併。這是使用 `cvs` 或 `update` 指令來執行。接著必須使用 `cvs` 或 `commit` 指令將資料傳送回儲存庫。只要瞭解此程序，新進人員就可輕鬆使用 CVS。

29.2.10 防止攻擊的安全性

在傳輸期間，應該保護資料以防攔截和竄改。CVS 與 *rsync* 都可以透過 *ssh* (安全的外圍程式) 來使用，提供安全性以防護此類攻擊。應該避免透過 *rsh* (遠端外圍程式) 執行 CVS。同樣地也不建議在不安全的網路中使用 *pserver* 機制存取 CVS。

29.2.11 針對資料遺失的防護

開發人員使用 CVS 來管理程式專案已經有很長的一段時間，而且極為穩定。因為開發的歷程記錄皆已儲存，所以 CVS 甚至提供保護，防止某些使用者錯誤發生，例如不小心刪除檔案。

表格 29.1 檔案同步化工具的功能：-- = 很差，- = 差或無法使用，o = 中等，+ = 良好，++ = 優異，x = 可用

	CVS	rsync
主/從	C-S	C-S
可攜式	Lin、Un*x、Win	Lin、Un*x、Win
互動	x	x
速度	o	+
衝突	++	o
檔案 Sel。	Sel./file, dir.	目錄
歷程	x	-
硬碟空間	--	o
GUI	o	-
困難度	o	+
攻擊	+(ssh)	+(ssh)
資料損失	++	+

29.3 CVS 簡介

如果經常編輯某些個別檔案，並且以檔案格式儲存，例如 ASCII 文字或程式來源文字，就非常適合使用 CVS 進行同步化。您可以使用 CVS 同步化其他格式的資料(例如 JPEG 檔案)，但是會產生大量的資料，因為檔案的所有變體都會永久儲存在 CVS 伺服器上。在這種情形下，CVS 的大部份功能都將無法使用。只有在所有工作站都可以存取同一伺服器時，才能使用 CVS 同步化檔案。

29.3.1 設定 CVS 伺服器

server 是所有有效檔案所在的主機，這包含所有檔案的最新版本。任何靜態工作站都可做為伺服器。可能的話，CVS 儲存庫的資料應該包含在定期備份中。

當設定 CVS 伺服器時，透過 SSH 授予使用者該伺服器的存取權可能是不錯的方式。如果使用者是以 *tux* 的身份登入伺服器，而且 CVS 軟體既安裝在伺服器上也安裝在用戶端上，則必須在用戶端上設定下列環境變數：

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

`cvsinit` 指令可用來從用戶端啟始 CVS 伺服器。這只需要做一次。

最後，必須為同步化指定名稱。在用戶端上選取或建立一個目錄，用於存放 CVS 所管理的檔案 (目錄也可以是空的)。該目錄的名稱也就是同步化的名稱。在此範例中，該目錄稱為 *synchome*。變更至此目錄，然後輸入下列指令將同步化名稱設為 *synchome*：

```
cvs import synchome tux wilber
```

許多 CVS 指令需要註解。因此，CVS 會啟動編輯器 (如果沒有定義編輯器，則會啟動環境變數 `$EDITOR` 或 `vi` 中所定義的編輯器。) 在指令行先輸入註解，就可以避免編輯器的呼叫，如下列範例所示：

```
cvs import -m 'this is a test' synchome tux wilber
```

29.3.2 使用 CVS

現在可以使用 `cvsco synchome` 從所有主機取出同步化儲存庫。這會在用戶端上建立新的子目錄 *synchome*。若要將變更交付至伺服器，請換至 *synchome* 目錄 (或其中一個子目錄)，然後輸入 `cvscommit`。

根據預設，所有的檔案 (包括子目錄) 都會交付給伺服器。若只要交付個別的檔案或目錄，請在 `cvscommit file1 directory1` 中指定它們。在將它們交付至伺服器前，必須使用像是 `cvsadd file1 directory1` 之類的指令，將新檔案與目錄新增至儲存庫。接著，使用 `cvscommit file1 directory1` 交付新增的檔案與目錄。

您更換至另一個工作站時，如果先前的工作階段尚未取出該工作站的同步化儲存庫，請現在取出。

使用 `cvsupupdate` 啟動與伺服器的同步化。依照 `cvsupupdate file1 directory1` 中的個別檔案或目錄來更新。若要查看目前檔案與伺服器上所存版本的差異，請使用 `cvsdiff` 或 `cvsdiff file1 directory1` 指令。使用 `cvns-nq update` 來查看哪些檔案會受到更新的影響。

以下是更新期間所顯示的一些狀態符號：

U

已更新本地版本。這將會影響伺服器所提供及在本地系統上所遺失的全部檔案。

M

已修改本地版本。如果在伺服器上有一些變更，可以在本地複本中將差異合併。

P

本地版本已使用伺服器版本修補。

C

本地檔案與儲存庫中目前的版本衝突。

?

這個檔案並不存在於 CVS。

M 狀態是指在本地修改過的檔案。或是將本地複本交付至伺服器，或是移除本地檔案後再執行一次更新。在此例中，會從伺服器擷取遺失的檔案。如果您交付本地已修改的檔案，而該檔案是在同一行中變更並交付，則有可能造成衝突，這是以 C 表示。

如果發生這種狀況，請檢視檔案中的衝突記號 (>> 與 <<)，並在兩個版本之間選擇一個。這有可能是相當麻煩的工作，您可能會決定捨棄變更、刪除本地檔案，然後輸入 `cvsup`，以便從伺服器擷取目前的版本。

29.4 rsync 簡介

當有大量的資料需要定期傳輸，但是並無太多變更時，rsync 就非常有用。例如，當建立備份時就非常適用。另一個應用程式則將焦點放在建置伺服器。這些伺服器儲存了網頁伺服器的完整目錄樹狀結構，會定期鏡像複製至 DMZ 中的網頁伺服器。

29.4.1 組態與作業

rsync 可以使用兩個模式來操作。它是用來歸檔或複製資料。若要完成此動作，在目標系統上只需要像是 ssh 的遠端外圍程序。然而，rsync 也可以像 daemon 一樣，用來為網路提供目錄。

rsync 的基本作業模式並不需要任何特殊的組態。rsync 直接允許將完整的目錄鏡像複製至另一個系統。例如，下列指令可在名為 sun 的備份伺服器上建立 tux 主目錄的備份：

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

下列指令可用來還原目錄：

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

到此為止，其處理方式與一般的複製工具 (例如 scp) 的處理沒有太大的差別。

rsync 應該在「rsync」模式中操作，才能充分使用其所有的功能。執行方法是在其中一個系統上啟動 rsyncd 精靈。在 /etc/rsyncd.conf 檔案中設定它。例如，如果要讓 /srv/ftp 目錄可供 rsync 使用，請使用下列組態：

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log
```

```
[FTP]
```

```
path = /srv/ftp
comment = An Example
```

接著使用 rcrsyncdstart 來啟動 rsyncd。在開機程序期間也可以自動啟動 rsyncd。設定的方式有兩種，一是在 YaST 所提供的執行層級編輯器中啟用此服

務，另一是手動輸入 `insservrsyncd` 指令。`rsyncd` 也可以由 `xinetd` 啟動。然而，只有對很少使用 `rsyncd` 的伺服器才建議這麼做。

本範例也建立了傾聽所有連接的記錄檔。這個檔案是儲存在 `/var/log/rsyncd.log`。

這樣才可以從用戶端系統測試傳輸。使用下列指令來執行此動作：

```
rsync -avz sun::FTP
```

此指令會列出伺服器上 `/srv/ftp` 目錄中所有存在的檔案。這個要求也會記錄在 `/var/log/rsyncd.log` 記錄檔中。若要啟動實際的傳輸，請提供目標目錄。請使用 `.` 來代表目前的目錄。例如：

```
rsync -avz sun::FTP .
```

依照預設，在使用 `rsync` 同步化時不會刪除檔案。如果要強制刪除檔案，就必須加上額外的選項 `--delete`。若要確保不會刪除較新的檔案，則可以改用 `--update` 選項。任何產生的衝突都必須手動解決。

29.5 如需更多資訊

CVS

可在首頁 <http://www.cvshome.org> 找到有關 CVS 的重要資訊。

rsync

關於 `rsync` 的重要資訊，請參閱手冊頁面。指令為 `manrsync` 和 `manrsyncd.conf`。如需關於 `rsync` 作業原則的技術參考資料，可在 `/usr/share/doc/packages/rsync/tech_report.ps` 中找到。您可以在專案網站 <http://rsync.samba.org/> 上找到關於 `rsync` 的最新消息。

Apache HTTP 伺服器

根據 <http://www.netcraft.com/> 的調查結果顯示，Apache HTTP 伺服器 (Apache) 在市面上佔有率已超過 50%，是目前全世界最多人使用的網頁伺服器。由 Apache 軟體基金會 (<http://www.apache.org/>) 研發的 Apache 可在大部分作業系統上使用。SUSE® Linux Enterprise Server 隨附 Apache 2.2 版。本章將介紹如何安裝、組態設定與設定 Web 伺服器，如何使用 SSL、CGI 與其他模組，以及如何排解 Apache 疑難。

30.1 快速入門

本節的說明可協助您快速設定和啟動 Apache。您的身分必須為 `root`，才能安裝和設定 Apache。

30.1.1 要求

在設定 Apache Web 伺服器之前，請先確定您已符合下列要求：

1. 此機器的網路已正確設定。如需有關這個主題的詳細資訊，請參閱第 21 章「基本網路」[243頁]。
2. 此機器的實際系統時間已透過時間伺服器進行同步維護。這是必要動作，因為 HTTP 通訊協定的部分內容會依據正確時間來運作。如需有關這個主題的詳細資訊，請參閱第 23 章「使用 NTP 進行時間同步化」[307頁]。

3. 已安裝最新的安全性更新。如果不清楚是否已安裝，請執行「YaST 線上更新」。
4. 防火牆中已開啟預設的 Web 伺服器連接埠 (80)。為此，請將 SuSEFirewall2 設定成允許在外部區域執行「*HTTP 伺服器*」服務。您可以使用 YaST 完成此設定。如需詳細資料，請參閱第 15.4.1 節「Configuring the Firewall with YaST」(第 15 章「*Masquerading and Firewalls*」, ↑*Security Guide*)。

30.1.2 安裝

SUSE Linux Enterprise Server 上預設未安裝 Apache。若要以可「直接」執行的預先定義標準組態進行安裝，請按照以下步驟操作：

過程 30.1 以預設組態安裝 *Apache*

- 1 啟動 YaST，然後選取「軟體」>「軟體管理」。
- 2 選擇「過濾器」>「模式」，然後在「伺服器功能」中選取「*Web 與 LAMP 伺服器*」。
- 3 請確蓋安裝個別套件，完成此安裝程序。

此項安裝會安裝多重處理模組 `apache2-prefork` 與 **PHP5** 模組。如需更多關於各種模組的詳細資訊，請參閱{第 30.4 節「安裝、啟用和設定模組」 [429頁]}

30.1.3 開始

您可讓 Apache 在開機時自動啟動或者手動將其啟動。

過程 30.2 自動啟動 *Apache*

- 1 為確定 Apache 會在開機階段的執行層級 3 與 5 自動啟動，請執行以下指令：

```
chkconfig -a apache2
```
- 2 或者，請啟動 YaST，然後選取「系統」>「系統服務 (執行層級)」。
- 3 搜尋 *apache2* 並「啟用」該服務。

網頁伺服器將立即啟動。

4 按一下「完成」儲存您的變更。

系統即設定為在開機階段的執行層級 3 與 5 自動啟動 Apache。

如需 SUSE Linux Enterprise Server 中執行層級的詳細資訊與 YaST 執行層級編輯器的說明，請參閱第 9.2.3 節「使用 YaST 設定 System Services (Runlevel)」[103頁]。

若要使用外圍程序手動啟動 Apache，請執行 `rcapache2 start`。

過程 30.3 檢查 Apache 是否正在執行

如果您在啟動 Apache 時未接收到錯誤訊息，這通常表示 Web 伺服器正在執行。若要對此進行測試：

1 啟動瀏覽器，並開啟 <http://localhost/>。

如果 Apache 已啟動且正在執行，系統會顯示「正常運作！」的測試頁面。

2 如果此頁面沒有出現，請參閱第 30.8 節「疑難排解」[448頁]。

現在網頁伺服器已經開始執行，您可以加入自己的文件、根據個人需求調整組態，或是安裝模組來新增功能。

30.2 設定 Apache

SUSE Linux Enterprise Server 提供了兩個組態選項：

- 手動設定 Apache [417頁]
- 使用 YaST 設定 Apache [421頁]

手動設定組態可以提供較詳細的設定，但是缺乏 YaST GUI 提供的方便性。

重要：在組態變更後重新載入或重新啟動 Apache

大多數組態變更需要重新載入 (有些還需要重新啟動) Apache 才能生效。請使用 `rcapache2 reload` 以手動方式重新載入 Apache，或使用第 30.3 節「啟動和停止 Apache」[427頁] 中所述的其中一個重新啟動選項。

如果使用 YaST 來設定 Apache，依照第 30.2.3.2 節「HTTP 伺服器組態」[425頁] 中所述將「*HTTP 服務*」設定為「已啟用」，即可讓上述操作自動完成。

30.2.1 Apache 組態檔案

本節提供 Apache 組態檔案的綜覽。如果使用 YaST 設定組態，則無需變更這些檔案。不過，如果您要在以後改為以手動方式設定組態，該資訊可能會對您有用。

您可以在下列兩個不同位置找到 Apache 組態檔案：

- `/etc/sysconfig/apache2` [414頁]
- `/etc/apache2/` [414頁]

30.2.1.1 `/etc/sysconfig/apache2`

`/etc/sysconfig/apache2` 可控制部分的 Apache 全域設定，例如要載入的模組、要包含的其他組態檔案、伺服器應該啟動的旗標，以及應該新增至指令行的旗標。此檔案對每個組態選項都進行了詳細說明，因此本文不予以介紹。針對一般用途的網頁伺服器，在 `/etc/sysconfig/apache2` 中的設定應該可以符合任何組態需求。

30.2.1.2 `/etc/apache2/`

`/etc/apache2/` 代管了 Apache 的所有組態檔案。以下各節將說明每個檔案的用途。每個檔案都包含了數個組態選項 (又稱為*指示詞*)。在這些檔案中的每個組態選項都會詳加說明，因此本文將不予以介紹。

Apache 組態檔案的組織方式如下：

```
/etc/apache2/  
|
```



```

|- charset.conv
|- conf.d/
|   |
|   |- *.conf
|
|- default-server.conf
|- errors.conf
|- httpd.conf
|- listen.conf
|- magic
|- mime.types
|- mod_*.conf
|- server-tuning.conf
|- ssl.*
|- ssl-global.conf
|- sysconfig.d
|   |
|   |- global.conf
|   |- include.conf
|   |- loadmodule.conf . .
|
|- uid.conf
|- vhosts.d
|   |- *.conf

```

在 `/etc/apache2/` 中的 *Apache* 組態檔案

`charset.conv`

指定不同語言所要使用的字元集。請不要編輯此檔案。

`conf.d/*.conf`

組態檔案由其他模組新增。這些組態檔案可以依實際需要包含至虛擬主機組態。如需範例，請參閱 `vhosts.d/vhost.template`。若要執行這個動作，您可以為不同的虛擬主機提供不同的模組組合。

`default-server.conf`

使用合理預設值設定所有虛擬主機的全域組態。這時不是變更組態值，而是採用虛擬主機組態覆寫組態值。

`errors.conf`

定義 *Apache* 處理錯誤的方式。若要自定這些傳送給所有虛擬主機的訊息，請編輯此檔案。另外一種方法是覆寫虛擬主機組態中的這些指示詞。

`httpd.conf`

主要的 Apache 伺服器組態檔案。請勿變更此檔案。此檔案主要包含 Include 陳述式和全域設定。為此處列出的相關組態檔案覆寫全域設定。變更虛擬主機組態的主機特定設定 (例如文件根目錄)。

`listen.conf`

繫結 Apache 至特定的 IP 位址與連接埠在此檔案中也可以設定以名稱為基礎的虛擬主機。如需詳細資料，請參閱章節「以名稱為基礎的虛擬主機」[418頁]。

`magic`

`mime_magic` 模組的資料，此模組可協助 Apache 自動判斷不明檔案的 MIME 類型。請不要變更此檔案。

`mime.types`

系統已知的 MIME 類型 (實際上是 `/etc/mime.types` 的連結)。請不要編輯此檔案。如果您需要新增這裡未列出的 MIME 類型，請將它們新增到 `mod_mime-defaults.conf`。

`mod_*.conf`

預設已安裝之模組的組態檔案。如需詳細資訊，請參閱第 30.4 節「安裝、啟用和設定模組」[429頁]。請注意，選用模組的組態檔案會存放在 `conf.d` 目錄。

`server-tuning.conf`

包含不同 MPM 的組態指示詞 (請參閱第 30.4.4 節「多重處理模組」[434頁]) 和可控制 Apache 效能的一般組態選項。請在變更此檔案之後為網頁伺服器進行適當測試。

`ssl-global.conf` 和 `ssl.*`

全域 SSL 組態和 SSL 憑證資料。如需詳細資訊，請參閱第 30.6 節「設定提供 SSL 的安全網頁伺服器」[439頁]。

`sysconfig.d/*.conf`

自動從 `/etc/sysconfig/apache2` 產生的組態檔案。請勿變更其中任何一個檔案，但可以編輯 `/etc/sysconfig/apache2`。請不要將其他組態檔案置於此目錄中。

`uid.conf`

指定要在哪個使用者和群組 ID 之下執行 Apache。請不要變更此檔案。

`vhosts.d/*.conf`

您的虛擬主機組態應存放於此處。該目錄包含採用或不採用 SSL 之虛擬主機的樣板檔案。此目錄中以 `.conf` 結尾的每個檔案都會自動包含在 Apache 組態中。如需詳細資訊，請參閱第 30.2.2.1 節「虛擬主機組態」[417頁]。

30.2.2 手動設定 Apache

以手動方式設定 Apache 是指以 `root` 使用者身分來編輯純文字組態檔案。

30.2.2.1 虛擬主機組態

「*虛擬主機*」一詞，是形容 Apache 從同一部實體機器提供多個通用資源識別字串 (URI, Universal Resource Identifier) 的能力。意思是一部實體機器上的單一網頁伺服器能同時執行數個網域，例如，`www.example.com` 和 `www.example.net`。

使用虛擬主機的目的，經常是為了節省管理工作 (只需要維護一部網頁伺服器) 和硬體開銷 (不需要將各個網域安裝在專屬伺服器上)。虛擬主機可以使用名稱、IP 或是連接埠作為基礎。

若要列出所有現有的虛擬主機，請使用指令 `httpd2 -S`。該指令將輸出一份清單，顯示預設伺服器和所有虛擬主機，以及它們的 IP 位址和監聽埠。此外，該清單還顯示每個虛擬主機在組態檔案中的位置。

虛擬主機可依照章節「*虛擬主機*」[424頁] 中所述透過 YaST 設定，或是手動編輯組態檔案來設定。依預設，系統會根據 `/etc/apache2/vhosts.d/` 中每部虛擬主機一個組態檔案的設定，為在 SUSE Linux Enterprise Server 中執行的 Apache 做好準備。此目錄中副檔名為 `.conf` 的所有檔案，都會自動包含至組態中。這個目錄會提供虛擬主機的基本樣板 (`vhost.template`，或是適用於提供 SSL 支援之虛擬主機的 `vhost-ssl.template`)。

提示：永遠要建立虛擬主機組態

建議您務必要建立虛擬主機組態檔案，即使網頁伺服器只代管一個網域。如此，您不但可以將網域專屬組態存放在一個檔案中，還可以隨時回復至運作正常的基本組態，只需移動、刪除或重新命名虛擬主機的組態檔案即可。同樣地，您應該也要分別為每個虛擬主機建立組態。

使用名稱型虛擬主機時，建議設定預設組態，以便在網域名稱與虛擬主機組態不相符時使用。系統會首先載入預設虛擬主機的組態。由於組態檔案的順序由檔案名稱決定，因此請在預設虛擬主機組態檔案名稱的開頭使用底線字元 (`_`)，以確定該檔案最先載入 (例如：`_default_vhost.conf`)。

`<VirtualHost>``</VirtualHost>` 區塊包含要套用到特定網域的資訊。當 Apache 接收到來自定義的虛擬主機的用戶端要求時，就會使用本節所包含的指示詞。幾乎所有指示詞都可以用於虛擬主機網路位置。如需更多有關 Apache 組態指示詞的詳細資訊，請參閱<http://httpd.apache.org/docs/2.2/mod/quickreference.html>。

以名稱為基礎的虛擬主機

使用以名稱為基礎的虛擬主機時，每個 IP 位址可以為數個網站提供服務。Apache 會使用用戶端所傳送之 HTTP 標頭中的主機欄位，將要求連接到與其中一個虛擬主機宣告相符的 `ServerName` 項目。如果沒有找到相符的 `ServerName`，就會預設使用第一個指定的虛擬主機。

`NameVirtualHost` 指示詞通知 Apache 要在哪個 IP 位址及哪個連接埠 (選擇性) 上監聽 HTTP 標頭中包含網域名稱的用戶端要求。這個選項會設定在組態檔案 `/etc/apache2/listen.conf`。

第一個引數可以是完全合格的網域名稱 (Fully Qualified Domain Name)，但是建議最好使用 IP 位址。第二個引數是連接埠，此引數是可選的。預設會使用連接埠 80，並且您可以透過 `Listen` 指示詞對其進行設定。

IP 位址和連接埠號碼都可以使用萬用字元 `*`，來接收所有介面上的要求。IPv6 位址必須包在方括號中。

範例 30.1 以名稱為基礎的 `VirtualHost` 項目變化

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.3.100:80
NameVirtualHost 192.168.3.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:364::]:80
```

開啟的 `VirtualHost` 標籤會將前面經由 `NameVirtualHost` 宣告的 IP 位址 (或完全合格的網域名稱) 當作以名稱為基礎之虛擬主機的組態引數。先前使用 `NameVirtualHost` 指示詞宣告的連接埠號碼屬於選擇性。

允許使用萬用字元 * 做為 IP 位址的替代符號。此語法只適用於在 NameVirtualHost * 中結合使用萬用字元的情形。如果是使用 IPv6 位址，該位址就必須用方括號包住。

範例 30.2 以名稱為基礎的 VirtualHost 指示詞

```
<VirtualHost 192.168.3.100:80>
...
</VirtualHost>

<VirtualHost 192.168.3.100>
...
</VirtualHost>

<VirtualHost *:80>
...
</VirtualHost>

<VirtualHost *>
...
</VirtualHost>

<VirtualHost [2002:c0a8:364::]>
...
</VirtualHost>
```

以 IP 為基礎的虛擬主機

此虛擬主機組態替代方法需要為一台機器設定多個 IP。一個 Apache 例項可裝載多個網域，每個網域都會指定不同的 IP。

實體伺服器必須為每部以 IP 為基礎的虛擬主機設定一個 IP 位址。當該電腦沒有安裝多張網路卡時，也可以使用虛擬網路介面 (IP 別名)。

下列範例中，Apache 正執行於 IP 為 192.168.3.100 的電腦上，並另外在 IP 192.168.3.101 與 192.168.3.102 上裝載了兩個網域。每部虛擬伺服器都必須具備個別的 VirtualHost 區塊。

範例 30.3 以 IP 為基礎的 VirtualHost 指示詞

```
<VirtualHost 192.168.3.101>
...
</VirtualHost>

<VirtualHost 192.168.3.102>
...
</VirtualHost>
```

這裡出現的 `VirtualHost` 指示詞僅指定給了除 `192.168.3.100` 以外的其他介面。如果 `192.168.3.100` 也有設定 `Listen` 指示詞，這時就必須建立另一個以 IP 為基礎的虛擬主機，向該介面回應 HTTP 要求，否則將套用預設伺服器組態 (`/etc/apache2/default-server.conf`) 中的指示詞。

基本虛擬主機組態

每個虛擬主機組態中至少要出現下列指示詞，才能設定虛擬主機。如需瞭解更多選項的詳細資訊，請參閱 `/etc/apache2/vhosts.d/vhost.template`。

`ServerName`

完全合格網域名稱，其下是應該要建立位址的主機。

`DocumentRoot`

目錄路徑，`Apache` 會從此路徑為此主機提供檔案。基於安全性考量，存取整個檔案系統是預設禁止的動作，所以您必須明確解除鎖定這個位在 `Directory` 容器中的目錄。

`ServerAdmin`

伺服器管理員的電子郵件地址。這個地址可顯示在 `Apache` 建立的錯誤頁面 (舉例說明)。

`ErrorLog`

此虛擬主機的錯誤記錄檔案。雖然沒必要為每個虛擬主機分別建立錯誤記錄檔案，但是多數人會這樣做，以便除錯更加容易。`/var/log/apache2/` 是 `Apache` 記錄檔案的預設目錄。

`CustomLog`

此虛擬主機的存取記錄檔案。雖然沒必要為每個虛擬主機分別建立存取記錄檔案，但是多數人會這樣做，以便分別為每部主機分析存取統計資料。`/var/log/apache2/` 是 `Apache` 記錄檔案的預設目錄。

正如前面所述，存取整個檔案系統已因安全性考量而預設為禁止動作。因此，請將 `Apache` 要處理之檔案所在的目錄明確解除鎖定 — 例如 `DocumentRoot`。

```
<Directory "/srv/www/www.example.com/docs">  
    Order allow,deny  
    Allow from all  
</Directory>
```

此完整組態看起來如下：

範例 30.4 基本 *VirtualHost* 組態

```
<VirtualHost 192.168.3.100>
  ServerName www.example.com
  DocumentRoot /srv/www/www.example.com/htdocs
  ServerAdmin webmaster@example.com
  ErrorLog /var/log/apache2/www.example.com_log
  CustomLog /var/log/apache2/www.example.com-access_log common
  <Directory "/srv/www/www.example.com/htdocs">
    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

30.2.3 使用 YaST 設定 Apache

若要使用 YaST 來設定您的網頁伺服器，請啟動 YaST 並依序選取「*網路服務*」>「*HTTP 伺服器*」。第一次啟動模組時，「*HTTP 伺服器精靈*」會啟動，提示您對伺服器管理進行一些基本設定。完成精靈之後，每當您呼叫「*HTTP 伺服器*」模組時，「*HTTP 伺服器組態*」對話方塊就會啟動。如需詳細資訊，請參閱第 30.2.3.2 節「*HTTP 伺服器組態*」[425頁]。

30.2.3.1 HTTP 伺服器精靈

HTTP 伺服器精靈包含有五個步驟。在最後一個步驟的對話方塊中，您可以進入進階組態模式以進行更多特定的設定。

網路設備選擇

在此，您可以指定 Apache 用來傾聽內送要求的網路介面和連接埠。您可以選取任何現有網路介面及其 IP 位址的組合。若連接埠 (連接埠隸屬以下三種：已知埠、註冊埠和動態或私人埠) 不供其他服務使用，則皆可供您使用。預設設定為在連接埠 80 上監聽所有網路介面 (IP 位址)。

核取「*在防火牆中開啟埠*」選項，可在防火牆中開啟 Web 伺服器監聽的連接埠。若要使網頁伺服器在網路 (包括 LAN、WAN 或公用網際網路) 上為可用狀態，請核取此選項。只有在測試時，並且此時不須由外部網路存取 Web 伺服器，才可以關閉該連接埠。如果您有多個網路介面，請按一下「*防火牆細節...*」以指定應對何介面開啟連接埠。

按「*下一步*」繼續設定組態。

模組

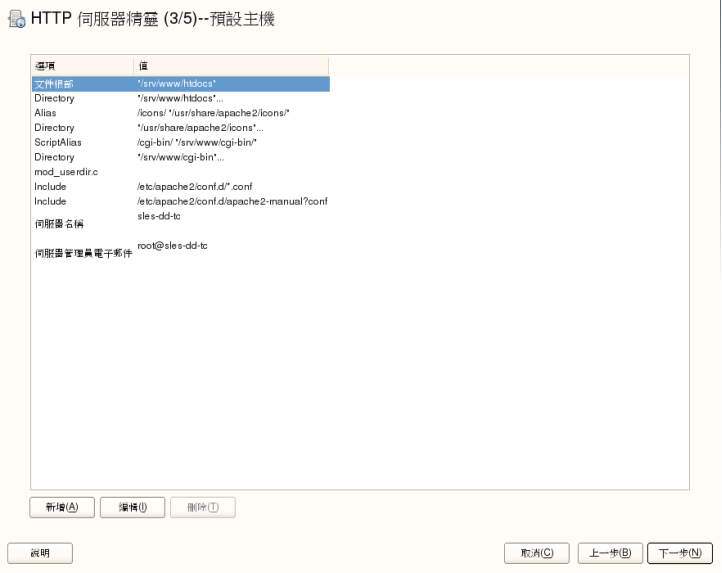
使用「*模組*」組態選項，可以啟用或停用 Web 伺服器應支援的程序檔語言。如需有關啟用或停用其他模組的詳細資訊，請參閱章節「*伺服器模組*」[426頁]。按一下「*下一步*」，繼續進行下一個對話方塊。

預設主機

此選項與預設網頁伺服器相關。正如第 30.2.2.1 節「*虛擬主機組態*」[417頁]內容所述，Apache 可以在一部實體機器上提供多個虛擬主機。組態檔案中第一個宣告的虛擬主機通常會被視為*預設主機*。每部虛擬主機都會繼承預設主機的組態。

若要編輯主機設定(又稱為*指示詞*)，請在表格中選擇適當項目，然後按一下「*編輯*」。若要新增指示詞，請按一下「*新增*」。若要刪除指示詞，請選取該指示詞，然後按一下「*刪除*」。

圖形 30.1 HTTP 伺服器精靈：預設主機



這是伺服器預設值的清單：

Document Root

目錄路徑，Apache 會從此路徑為此主機提供檔案。/srv/www/htdocs 是預設位置。

Alias

在配合 Alias 指示詞時，URL 可以映射到實體檔案系統位置。這表示某個路徑即使不在檔案系統的 Document Root 中，仍可藉由該路徑別名的 URL 進行存取。

預設的 SUSE Linux Enterprise Server Alias /icons 指向 /usr/share/apache2/icons，做為目錄索引檢視中顯示的 Apache 圖示。

ScriptAlias

功能相似於 Alias 指示詞，ScriptAlias 指示詞可以將 URL 映射到檔案系統位置。兩者差別在於 ScriptAlias 可以將目標目錄指定作為 CGI 位置，表示該 CGI 程序檔必須在該位置執行。

Directory

使用 Directory 設定時，您可以指定一組組態選項，只將其中的選項套用到特定目錄。

在此可以設定 /srv/www/htdocs、/usr/share/apache2/icons 和 /srv/www/cgi-bin 目錄的存取和顯示選項。其中預設值應該不需要進行改變。

Include

使用 Include 可以指定其他的組態檔案。預先設定的 Include 指示詞有兩個：/etc/apache2/conf.d/ 為外部模組隨附之組態檔所在的目錄。使用此指示詞時，此目錄中所有以 .conf 結尾的檔案都會包含在內。使用第二個指示詞時，/etc/apache2/conf.d/apache2-manual.conf，即 apache2-manual 組態檔將包含在內。

Server Name

這個項目可以指定用戶端用來聯絡網頁伺服器的預設 URL。請使用完全合格的網域名稱 (FQDN) 來連接 http://FQDN/ 的網頁伺服器或其 IP 位址。您不能在此選擇任意名稱 — 採用此名稱的伺服器必須是「已知」的。

Server Administrator E-Mail

伺服器管理員的電子郵件地址. 這個地址可顯示在 Apache 建立的錯誤頁面 (舉例說明)。

完成設定「預設主機」步驟後，請按一下「下一步」，繼續下一個組態步驟。

虛擬主機

在此步驟中，精靈會顯示已完成設定之虛擬主機的清單 (請參閱第 30.2.2.1 節「虛擬主機組態」[417頁])。如果在啟動 YaST HTTP 精靈之前尚未進行手動變更，則不會顯示虛擬主機。

若要新增主機，請按一下「新增」開啟對應的對話方塊，並在其中輸入主機的基本資訊，例如「伺服器名稱」、「伺服器內容根目錄」(DocumentRoot) 和「管理員電子郵件」。「伺服器解析」可用來決定主機的識別方式 (以名稱為基礎或是以 IP 為基礎)。透過「變更虛擬主機 ID」指定名稱或 IP 位址

按一下「下一步」，繼續進入虛擬主機組態對話方塊的第二部分。

在虛擬主機組態對話方塊的第二部分，您可以指定是否要啟用 CGI 程序檔，以及這些程序檔要使用哪個目錄。您也可以在此啟用 SSL。如果執行了這個動作，您就必須同時指定憑證的路徑。如需有關 SSL 和憑證的詳細資訊，請參閱第 30.6.2 節「設定提供 SSL 的 Apache」[444頁]。使用「目錄索引」選項，可以指定當用戶端要求目錄時要顯示哪個檔案 (預設為 index.html)。如果您要變更這個設定，請新增一個或多個檔名 (以空格分隔)。使用「啟用公用 HTML」時，使用者公用目錄 (~使用者/public_html/) 的內容就可由伺服器公開於 <http://www.example.com/~使用者上>。

重要：建立虛擬主機

您不能在此隨意新增虛擬主機。如果使用以名稱為基礎的虛擬主機，就必須在網路上解析每部主機名稱。如果是使用以 IP 為基礎的虛擬主機，每個可用 IP 位址就只能指派一部主機。

摘要

這是精靈的最後一個步驟。您可以在此處決定 Apache 伺服器啟動的方式和時間：開機時啟動或手動啟動。同時可檢視目前已完成之組態的簡短摘要。如果您接受目前設定，請按一下「完成」以完成組態設定。如果要變更某些設定，

請按「上一步」，直到出現您需要的對話方塊。按一下「*HTTP 伺服器進階組態*」便可開啟第 30.2.3.2 節「*HTTP 伺服器組態*」[425頁] 所介紹的對話方塊。

圖形 30.2 *HTTP 伺服器精靈：摘要*

30.2.3.2 HTTP 伺服器組態

「*HTTP 伺服器組態*」對話方塊可提供比精靈更多的組態調整 (精靈 只會在第一次設定網頁伺服器時執行)。其中包含下列要介紹的四個索引標籤。在此變更的任何組態選項都無法立即生效 — 您必須先按一下「**完成**」進行確認之後，它們才會生效。按一下「**中止**」，系統將不變更組態模組，並會捨棄您的變更。

傾聽連接埠和位址

在「*HTTP 服務*」中，選取執行 (「*啟用*」) 或停止 (「*停用*」) Apache。在「*傾聽埠*」中，「**新增**」、「**編輯**」或「**刪除**」可透過其使用伺服器的位址和連接埠。預設會在連接埠 80 上監聽所有介面。任何情況下都必須核取「**在防火牆中開啟埠**」，否則將無法從外部連接 Web 伺服器。只有在測試時，並且此時不須由外部網路存取 Web 伺服器，才可以關閉該連接埠。如果您有多個網路介面，請按一下「**防火牆細節...**」以指定應對何介面開啟連接埠。

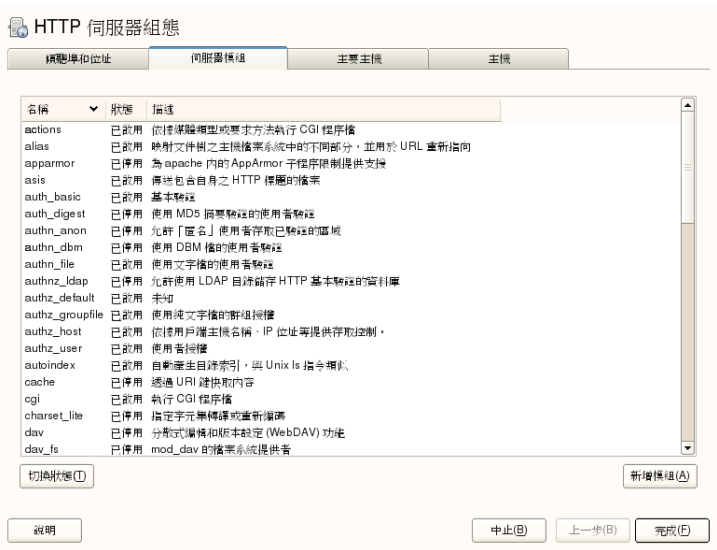
使用「記錄檔案」時，可檢視存取記錄或錯誤記錄。測試組態時此選項非常有用。記錄檔案會在另一個視窗中開啟，您也可以在此處重新啟動或重新載入 Web 伺服器。如需詳細資料，請參閱第 30.3 節「啟動和停止 Apache」[427 頁]。這些指令會立即生效，其記錄訊息也會即刻顯示。

圖形 30.3 HTTP 伺服器組態：傾聽連接埠和位址

伺服器模組

您可以按一下「切換狀態」，變更 Apache2 模組的狀態 (啟用或停用)。按一下「新增模組」，可新增已經安裝但是未列出的新模組。若要更進一步認識模組，請參閱第 30.4 節「安裝、啟用和設定模組」[429 頁]。

圖形 30.4 HTTP 伺服器組態：伺服器模組



主要主機

這些對話方塊相同於前面已介紹過的對話方塊。請參閱章節「預設主機」[422頁]和章節「虛擬主機」[424頁]。

30.3 啟動和停止 Apache

如果 Apache 是依照第 30.2.3 節「使用 YaST 設定 Apache」[421頁]中所述透過 YaST 來設定，它會於開機階段的執行層級 3 和 5 啟動，在執行層級 0、1、2 和 6 停止。您可以使用 YaST 的執行層級編輯器或指令行工具 `chkconfig` 來變更此行為。

若要在執行中的系統上啟動、停止或操作 Apache，請使用 `init` 程序檔 `/usr/sbin/rcapache2`。如需 `init` 程序檔的一般資訊，請參閱第 9.2.2 節「Init 程序檔」[100頁]。`rcapache2` 指令會接受下列參數：

狀態

檢查 Apache 是否已啟動。

`start`

啟動尚未執行的 Apache。

`startssl`

若採用 SSL 支援的 Apache 不在執行中，則將其啟動。如需更多有關 SSL 支援的詳細資訊，請參閱第 30.6 節「設定提供 SSL 的安全網頁伺服器」[439頁]。

停止

透過終止父處理程序來停止 Apache。

`restart`

停止 Apache，然後重新啟動。啟動之前並未在執行中的網頁伺服器。

`try-restart`

若 Apache 已在執行中，則將其停止並重新啟動。

`reload` 或 `graceful`

通知所有 Apache 衍生處理程序在關機之前先完成各自的要求，以停止網頁伺服器。每個程序結束後都會被一個新啟動的程序所取代，最終會將 Apache 完全「重新啟動」。

提示：在線上環境中重新啟動 Apache

若要啟用 Apache 組態中的變更而不引起連線中斷，請使用 `rcapache2 reload` 指令。

`restart-graceful`

啟動另一部可立即處理所有收到的要求的 Web 伺服器。Web 伺服器的上一個例項繼續處理所有現有的要求，持續時間為 `GracefulShutdownTimeout` 所設定的指定期間。

若要升級到新版本或變更需要重新啟動的組態選項，`rcapache2 restart-graceful` 十分有用。使用此選項可讓伺服器的停機時間降至最低。

必須設定 `GracefulShutdownTimeout`，否則 `restart-graceful` 將導致系統定期重新啟動。若設定為零，伺服器將無限期等待，直到所有剩餘的要求全部處理完為止。

若原始 Apache 例項無法清除所有必需的資源，則正常的重新啟動可能會失敗。在這種情況下，該指令將導致漸進式停止。

`stop-graceful`

於 `GracefulShutdownTimeout` 所設定的指定期間後停止 Web 伺服器，以確保系統可以完成現有的要求。

必須設定 `GracefulShutdownTimeout`，否則 `stop-graceful` 將導致系統定期重新啟動。若設定為零，伺服器將無限期等待，直到所有剩餘的要求全部處理完為止。

`configtest` 或 `extreme-configtest`

在不影響執行中之網頁伺服器的情況下，檢查組態檔案的語法。因為這項檢查會在每次伺服器啟動、重新載入或重新啟動時強制進行，所以通常並不需要明確執行該測試 (若發現有組態錯誤，Web 伺服器就不會完成啟動、重新載入或是重新啟動作業)。 `extreme-configtest` 選項會以使用者 `nobody` 的身分啟動 Web 伺服器並實際載入組態，因此系統可能會偵測到較多錯誤。請注意，雖然載入了組態，但是無法測試 SSL 設定，因為 `nobody` 無法讀取 SSL 證書。

`probe`

查探重新載入的重要性 (檢查組態是否有變更) 並建議 `rcapache2` 指令的必要引數。

`server-status` 和 `full-server-status`

分別傾印簡要或完整的狀態畫面。要求必須安裝 `lynx` 或 `w3m` 並啟用 `mod_status` 模組。除此之外，`status` 必須加入 `/etc/sysconfig/apache2` 檔案的 `APACHE_SERVER_FLAGS`。

提示：其他旗標

如果您為 `rcapache2` 指定其他旗標，這些旗標就會傳遞通過網頁伺服器。

30.4 安裝、啟用和設定模組

Apache 軟體採用了模組化設計：除了部分核心任務，其餘所有功能皆由模組處理。這種進步幅度很大，甚至連 HTTP 都是由模組 (`http_core`) 處理。

Apache 模組可以在建立階段編譯成 Apache 二進位檔案，或是在執行階段動態載入。如需瞭解如何動態載入模組的詳細資訊，請參閱第 30.4.2 節「啟用和停用」[431頁]。

Apache 模組可以分成四種不同類別：

基本模組

基本模組會依預設編譯到 Apache。SUSE Linux Enterprise Server 中的 Apache 僅編譯了 `mod_so` (用於載入其他模組) 與 `http_core`。所有其他模組均以共享物件的方式提供，即在執行期間加入，而不包含在伺服器二進位檔案中。

延伸模組

一般說來，Apache 軟體套件會包含標示為延伸的模組，但是通常不會使用靜態方式將這些模組編譯到伺服器中。在 SUSE Linux Enterprise Server 中，這類模組以共享物件方式提供，並可在執行時期載入到 Apache 中。

外部模組

標示為外部的模組不會包含於 Apache 正式發行版本中。不過，SUSE Linux Enterprise Server 提供了其中的一些模組。

多重處理模組 (MPM)

MPM 會負責接收和處理網頁伺服器所收到的要求，因此屬於網頁伺服器軟體的核心部分。

30.4.1 模組安裝

如果您已依照第 30.1.2 節「安裝」[412頁]中所述完成預設安裝，則下列模組此時都已安裝：所有基礎模組與延伸模組、多重處理模組 Prefork MPM 以及外部模組 `mod_php5` 與 `mod_python`。

您可以啟動 YaST 並依序選擇「軟體」>「軟體管理」，以安裝其他外部模組。現在，請依序選擇「過濾器」>「搜尋」，然後搜尋 *apache*。結果清單中除其他套件之外，還會包含所有可用的外部 Apache 模組。

30.4.2 啟用和停用

以手動方式或透過 YaST 啟動或取消啟動特定模組。在 YaST 中，若要啟用或停用程序檔語言模組 (PHP5、Perl 和 Python)，需要使用第 30.2.3.1 節「HTTP 伺服器精靈」[421頁]中所述的模組組態。所有其他模組都可以依據章節「伺服器模組」[426頁]說明步驟來啟用或停用。

如果您偏好手動啟用或停用模組，請分別使用 `a2enmod mod_foo` 或 `a2dismod mod_foo` 指令。`a2enmod -l` 會輸出目前所有的使用中模組清單。

重要：包含外部模組的組態檔案

如果您已經手動啟用外部模組，請確定將其組態檔案載入至所有的虛擬主機組態。外部模組的組態檔案會存放在 `/etc/apache2/conf.d/` 之下，而且不會預設載入。如果您需要在每個虛擬主機上載入相同模組，您可以含入此目錄中的 `*.conf`。另一種做法是含入個別檔案。如需取得範例說明，請參閱 `/etc/apache2/vhost.d/vhost.template`。

30.4.3 基本和延伸模組

Apache 說明文件中詳細介紹了所有的基本模組和延伸模組。本文件只提供最重要模組的概要說明。如需關於每個模組的詳細資訊，請參閱 <http://httpd.apache.org/docs/2.2/mod/>。

`mod_actions`

提供在需要特定 MIME 類型 (例如 `application/pdf`)、具有特定副檔名的檔案 (例如 `.rpm`) 或特定要求方法 (例如 `GET`) 時執行程序檔的方法。這是預設啟用的模組。

`mod_alias`

提供 `Alias` 和 `Redirect` 指示詞，供您用來將 URL 映射至特定目錄 (`Alias`) 或將所要求的 URL 重新導向至其他位置。這是預設啟用的模組。

`mod_auth*`

驗證模組提供了幾種不同的驗證方式：使用 `mod_auth_basic` 進行基本驗證，或使用 `mod_auth_digest` 進行摘要驗證。Apache 2.2 的摘要驗證方式仍屬實驗性質。

`mod_auth_basic` 和 `mod_auth_digest` 必須與驗證提供者模組 `mod_authn_*` (例如適用於基於文字檔案之驗證的 `mod_authn_file`) 以及驗證模組 `mod_authz_*` (例如適用於使用者驗證的 `mod_authz_user`) 結合使用。

關於此主題的詳細資訊，請參閱 <http://httpd.apache.org/docs/2.2/howto/auth.html> 上的驗證 *HOWTO*。

`mod_autoindex`

Autoindex 會在沒有任何索引檔案 (例如，`index.html`) 出現時產生目錄清單。這些索引的外觀可加以設定。這是預設啟用的模組。然而，目錄清單預設由 `Options` 指示詞停用 — 這會覆寫虛擬主機組態的此項設定。這個模組的預設組態檔案會存放在 `/etc/apache2/mod_autoindex-defaults.conf`。

`mod_cgi`

執行 CGI 程序檔時必須使用 `mod_cgi`。這是預設啟用的模組。

`mod_deflate`

使用這個模組時，Apache 可以設定成即時壓縮成指定檔案類型之後，再進行傳送。

`mod_dir`

mod_dir 可提供 `DirectoryIndex` 指示詞，供您用來設定當要求目錄 (預設是 `index.html`) 時要自動傳遞哪類檔案。它還提供另一項功能：當目錄要求沒有包含末尾斜線時，就會自動重新導向到正確 URL。這是預設啟用的模組。

`mod_env`

控制傳遞給 CGI 程序檔或 SSI 頁面的環境。可以在呼叫 `httpd` 程序的外圍程序中設定、取消設定或傳遞環境變數。這是預設啟用的模組。

`mod_expires`

使用 `mod_expires` 時，您可以透過傳送 `Expires` 標頭，來控制代理和瀏覽器快取重新整理文件的頻率。這是預設啟用的模組。

`mod_include`

`mod_include` 可讓您使用 `Server Side Include (SSI)`，這項工具會提供動態產生 HTML 頁面的基本功能。這是預設啟用的模組。

mod_info

可透過 <http://localhost/server-info/> 提供伺服器組態的綜合綜覽。基於安全性考量，您應該永遠限制這個 URL 的存取權限。預設只允許 localhost 存取這個 URL。mod_info 是在 `/etc/apache2/mod_info.conf` 中設定。

mod_log_config

使用此模組時，您可以設定 Apache 記錄檔案的外觀。這是預設啟用的模組。

mod_mime

此 mime 模組會依據傳送檔案的副檔名，來確定其是否包含正確的 MIME 標頭 (例如 HTML 文件為 `text/html`)。這是預設啟用的模組。

mod_negotiation

內容協商 (Content Negotiation) 所需的模組。如需更多詳細資訊，請參閱 <http://httpd.apache.org/docs/2.2/content-negotiation.html>。這是預設啟用的模組。

mod_rewrite

可提供 mod_alias 的功能，但具備更多功能和更大的靈活性。使用 mod_rewrite 時，您可以依據多個規則、要求標頭和其他條件來重新導向 URL。

mod_setenvif

根據用戶端的要求設定環境變數，如用戶端傳送的瀏覽器字串或用戶端的 IP 位址。這是預設啟用的模組。

mod_speling

mod_speling 會嘗試自動修正 URL 中出現的打字錯誤，例如大小寫錯誤。

mod_ssl

啟用網頁伺服器和用戶端之間的加密連線。如需詳細資料，請參閱 第 30.6 節「設定提供 SSL 的安全網頁伺服器」[439頁]。這是預設啟用的模組。

mod_status

可透過 <http://localhost/server-status/> 提供有關伺服器活動及效能的資訊。基於安全性考量，您應該永遠限制這個 URL 的存取權限。預設只允許 localhost 存取這個 URL。mod_status 是在 `/etc/apache2/mod_status.conf` 中設定。

`mod_suexec`

`mod_suexec` 可讓您以不同使用者和群組身分來執行 CGI 程序檔。這是預設啟用的模組。

`mod_userdir`

啟用在 `~user/` 之下提供使用者特定目錄。在組態中必須指定 `UserDir` 指示詞。這是預設啟用的模組。

30.4.4 多重處理模組

SUSE Linux Enterprise Server 提供了兩個不同的多重處理模組 (MPM) 與 Apache 配合使用：

- Prefork MPM [434頁]
- 第 30.4.4.2 節「Worker MPM」[434頁]

30.4.4.1 Prefork MPM

Prefork MPM 會實作非執行緒、預衍生的 Web 伺服器。這個模組會讓 Web 伺服器以類似 Apache 1.x 版的行為作業。在此版本中，Apache 會透過衍生出獨立的子程序，將各個要求分開處理。這樣發生問題的要求就不會影響其他要求，進而避免網頁伺服器出現鎖定現象。

雖然透過這種以處理程序為主的方法可以提供穩定性，但是比起 Worker MPM，Prefork MPM 會耗用較多的系統資源。Unix 作業系統會將 Prefork MPM 當作預設 MPM。

重要：本文件的 MPM

本文件會假設 Apache 是使用 Prefork MPM。

30.4.4.2 Worker MPM

Worker MPM 會提供多執行緒 Web 伺服器。執行緒是「輕量級」的處理程序。執行緒和處理程序相比的優點是，它消耗的資源較少。Worker MPM 不只會衍生子處理程序，它還可使用執行緒和伺服器處理程序，來為要求提供服務。預

衍生的子程序具有多重執行緒。這種方法因為耗用比 Prefork MPM 更少的系統資源，因此可以提高 Apache 的執行效能。

一個主要缺點就是 Worker MPM 的穩定性：當某執行緒毀損時，處理程序的所有執行緒都會受到影響。最嚴重的情況下，甚至還會造成伺服器當機。尤其是在負載量高的 Apache 上使用通用閘道介面 (CGI) 時，可能就會因線串無法與系統資源進行通訊而產生內部伺服器錯誤。在 Apache 上使用 worker MPM 的另外一點爭議，就是並非所有可用的 Apache 模組都能安全地使用執行緒，這樣就無法配合 worker MPM 使用。

警告：搭配 MPM 使用 PHP 模組

並非所有可用的 PHP 模組都是安全執行緒。因此最好不要搭配 worker MPM 來使用 mod_php。

30.4.5 外部模組

此處提供了 SUSE Linux Enterprise Server 隨附的所有外部模組清單。

mod-apparmor

為 Apache 提供額外支援，對由 mod_php5 和 mod_perl 這類模組處理的個別 CGI 程序檔設定 AppArmor 限制。

套件名稱：apache2-mod_apparmor

詳細資訊：第 IV 部分「Confining Privileges with AppArmor」(*↑Security Guide*)

mod_mono

mod_auth_kerb 提供對 Apache Web 伺服器的 Kerberos 驗證。

套件名稱：apache2-mod_auth_kerb

詳細資訊：<http://modauthkerb.sourceforge.net/configure.html>

mod_mono

使用 mod_mono 可讓您在伺服器中執行 ASP.NET 頁面。

套件名稱：apache2-mod_mono

組態檔案：/etc/apache2/conf.d/mod_mono.conf

mod_perl

mod_perl 可讓您使用內嵌解譯器來執行 Perl 程序檔。內嵌在伺服器的常駐解譯器可以避免因啟動外部解譯器造成的負荷，以及在 Perl 啟動階段時降低速度。

套件名稱：apache2-mod_perl

組態檔案：/etc/apache2/conf.d/mod_perl.conf

詳細資訊：/usr/share/doc/packages/apache2-mod_perl

mod_php5

PHP 是一種伺服器端、跨平台式的 HTML 內嵌程序檔語言。

套件名稱：apache2-mod_php5

組態檔案：/etc/apache2/conf.d/php5.conf

詳細資訊：/usr/share/doc/packages/apache2-mod_php5

mod_python

mod_python 允許在 Apache HTTP 伺服器中內嵌 Python，以便大幅提高效能和增加網頁應用程式的設計彈性。

套件名稱：apache2-mod_python

詳細資訊：/usr/share/doc/packages/apache2-mod_python

mod_security

mod_security 提供 Web 應用程式防火牆，用於保護 Web 應用程式免受各種攻擊。此外，它還支援 HTTP 流量監控和即時分析。

套件名稱：apache2-mod_security2

組態檔案：/etc/apache2/conf.d/mod_security2.conf

詳細資訊：/usr/share/doc/packages/apache2-mod_security2

文件：<http://modsecurity.org/documentation/>

30.4.6 編譯

Apache 允許進階使用者編寫自定模組進行延伸。若要開發 Apache 模組或編譯協力廠商模組，除了相對應開發工具外，還需要套件 apache2-devel。apache2-devel 也包含了 apxs2 工具，這是在編譯 Apache 其他模組時，需要用到的工具。

apxs2 可以從原始程式碼進行模組編譯和安裝(其中包括必要的組態檔案變更)，並建立可於 Runtime 載入 Apache 的動態共享物件(DSO)。

apxs2 二進位檔案位在 /usr/sbin 下方：

- /usr/sbin/apxs2 — 適合用來建立可配合任何 MPM 使用的延伸模組。安裝位置是 /usr/lib/apache2。
- /usr/sbin/apxs2-prefork — 適合用於 Prefork MPM 模組。安裝位置是 /usr/lib/apache2-prefork。
- /usr/sbin/apxs2-worker — 適用於 Worker MPM 模組。安裝位置是 /usr/lib/apache2-worker。

請使用下列指令透過原始碼安裝並啟用模組：

```
cd /path/to/module/source; apxs2 -cia  
    mod_foo.c
```

其中，-c 用於編譯模組，-i 用於安裝模組，-a 用於啟用模組。如需有關 apxs2 的其他選項資訊，請參閱 apxs2(1) man 頁面。

30.5 啟用 CGI 程序檔

Apache 的通用閘道介面 (CGI) 可讓您使用程式或程序檔 (通常指 CGI 程序檔) 建立動態內容。CGI 程序檔可以用任何程式設計語言來編寫。通常會使用類似 Perl 或 PHP 等程式檔設計語言。

若要讓 Apache 傳送 CGI 程序檔建立的內容，就必須啟用 mod_cgi 模組。同時還需要用到 mod_alias。這兩種都是預設啟用的模組。如需啟用模組的詳細資訊，請參閱第 30.4.2 節「啟用和停用」[431頁]。

警告：CGI 安全性

允許伺服器執行 CGI 程序檔會產生潛在的安全性弱點。請參考第 30.7 節「避免安全性問題」[446頁]，以取得其他資訊。

30.5.1 Apache 組態

在 SUSE Linux Enterprise Server 中，CGI 程序檔只能在 `/srv/www/cgi-bin/` 目錄中執行。這個位置已設定用來執行 CGI 程序檔。如果您已經建立虛擬主機組態 (請參閱第 30.2.2.1 節「虛擬主機組態」[417頁]) 並想要將程序檔放置到主機特定的目錄，則必須解除鎖定和設定此目錄。

範例 30.5 VirtualHost CGI 組態

```
ScriptAlias /cgi-bin/ "/srv/www/www.example.com/cgi-bin/"❶

<Directory "/srv/www/www.example.com/cgi-bin/">
    Options +ExecCGI❷
    AddHandler cgi-script .cgi .pl❸
    Order allow,deny❹
    Allow from all
</Directory>
```

- ❶ 告知 Apache 依照 CGI 程序檔方式來處理位在這個目錄中的所有檔案。
- ❷ 啟用 CGI 程序檔執行
- ❸ 告知伺服器依照 CGI 程序檔方式來處理包含 `.pl` 和 `.cgi` 副檔名的檔案。依據個人需要來加以調整。
- ❹ `Order` 和 `Allow` 指示詞可控制評估 `Allow` 和 `Deny` 指示詞時的預設存取狀態和順序。在這個範例中，會先評估 `deny` 陳述式，接著才評估 `allow` 陳述式，並啟用通用存取。

30.5.2 執行程序檔範例

CGI 程式設計不同於「一般」程式設計；因為 CGI 程式和程序檔的最前面必須是 MIME-Type 標頭，例如 `Content-type: text/html`。這個標頭會傳送到用戶端，使其瞭解所接收內容的類型。其次，程序檔的輸出必須是用戶端 (通常是指 Web 瀏覽器) 可瞭解的內容 — 舉例來說，在多數情況下是指 HTML、純文字或影像。

Apache 套件會在 `/usr/share/doc/packages/apache2/test-cgi` 提供簡單的測試程序檔。這個程序檔會以純文字方式輸出部分環境變數的內容。請將這段程序檔複製到 `/srv/www/cgi-bin/` 或是虛擬主機的程序檔目錄 (`/srv/www/example.com/cgi-bin/`)，並將其命名為 `test.cgi`。

可由 Web 伺服器存取的檔案應該屬於 `root` 使用者所有。如需其他資訊，請參閱第 30.7 節「避免安全性問題」[446頁]。因為網頁伺服器可由不同使用者身分

執行，所以 CGI 程序檔必須具備可供全球執行和可供全球讀取等特性。變更 CGI 目錄和使用 `chmod 755 test.cgi` 指令，便可套用適當的許可權。

現在，請呼叫 `http://localhost/cgi-bin/test.cgi` 或 `http://www.example.com/cgi-bin/test.cgi`。這時應該會顯示「CGI/1.0 測試程序檔報告」。

30.5.3 CGI 疑難排解

如果這時沒有顯示測試程式的輸出結果，而是出現錯誤訊息，請檢查下列項目：

CGI 疑難排解

- 您是否有在變更組態之後重新載入伺服器？請使用 `rcapache2 probe` 進行檢查。
- 您是否已正確設定自定的 CGI 目錄 (若有的話)？如果您不確定，請在預設的 CGI 目錄 `/srv/www/cgi-bin/` 中測試此程序檔，並使用 `http://localhost/cgi-bin/test.cgi` 進行呼叫。
- 檔案許可權是否正確？請切換至 CGI 目錄並執行 `ls -l test.cgi`。此測試輸出開頭應該是

```
-rwxr-xr-x 1 root root
```
- 請確定程序檔沒有包含任何程式設計錯誤。如果您未變更過 `test.cgi`，此情況應該就不會發生，但是如果您是使用自己的程式，請務必確定這些程式中沒有任何程式設計錯誤。

30.6 設定提供 SSL 的安全網頁伺服器

如果 Web 伺服器和用戶端之間會傳輸信用卡資訊等敏感性資料，最好使用需經過驗證的安全加密連線。`mod_ssl` 會為用戶端和網頁伺服器之間的 HTTP 通訊，提供使用安全通訊端層 (Secure Sockets Layer, SSL)、以及傳輸層安全性 (Transport Layer Security, TLS) 通訊協定的強式加密。使用 SSL/TLS 時，網頁伺服器和用戶端之間就會建立私人連線。如此便可確保資料完整性，使用戶端和伺服器端可以彼此進行驗證。

為了完成這個目的，伺服器會在回覆任何 URL 要求之前，先傳送可證明伺服器有效身分之相關資訊的 SSL 憑證。如此即可確保該伺服器是此通訊的唯一正確端點。此外，該憑證會在用戶端和伺服器端建立加密連線，以便在沒有洩漏敏感、純文字內容的風險情況下傳輸資訊。

`mod_ssl` 本身不會實作 SSL/TSL 通訊協定，而是扮演 Apache 和 SSL 程式庫之間的介面。在 SUSE Linux Enterprise Server 中是使用 OpenSSL 程式庫。OpenSSL 會自動隨 Apache 完成安裝。

使用 `mod_ssl` 搭配 Apache 的最明顯特徵，就是 URL 的字首都會加上 `https://`，而不是 `http://`。

提示：範例證書

安裝 `apache2-example-certificates` 套件時，可以使用一家假定公司「Snake Oil」的範例證書。

30.6.1 建立 SSL 憑證

為了搭配使用 SSL/TSL 與網頁伺服器，您必須建立 SSL 憑證。網頁伺服器和用戶端在彼此驗證時要用到這項憑證，以便讓任一方可以清楚識別對方。為了確保憑證的完整性，其必須由每位使用者信任的一方加以簽章。

您可以建立下列三種類型的憑證：僅供測試使用的「虛擬」憑證、供已定義信任圈使用者使用的自我簽發憑證，以及由獨立、公開的憑證授權機構(CA)簽發的憑證。

憑證建立基本上可分為兩個步驟。首先產生憑證授權機構的私密金鑰，接著再使用該金鑰簽發伺服器憑證。

提示：如需更多資訊

若要更進一步蓋識 SSL/TSL 的概念和定義，請參閱 http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html。

30.6.1.1 建立「虛擬」憑證

產生虛構憑證的步驟很簡單。您只要呼叫程序檔 `/usr/bin/gensslcert`，此操作會建立或覆寫下列檔案。使用 `gensslcert` 的可選參數可以校調證書。如需詳細資訊，可呼叫 `/usr/bin/gensslcert -h`。

- `/etc/apache2/ssl.crt/ca.crt`
- `/etc/apache2/ssl.crt/server.crt`
- `/etc/apache2/ssl.key/server.key`
- `/etc/apache2/ssl.csr/server.csr`
- `/root/.mkcert.cfg`

`ca.crt` 的複製本也會放在 `/srv/www/htdocs/CA.crt` 提供下載。

重要：僅供測試之用

虛構憑證絕對不可用於生產環境系統。這類憑證只能用於測試目的。

30.6.1.2 建立自我簽發憑證

如果您要設定供內部網路或已定義使用者圈使用的安全 Web 伺服器，透過您自己的憑證管理中心 (CA) 簽發憑證就可有效符合此時的憑證需求。

自我簽署憑證的建立程序分為互動的九個步驟。請切換至目錄 `/usr/share/doc/packages/apache2`，並執行下列指令：`./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/ custom`。請勿嘗試從這個目錄外面執行這個指令。這個程式會提供一系列提示訊息，其中有部分提示需要使用者輸入。

過程 30.4 使用 `mkcert.sh` 建立自我簽發憑證

1 決定憑證所使用的簽章演算法

選擇 RSA (R，此為預設選項)，因為有些早期瀏覽器無法使用 DSA。

2 產生 CA 的 RSA 私密金鑰 (1024 位元)

這時不須進行任何互動。

3 產生 CA 的 X.509 憑證簽發要求

在此建立 CA 的可辨識名稱。這時系統會要求您回答一些問題，例如國家/地區名或組織名稱。請輸入有效資料，因為您在此輸入的每項資料將來都會顯示在憑證中。您不需要回答每個問題。如果有不適用的問題或是您希望保留空白，請使用「.」。通用名稱是指 CA 本身的名稱 — 請選擇明顯的名稱，例如 *My company CA*。

重要：CA 的通用名稱

CA 的通用名稱必須區別於伺服器的通用名稱，因此不要在此步驟中選擇完全合格的主機名稱。

4 產生 CA 本身簽發的 X.509 憑證

選擇憑證版本 3 (預設選項)。

5 產生 SERVER 的 RSA 私密金鑰 (1024 位元)

這時不須進行任何互動。

6 產生 SERVER 的 X.509 憑證簽發要求

在此建立伺服器金鑰的可識別名稱。這時要回答的問題與建立 CA 可識別名稱時回答的問題幾乎一樣。在此輸入的資料會套用到網頁伺服器，因此不需要和 CA 資料完全相同 (例如，伺服器可能會出於任意位置)。

重要：選取通用名稱

您在此輸入的通用名稱必須是安全伺服器的完全合格主機名稱 (例如，www.example.com)。否則瀏覽器會在存取網頁伺服器時發出警告，表示憑證與伺服器不相符。

7 產生本身 CA 簽發的 X.509 憑證

選擇憑證版本 3 (預設選項)。

8 使用密碼片語為 CA 的 RSA 私密金鑰加密，以提高安全性

我們強烈建議您使用密碼來加密 CA 的私密金鑰，請選擇 Y 來輸入密碼。

9 使用密碼片語為 SERVER 的 RSA 私密金鑰加密，以提高安全性

若使用密碼為伺服器金鑰加密，則每當要啟動網頁伺服器時就必須輸入這個密碼。如此一來就很難自動在開機時啟動伺服器或是重新啟動網頁伺服器。因此，使用者通常會在回答這個問題時選擇 N。請注意金鑰在沒有使用密碼加密時是不受保護狀態，同時請確定只有經授權人員可以存取該金鑰。

重要：加密伺服器金鑰

如果您選擇使用密碼為伺服器金鑰進行加密，請為存放在 `/etc/sysconfig/apache2` 的 `APACHE_TIMEOUT` 提高設定值。否則，您在嘗試啟動伺服器之前可能來不及輸入密碼片語，但是伺服器早就啟動失敗而停止。

程序檔的結果頁面會出現憑證清單，以及其所產生的金鑰。不同於程序檔輸出的結果，這些檔案並不是產生到本地目錄 `conf`，而是產生到 `/etc/apache2/` 下面的正確目錄。

最後一個步驟就是從 `/etc/apache2/ssl.crt/ca.crt` 將 CA 憑證檔案複製到使用者可存取的位置，以便使用者將該檔案納入其網頁瀏覽器已知和信任的 CA 清單中。否則，瀏覽器會報告該憑證是由不明授權機構所簽發。這類憑證的有效期限是一年。

重要：自行簽署的證書

僅在供認識您、且信任您為證書管理中心之使用者存取的網頁伺服器上，方可使用自我簽署憑證。我們不建議您在公開商店等場所使用此類證書。

30.6.1.3 取得官方簽發憑證

目前有一些可簽署憑證的官方證書管理中心。這類憑證是由值得信任的協力廠商所簽署，因此可以完全信任。對外運作的安全網頁伺服器通常已取得官方簽發憑證。

最有名的官方 CA 是 Thawte (<http://www.thawte.com/>) 或 Verisign (<http://www.verisign.com>)。這些 CA 和其他 CA 都已經編譯到所有瀏覽器中，所以瀏覽器會自動接受這些憑證授權機構簽發的憑證。

在要求官方簽署的憑證時，您並不需要向 CA 傳送憑證，而只需傳送憑證簽署要求 (Certificate Signing Request, CSR)。若要建立 CSR，請呼叫程序檔
`/usr/share/ssl/misc/CA.sh -newreq。`

首先，程序檔會要求提供該 CSR 進行加密時所使用的密碼。接著，要求您輸入可識別名稱。這時系統會要求您回答一些問題，例如國家/地區名或組織名稱。請輸入有效資料——您在此輸入的每項資料將來都會顯示在憑證中並用於檢查。您不需要回答每個問題。如果有不適用的問題或是您希望保留空白，請使用「.」。通用名稱是指 CA 本身的名稱——請選擇明顯的名稱，例如 *My company* CA。最後，必須輸入挑戰密碼和替用的公司名稱。

從您呼叫程序檔的目錄中找出此 CSR。這個檔案名稱是 `newreq.pem`。

30.6.2 設定提供 SSL 的 Apache

在網頁伺服器端上，SSL 和 TLS 要求的預設連接埠是 443。同時有傾聽連接埠 80 的「一般」Apache 和傾聽連接埠 443 之已啟用 SSL/TLS 的 Apache，並不會產生衝突。事實上，HTTP 和 HTTPS 可以執行相同的 Apache 例項。常這時會使用不同的虛擬主機，將連接埠 80 和連接埠 443 的要求分派到不同的虛擬伺服器。

重要：防火牆組態

請不要忘記為連接埠 443 上已啟用 SSL 的 Apache 開啟防火牆。您可以依據第 15.4.1 節「Configuring the Firewall with YaST」(第 15 章「*Masquerading and Firewalls*」, ↑*Security Guide*) 所述方式，透過 YaST 完成這個動作。

在全域伺服器組態中，預設會啟用 SSL 模組。如果主機上停用了該模組，請使用 `a2enmod ssl` 指令將其啟用。若最終要啟用 SSL，需使用旗標「SSL」啟動伺服器。此時，請呼叫 `a2enflag SSL`。如果選擇使用密碼來加密伺服器證書，您還需要提高 `/etc/sysconfig/apache2` 中 `APACHE_TIMEOUT` 的設定值，以便您在啟動 Apache 時有足夠的時間輸入該密碼片語。請重新啟動伺服器來確保這些變更生效。只是重新載入並無法保證變更生效。

虛擬主機組態目錄包含了樣板 `/etc/apache2/vhosts.d/vhost-ssl.template` 和 SSL 特定指示詞 (將提供詳細文件說明)。如需一般虛擬主機組態的詳細資訊，請參閱第 30.2.2.1 節「虛擬主機組態」[417頁]。

若要開始，請將樣板複製到 `/etc/apache2/vhosts.d/mySSL-host.conf` 並進行編輯。充分調整下列指示詞的值：

- DocumentRoot
- ServerName
- ServerAdmin
- ErrorLog
- TransferLog

30.6.2.1 以名稱為基礎的虛擬主機和 SSL

依預設，在只有一個 IP 位址的伺服器上，無法同時執行多個啟用了 SSL 的虛擬主機。以名稱為基礎的虛擬主機需要 Apache 瞭解所要求的伺服器名稱。使用 SSL 連線的問題在於，此類要求只能在使用預設虛擬主機建立了 SSL 連線後才能讀取。如此一來，使用者將會收到證書與伺服器名稱不符的警告訊息。

SUSE Linux Enterprise Server 提供了一項 SSL 通訊協定的延伸：伺服器名稱指示 (Server Name Indication, SNI)。該項延伸會在 SSL 協議中傳送虛擬網域的名稱，以此解決這個問題。這可讓伺服器早些「切換」至正確的虛擬網域，並在瀏覽器中顯示正確的證書。

SUSE Linux Enterprise Server 上預設會啟用 SNI。若要針對 SSL 啟用以名稱為基礎的虛擬主機，請依照章節「以名稱為基礎的虛擬主機」[418頁]中所述設定伺服器 (請注意，您需要對 SSL 連線使用連接埠 443 而非 80)。

重要：SNI 瀏覽器支援

用戶端上也必須支援 SNI。儘管大多數的瀏覽器都支援 SNI，但一些用於行動硬體的瀏覽器以及 Internet Explorer 和 Windows* XP 上的 Safari 不支援 SNI。如需詳細資料，請參閱 http://en.wikipedia.org/wiki/Server_Name_Indication。

請使用指示詞 `SSLStrictSNIVHostCheck` 設定如何處理不支援 **SNI** 的瀏覽器。若在伺服器組態中設定為 `on`，則不支援 **SNI** 的瀏覽器對所有虛擬主機的存取都會遭到拒絕。若在某個 `VirtualHost` 指示詞中設定為 `on`，則對於此特定主機的存取將遭到拒絕。

若在伺服器組態中設定為 `off`，則伺服器將表現為不支援 **SNI**。**SSL** 要求將由為連接埠 443 定義的第一個虛擬主機處理。

30.7 避免安全性問題

向公用網際網路公開的網頁伺服器，必須持續進行系統管理。軟體和意外的錯誤設定不可避免地會產生安全性問題。下面是可用來處理這些問題的幾項秘訣。

30.7.1 更新軟體

SUSE 會在發現 Apache 軟體弱點時，發出安全性建議事項。其中包含應儘速套用的弱點修正指示。請由下列位置取得 SUSE 安全性公告：

- 網頁 <http://www.novell.com/linux/security/securitysupport.html>
- 郵寄清單歸檔 <http://lists.opensuse.org/opensuse-security-announce/>
- **RSS Feed** http://www.novell.com/linux/security/suse_security.xml

30.7.2 DocumentRoot 許可權

依預設，在 SUSE Linux Enterprise Server 中，`DocumentRoot` 目錄 `/srv/www/htdocs` 與 `CGI` 目錄 `/srv/www/cgi-bin` 的所有權屬於 `root` 使用者和群組。這些許可權不可變更。如果目錄對所有人開放寫入權限，則任何使用者都可以將檔案放入其中。然後，這些檔案可能會由具有 `wwwrun` 許可權的 Apache 執行，而這種情況可能會造成使用者取得非預期的檔案系統資源存取權限。使用

`/srv/www` 子目錄來存放虛擬主機的 `DocumentRoot` 和 `CGI` 目錄，並確定這些目錄所有權屬於 `root` 使用者和群組。

30.7.3 檔案系統存取

依預設，`/etc/apache2/httpd.conf` 已設定成拒絕存取整個檔案系統。切勿覆寫這些指示詞，不過您可以特別啟用 `Apache` 應當能夠讀取之所有目錄的存取權限。如需詳細資料，請參閱章節「基本虛擬主機組態」[420頁]。如果要執行這個動作，請確保沒有任何重要檔案 (例如密碼或系統組態檔案) 可由外界進行讀取。

30.7.4 CGI 程序檔

使用 `Perl`、`PHP`、`SSI` 或是任何其他程式設計語言的互動式程序檔，基本上都可以執行任意指令，因此會產生常見的安全性問題。將從伺服器執行的程序檔，只能由伺服器管理員信任的來源進行安裝——通常最好不要讓使用者執行他們自己的程序檔。同時建議您為所有程序檔進行安全性稽核。

為了盡可能簡化程序檔的管理工作，通常建議您限制 `CGI` 程序檔在特定目錄中執行，而不是全域性開放執行。您可以使用 `ScriptAlias` 和 `Option ExecCGI` 指示詞來進行組態設定。`SUSE Linux Enterprise Server` 的預設組態不允許隨處執行 `CGI` 程序檔。

所有 `CGI` 程序檔都是以相同使用者身分執行，所以不同的程序檔彼此之間可能會產生衝突。`module suEXEC` 可讓您以不同使用者和群組身分來執行 `CGI` 程序檔。

30.7.5 使用者目錄

在啟用使用者目錄 (使用 `mod_userdir` 或 `mod_rewrite`) 時，您應該審慎考慮不要允許覆寫 `.htaccess` 檔案，因為這會允許使用者覆寫安全性設定。至少您應該使用 `AllowOverride` 指示詞來限制使用者的應用範圍。在 `SUSE Linux Enterprise Server` 中，`.htaccess` 檔案預設為啟用狀態，但是使用者在使用 `mod_userdir` 時不能覆寫任何 `Option` 指示詞 (請參閱 `/etc/apache2/mod_userdir.conf` 組態檔案)。

30.8 疑難排解

如果 Apache 未啟動，網頁就無法存取，或者使用者無法連接網頁伺服器，因此找出問題的根源是很重要的工作。下面是您可在其中尋找錯誤原因的幾個常見位置以及需要檢查的重點：

rcapache2 的輸出

請不要使用二進位檔 `/usr/sbin/httpd2` 啟動和停止 Web 伺服器，而應使用 `rcapache2` 程序檔 (如第 30.3 節「啟動和停止 Apache」[427頁] 中所述)。該程序檔會對錯誤進行詳細說明，甚至會提供一些修復組態錯誤的祕訣與提示。

記錄檔案與詳細層級

無論發生了嚴重錯誤還是非嚴重錯誤，都可以檢查 Apache 記錄檔案尋找原因，主要檢查預設位於 `/var/log/apache2/error_log` 的錯誤記錄檔案。此外，如果需要檢視記錄檔案中更多的詳細資訊，還可以透過 `LogLevel` 指示詞來控制記錄訊息的詳細程度。

提示：簡單測試

請使用 `tail -F /var/log/apache2/my_error_log` 指令來檢視 Apache 記錄訊息。然後執行 `rcapache2 restart`。現在，請嘗試連接到瀏覽器，並檢查輸出結果。

防火牆與連接埠

一個常見的錯誤是，沒有在伺服器的防火牆組態中開啟 Apache 的連接埠。如果是使用 YaST 來設定 Apache，可以透過一個單獨的選項來檢查這個特定問題 (請參閱第 30.2.3 節「使用 YaST 設定 Apache」[421頁])。如果您要手動設定 Apache，請透過 YaST 防火牆模組來開啟 HTTP 和 HTTPS 的連接埠。

如果無法透過這些功能來查出錯誤原因，則請查閱 http://httpd.apache.org/bug_report.html 的線上 Apache 錯誤資料庫。此外，也可以從 <http://httpd.apache.org/userslist.html> 取得可用的郵件清單，聯絡 Apache 使用者社群。推薦的新聞群組是 comp.infosystems.www.servers.unix。

30.9 如需更多資訊

apache2-doc 套件在許多位置包含了完整的 Apache 手冊，用於本地安裝及作為參考文件。這個套件不是預設安裝選項 — 安裝此套件的最快方式就是使用 `zypper in apache2-doc` 指令。完成安裝之後，您就可以從 <http://localhost/manual/> 使用 Apache 手冊。您也可以從 <http://httpd.apache.org/docs-2.2/> 網站位置來存取這份手冊。`/usr/share/doc/packages/apache2/README.*` 目錄會提供 SUSE 特定組態秘訣資訊。

30.9.1 Apache 2.2

如需 Apache 2.2 最新功能的清單，請參閱 http://httpd.apache.org/docs/2.2/new_features_2_2.html。如需從 2.0 升級至 2.2 版的資訊，請參閱下列網址資訊：<http://httpd.apache.org/docs-2.2/upgrading.html>。

30.9.2 Apache 模組

有關第 30.4.5 節「外部模組」[435頁] 中簡要介紹的外部 Apache 模組的詳細資訊，可在以下位置找到：

`mod-apparmor`

<http://en.opensuse.org/SDB:AppArmor>

`mod-auth_kerb`

<http://modauthkerb.sourceforge.net/>

`mod_mono`

http://www.mono-project.com/Mod_mono

`mod_perl`

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

`mod_php5`

<http://www.php.net/manual/en/install.unix.apache2.php>

mod_python
<http://www.modpython.org/>

mod_security
<http://modsecurity.org/>

30.9.3 開發

如需更多有關開發 Apache 模組或是參與 Apache 網頁伺服器計畫的詳細資訊，請參閱下列主題內容：

Apache 開發人員資訊
<http://httpd.apache.org/dev/>

Apache 開發人員說明文件
<http://httpd.apache.org/docs/2.2/developer/>

使用 Perl 和 C 來編寫 Apache 模組
<http://www.modperl.com/>

30.9.4 其他資源

如果您在 SUSE Linux Enterprise Server 中遇到與 Apache 有關的問題，請查閱「技術資訊搜尋」，網址為：<http://www.novell.com/support>。關於 Apache 的歷程，請參閱http://httpd.apache.org/ABOUT_APACHE.html。此頁面也說明稱伺服器為 Apache 的原因。

使用 YaST 設定 FTP 伺服器

使用 YaST 的「*FTP 伺服器*」模組，可以將機器設定為 FTP (檔案傳輸通訊協定) 伺服器。匿名和/或驗證使用者可以連接至您的機器並使用 FTP 通訊協定下載檔案，還可以將檔案上載至 FTP 伺服器 (視組態而定)。YaST 為您系統上安裝的各個 FTP 伺服器精靈提供了統一的組態介面。

您可以使用 YaST 的「*FTP 伺服器*」組態模組設定兩個不同的 FTP 伺服器精靈：

- vsftpd (非常安全的 FTP 精靈) 和
- pure-ftpd

只能設定已安裝的伺服器。

vsftpd 與 pure-ftpd 伺服器中所含的組態選項略有不同，特別是在「*進階設定*」對話方塊中。本章介紹了 vsftpd 伺服器的設定。

如果無法在系統中使用「YaST FTP 伺服器」模組，請安裝 `yast2-ftp-server` 套件。

若要使用 YaST 設定 FTP 伺服器，請執行以下步驟：

- 1 開啟「YaST 控制中心」並選擇「*網路服務*」>「*FTP 伺服器*」，或以 root 身份執行 `yast2 ftp-server` 指令。

- 2 如果系統中未安裝任何 FTP 伺服器，系統將在「YaST FTP 伺服器」模組啟動時詢問您要安裝哪個伺服器。選擇一個伺服器然後確認對話方塊。如果安裝了兩個伺服器，請選擇首選的伺服器，然後按一下「確定」。
- 3 在「啟動」對話方塊中，設定啟動 FTP 伺服器的相關選項。如需詳細資訊，請參閱第 31.1 節「啟動 FTP 伺服器」[452頁]。

在「一般」對話方塊中，設定 FTP 目錄、歡迎訊息、檔案建立遮罩和各種其他參數。如需詳細資訊，請參閱第 31.2 節「FTP 一般設定」[453頁]。

在「效能」對話方塊中，設定會影響 FTP 伺服器負載的參數。如需詳細資訊，請參閱第 31.3 節「FTP 效能設定」[454頁]。

在「驗證」對話方塊中，設定匿名和/或已驗證的使用者是否可使用 FTP 伺服器。如需詳細資訊，請參閱第 31.4 節「驗證」[454頁]。

在「進階設定」對話方塊中，設定 FTP 伺服器的操作模式、SSL 連線與防火牆設定。如需詳細資訊，請參閱第 31.5 節「進階設定」[455頁]。

- 4 按「完成」以儲存這些組態。

31.1 啟動 FTP 伺服器

在「*FTP 啟動*」對話方塊的「服務啟動」框架中，可以設定 FTP 伺服器的啟動方式。您可以選擇在系統開機時自動啟動伺服器，或是手動啟動伺服器。如果 FTP 伺服器只能在提出 FTP 連線要求之後啟動，請選擇「透過 *xinetd*」。

FTP 伺服器的目前狀態將顯示在「*FTP 啟動*」對話方塊的「開啟與關閉」框架中。按一下「立即啟動 *FTP*」可以啟動 FTP 伺服器。若要停止伺服器，可按一下「立即停止 *FTP*」。變更伺服器的設定後，請按一下「儲存設定並立即重新啟動 *FTP*」。如果按一下「完成」離開組態模組，組態將儲存。

「*FTP 啟動*」對話方塊的「選取的服務」框架顯示所使用的 FTP 伺服器：*vsftpd* 或 *pure-ftpd*。如果兩個伺服器均已安裝，可以在兩者之間切換——目前的組態會自動轉換。

圖形 31.1 FTP 伺服器組態 — 啟動



31.2 FTP 一般設定

在「*FTP 一般設定*」對話方塊的「一般設定」框架中，您可以設定連接至 FTP 伺服器後將會顯示的「歡迎訊息」。

如果核取「*Chroot 每一個*」選項，則所有本地使用者登入後都將進入其主目錄中的 Chroot Jail。此選項含安全性要求，特別是當使用者具有上載權限或外圍程序存取權限時，因此啟用此選項時請務必小心。

如果核取「*詳細記錄*」選項，則將記錄所有 FTP 請求與回應。

您可以透過 Umask 對由匿名和/或已驗證的使用者建立之檔案的權限加以限制。請在「*匿名使用者 Umask*」中為匿名使用者設定檔案建立遮罩，並在「*已驗證使用者 Umask*」中為已驗證的使用者設定檔案建立遮罩。應以八進位數字(前面加零)輸入遮罩。如需有關 umask 的詳細資訊，請參閱 umask 的 man 頁面 (man lp umask)。

在「*FTP 目錄*」框架中設定用於匿名使用者與已驗證使用者的目錄。按一下「*瀏覽*」可從本地檔案系統選取要使用的目錄。對於匿名使用者，預設 FTP 目錄為 /srv/ftp。請注意，vsftpd 不允許所有使用者都可以寫入此目錄，而會為匿名使用者建立具有寫入權限的子目錄 upload。

注意：FTP 目錄的寫入權限

pure-ftpd 伺服器允許匿名使用者可以寫入 FTP 目錄。在兩個伺服器間切換時，請確定在切換回 vsftpd 伺服器之前，已移除曾用於 pure-ftpd 之目錄中的寫入權限。

31.3 FTP 效能設定

在「效能」對話方塊中，設定會影響 FTP 伺服器負載的參數。「最大閒置時間」表示遠端用戶端在兩個 FTP 指令之間等待的最長時間 (以分鐘計)。如果發生了更長時間的閒置，將中斷遠端用戶端的連線。「同一個 IP 最大用戶端數」決定可從單一 IP 位址連接的最大用戶端數目。「最大用戶端數」決定可以連接的最大用戶端數目。任何額外用戶端都將收到一則錯誤訊息。

可在「最大本地速率」和「最大匿名速率」中分別為本地已驗證的使用者及匿名用戶端設定最大資料傳輸速率。速率設定的預設值為 0，表示資料傳輸速率無限制。

31.4 驗證

在「驗證」對話方塊的「啟用/停用匿名使用者和本地使用者」框架中，您可以設定允許存取 FTP 伺服器的使用者。您還可以從以下選項中進行選擇：僅授予匿名使用者存取權限、僅授予驗證使用者 (擁有系統帳戶) 存取權限，或者同時授予這兩類使用者存取權限。

若要允許使用者上載檔案至 FTP 伺服器，請核取「驗證」對話方塊之「上載」框架中的「啟用上載」。在此處核取對應的方塊後，您就可以允許包括匿名使用者在內的使用者上載或建立目錄。

注意：vsftp—允許匿名使用者上載檔案

如果使用的是 vsftpd 伺服器而您希望匿名使用者能夠上載檔案或建立目錄，則需要在匿名 FTP 目錄中為所有使用者建立具有寫入權限的子目錄。

31.5 進階設定

FTP 伺服器既可以在主動模式中執行，也可以在被動模式中執行。依預設伺服器在被動模式中執行。若要切換至主動模式，只需取消核取「*進階設定*」對話方塊中的「*啟用被動模式*」選項。您還可以調整「*被動模式的最小連接埠*」與「*被動模式的最大連接埠*」選項來變更伺服器上用於資料流的連接埠範圍。

若要在用戶端與伺服器之間使用加密通訊，可以選取「*啟用 SSL*」。檢查要支援之協定的版本，並指定用於 SSL 加密連線的 DSA 證書。

如果系統受防火牆保護，請核取「*在防火牆中開啟埠*」以啟用到 FTP 伺服器的連線。

31.6 更多資訊

如需有關 FTP 伺服器的詳細資訊，請參閱 pure-ftpd、vsftpd 與 vsftpd.conf 的手冊頁。

Squid 代理伺服器

Squid 是 Linux 與 UNIX 平台普遍使用的代理快取。這表示它會將要求的網際網路物件 (例如網頁伺服器或 FTP 伺服器上的資料), 儲存在比伺服器更接近要求工作站的機器上。您可設定多階層, 以確保即使在終端使用者無法察覺的模式中, 也能達到最佳的反應時間及較低的頻寬使用率。您可使用其他軟體如 squidGuard, 以過濾網路內容。

Squid 可做為代理快取記憶體。它會將物件要求從用戶端 (在此例中是從網頁瀏覽器) 重新導向至伺服器。當從伺服器而來的要求物件到達時, 它會將物件傳送到用戶端, 並在硬碟快取記憶體中保留物件的副本。快取的其中一個優點為, 當有數個用戶端要求相同的物件時, 可從硬碟快取記憶體來提供。這可讓用戶端比從網際網路更快地擷取資料。這個程序也可以減少網路流量。

除了實際快取之外, Squid 還提供眾多功能, 例如將負載分散到互相通訊的代理伺服器階層、為所有存取代理的用戶端定義嚴格的存取控制清單、允許或拒絕使用其他應用程式來存取特定網頁, 以及產生經常瀏覽之網頁的統計資料, 以評估使用者的瀏覽習慣。Squid 不是一般的代理。一般而言, 它只會代理 HTTP 連線。此外, 也支援 FTP、Gopher、SSL 以及 WAIS 等通訊協定, 但不支援其他網際網路通訊協定, 例如 Real Audio、新聞或視訊會議。因為 Squid 只支援 UDP 通訊協定提供不同快取之間的通訊, 許多其他的多媒體程式並不支援。

32.1 關於代理快取的說明

當 Squid 做為代理快取記憶體時, 使用方法有多種。若與防火牆合併, 它有助於提高安全性。多個代理可一起使用。它也可以判斷應該快取物件類型和持續的時間長短。

32.1.1 Squid 以及安全性

Squid 可與防火牆配合使用，以便使用代理快取記憶體來保護內部網路不受外部的存取。防火牆將會拒絕所有的用戶端存取 Squid 以外的外部服務。所有的網路連線都必須由代理來建立。藉由這種組態方式，Squid 可完全控制網頁存取。

如果防火牆組態包含 DMZ，則代理應在此區域中操作。第 32.5 節「設定操作順暢的代理」[467頁]將描述如何執行「透明」代理。這簡化了用戶端的組態，因為在此情況下，它們不需要有關代理的任何資訊。

32.1.2 多個快取

經過設定之後，可在多個 Squid 例項之間交換物件。這樣可以減少系統的總負載，並可增加在本地網路中找到現有物件的機會。您也可以設定快取記憶體階層，使快取記憶體可以將物件要求轉遞至同層級或上層的快取記憶體——使其可從本地網路的另一個快取記憶體或直接從來源取得物件。

為快取記憶體階層選擇適當的拓樸是非常重要的，因為這樣它就不會增加網路的整體流量。就大型的網路而言，就非常合適為每個子網路設定代理伺服器，並將它們連線至上層的代理，這樣就可以連線至 ISP 的代理快取。

這些通訊都是由在 UDP 通訊協定最上層執行的 ICP (網際網路快取通訊協定) 所處理。在快取之間的資料傳輸是使用以 TCP 為基礎的 HTTP (超文字傳輸通訊協定，Hypertext Transmission Protocol) 來處理。

為了能找到最適合的伺服器來取得物件，某個快取記憶體會將 ICP 要求傳送到所有同層級的代理。如果有偵測到物件，這些代理就會透過具有 HIT 代碼的 ICP 回應來回覆這些要求；如果沒有偵測到物件，則會透過具有 MISS 代碼的 ICP 回應來回覆這些要求。如果找到多個 HIT 回應，代理伺服器會根據某些因素 (例如哪個快取記憶體傳送回覆的速度最快，哪個伺服器距離最近) 來決定要從哪部伺服器下載。如果沒有收到符合的回應，則會將要求傳送到上層快取。

提示

為了避免網路上不同的快取記憶體中出現物件重複，系統會使用其他 ICP 通訊協定。例如 CARP (快取陣列路由通訊協定) 或 HTCP (超文字快取通訊協定)。在網路中維護愈多的物件，則找到所需物件的機率也就愈大。

32.1.3 快取網際網路物件

網路中所有可用的物件並不全是靜態。其中有許多動態產生的 CGI 頁面、訪客計數器以及加密的 SSL 內容文件。諸如此類的物件是不會被快取的，因為每次存取它們時，它們都會改變。

還有一個問題就是，所有儲存在快取記憶體中的其他物件，應該在那里保留多長時間。為了決定停留時間，系統會指派各種可能的狀態給快取記憶體中的所有物件。網頁以及代理伺服器會藉由新增標頭至這些物件來找出物件的狀態，例如「上一次修改」或「到期」以及對應的日期。也會使用不應該快取指定該物件的其他標題。

由於缺少可用的硬碟空間，系統一般會使用 LRU (最近使用) 等演算法來取代快取記憶體中的物件。基本上這表示代理會清空那些最久沒有被要求的物件。

32.2 系統需求

最重要的事情是要決定系統必須承受的最大網路負載。因此需要特別注意負載峰值，峰值有可能超出日均值的四倍。當存在疑問時，最好高估系統的需求，因為如果讓 Squid 在接近其容量的限制下工作，有可能會造成服務品質的嚴重損失。接下來的小節將依重要順序指出系統因素。

32.2.1 硬碟

速度在快取處理過程中扮演很重要的角色，因此應該特別注意這個因素。對硬碟而言，此參數可稱為「隨機搜尋時間」，以毫秒為單位。因為 Squid 所讀取或寫入硬碟的資料區塊通常都相當的小，所以硬碟的搜尋時間比其資料輸送量還要重要。如果要使用代理，最好選擇具有高旋轉速的硬碟，因為這種硬碟可以較快的速度將讀寫頭放置在所需的位置。有一個方法可能可以增加系統的速度，就是同時使用多個磁碟或是運用分段 RAID 陣列。

32.2.2 磁碟快取的大小

在小的快取記憶體中，HIT (發現要求的物件已在該處) 的機率比較小，因為快取記憶體很容易就會填滿，且新的物件會取代不太被要求的物件。例如，如果

快取有 1 GB 可用，而且使用者一天只瀏覽 10 MB，則需要一百天以上才能將快取填滿。

決定所需快取記憶體大小的最簡易方法為，考量連線的最大傳輸速率。連線速率為 1 Mbit/s 時，其最大的傳輸速率為 125 125 KB/s。如果所有這些流量最後都保留在快取記憶體中，則 1 個小時內就會增至 450 MB，假設所有的流量都只在 8 個工作小時中產生，則一天就可達到 3.6 GB。由於連線一般都不會用到其容量上限，因此可以假設快取記憶體所處理的總資料容量大約為 2 GB。這就是為什麼範例中 Squid 需要 2 GB 的磁碟空間，以快取一天中已瀏覽的資料量。

32.2.3 RAM

Squid 所需的記憶體容量 (RAM) 與快取記憶體中的物件數目直接相關。Squid 也會將快取記憶體物件的參照以及常要求的物件儲存在主記憶體中以加速此資料的擷取速度。隨機存取記憶體比硬碟的速度快很多。

除此之外，Squid 需要在記憶體中保留其他的資料，例如所有已處理 IP 位址的表格、精確的網域名稱快取、最常要求的物件、存取控制清單、緩衝區等等。

為 Squid 處理程序保留足夠的記憶體是非常重要的，因為若使用磁碟進行交換，系統效能就會大幅地降低。cachemgr.cgi 工具可用於快取記憶體管理。此工具會在第 32.6 節「cachemgr.cgi」[470 頁] 中加以介紹。

32.2.4 CPU

Squid 不是一個需要密集使用 CPU 的程式。只有在載入或檢查快取記憶體的內容時，才會增加處理器的負載。使用多處理器的機器並不能提升系統的效能。若要提升效率，最好買更快的磁碟或新增更多的記憶體。

32.3 啟動 Squid

如果尚未安裝 squid 套件，請加以安裝。squid 不屬於 SUSE Linux Enterprise Server 預設安裝的部分。

Squid 在 SUSE® Linux Enterprise Server 中已經過預先設定，所以可在安裝後立即啟動。為了確保啟動更平順，應該將網路設定為至少使用一部名稱伺服器，而且可連接網際網路。如果撥號連線是使用動態 DNS 組態，就有可能產生問

題。在此範例中，至少應該輸入名稱伺服器，因為如果 Squid 在 `/etc/resolv.conf` 中偵測不到 DNS 伺服器，它就不會啟動。

32.3.1 開始和停止 Squid 的指令

若要啟動 Squid，請以 root 的身分在指令行中輸入 `rcsquid start`。第一次啟動時，必須先在 `/var/cache/squid` 中定義快取記憶體目錄結構。目錄的定義可由 `/etc/init.d/squid` 啟動程序檔自動完成，這可能需要花費數分鐘，甚至幾分鐘。如果 `done` 以綠色出現在右邊，則表示已成功載入 Squid。若要在本地系統上測試 Squid 的功能，請在瀏覽器中輸入 `localhost` 做為代理，並輸入 `3128` 做為埠。

若要允許本地系統和其他系統的使用者存取 Squid 和網際網路，請將 `/etc/squid/squid.conf` 組態檔中的 `http_access deny all` 項目變更為 `http_access allow all`。然而，當您這麼做時，請考量到此動作將使 Squid 可供任何人完全存取。因此，請定義控制代理存取權限的 ACL。如需關於此的詳細資訊，請參閱第 32.4.2 節「存取控制的選項」[465頁]。

在修改 `/etc/squid/squid.conf` 組態檔後，Squid 必須重新載入組態檔。請使用 `rcsquid reload` 完成此動作。或者也可以使用 `rcsquid restart` 徹底重新啟動 Squid。

`rcsquid status` 指令可用來檢查代理是否正在執行。`rcsquid stop` 指令可關閉 Squid。這可能需要花一段時間，因為 Squid 會在中斷與用戶端的連線並將其資料寫入磁碟前，先等待半分鐘（在 `/etc/squid/squid.conf` 中的 `shutdown_lifetime` 選項）。

警告：終止 Squid

使用 `kill` 或 `killall` 終止 Squid 可能會損毀快取記憶體。若要想重新啟動 Squid，必須刪除損毀的快取。

如果 Squid 在成功啟動後，仍然於一小段時間後即停止運作，請檢查是否有錯誤的名稱伺服器項目，或者是否缺少 `/etc/resolv.conf` 檔案。Squid 會在 `/var/log/squid/cache.log` 檔案中記錄啟動失敗的原因。如果要在系統開機時自動載入 Squid，請使用 YaST Runlevel 編輯器針對所需的 Runlevel 啟用 Squid。請參閱第 9.2.3 節「使用 YaST 設定 System Services (Runlevel)」[103頁]。

解除安裝 Squid 時不會移除快取記憶體階層或記錄檔。若要移除這些階層，請手動刪除 `/var/cache/squid` 目錄。

32.3.2 本地 DNS 伺服器

即使本地 DNS 伺服器不管理自己的網域，也可以設定本地 DNS 伺服器。它可以做為僅供快取的名稱伺服器，也可以透過根名稱伺服器來解析 DNS 要求，而不需任何特殊的組態 (請參閱第 24.4 節「啟動 BIND 名稱伺服器」[324頁])。如何達成此目的，取決於您在設定網際網路連線的組態時是否選擇了動態 DNS。

動態 DNS

一般而言，使用動態 DNS 時，會由提供者在建立網際網路連線期間設定 DNS 伺服器，且 `/etc/resolv.conf` 本地檔案會自動進行調整。此行為由 `/etc/sysconfig/network/config` 檔案透過 `NETCONFIG_DNS_POLICY` `sysconfig` 變數進行控制。使用 YaST `sysconfig` 編輯器將 `NETCONFIG_DNS_POLICY` 設定為 `"` (請參閱第 9.3.1 節「使用 YaST Sysconfig 編輯器變更系統組態」[106頁])。然後在 `/etc/resolv.conf` 檔案中輸入本地 DNS 伺服器，以 `127.0.0.1` 做為 `localhost` 的 IP 位址。這樣一來在啟動時，Squid 就可以永遠找到本地名稱伺服器。

為了能夠存取提供者的名稱伺服器，必須在 `forwarders` 下的 `/etc/named.conf` 組態檔中輸入提供者的名稱及其 IP 位址。若使用動態 DNS，只要將 `sysconfig` 變數 `NETCONFIG_DNS_POLICY` 設為 `auto`，就可以在建立連線時自動完成此動作。

靜態 DNS

若使用靜態 DNS，建立連線時將不會執行任何自動的 DNS 調整，所以不必變更任何 `sysconfig` 變數。但是您必須依照上述方式在 `/etc/resolv.conf` 檔案中輸入本地的 DNS 伺服器。除此之外，還必須在 `forwarders` 下的 `/etc/named.conf` 檔案中手動輸入提供者的靜態名稱伺服器及其 IP 位址。

提示：DNS 與防火牆

如果您有執行防火牆，請確定 DNS 要求可以通過防火牆。

32.4 /etc/squid/squid.conf 組態檔案

所有的 Squid 代理伺服器的設定值都是在 /etc/squid/squid.conf 檔案中設定。在第一次啟動 Squid 時，此檔案不需做任何變更，但是外部用戶端一開始為拒絕存取。代理可供 localhost 使用。預設的連接埠是 3128。預先安裝的 /etc/squid/squid.conf 組態檔案提供關於選項及許多範例的詳細資訊。幾乎所有的項目都是以 # (加備註的行) 開始，而且可以在行的結尾找到相關的規格。指定的值永遠都與預設值相關，因此在大部分情況下，如果移除備註符號而不變更任何參數，實際上沒有什麼效果。如果有可能，請保留原始的範例，並在行的下方插入選項以及修改過的參數。如此一來，就可以輕易復原預設值，並與變更做比較。

提示：在更新後調整組態檔案

如果您是從較早的 Squid 版本更新，建議您編輯新的 /etc/squid/squid.conf，並且只套用在舊檔案中所做的變更。如果嘗試使用舊的 squid.conf，可能會面臨組態不再起作用的問題，因為選項有時會發生修改並新增變更。

32.4.1 一般組態選項 (選擇)

`http_port 3128`

這是 Squid 傾聽用戶端要求所用的連接埠。預設的連接埠是 3128，但是 8080 也是常用的連接埠。如果有需要，請指定數個以空白分隔的埠號碼。

`cache_peer hostnametypeproxy-porticp-port`

在此可以輸入上層代理，例如如果您想要使用 ISP 的代理。針對主機名稱的部分，輸入要使用的代理的名稱或 IP 位址，針對類型的部分，輸入 parent。至於代理連接埠的部分，則輸入同樣由父代運算子指定的埠號，以便在瀏覽器中使用 (通常是 8080)。如果上層的 ICP 埠是未知的，而且其用途與提供者無關，請將 icp-port 設為 7 或 0。除此之外，還可在埠號碼後面指定 default 與 no-query，禁止使用 ICP 通訊協定。就提供者代理而言，Squid 接著就會像一般的瀏覽器一樣地運作。

`cache_mem 8 MB`

這個項目定義 Squid 可用於常見回覆的記憶體容量。預設值為 8 MB。這不指定 Squid 的記憶體使用量，而且可以超過。

`cache_dir ufs /var/cache/squid/ 100 16 256`

`cache_dir` 項目定義磁碟上儲存所有物件的目錄。在結尾處的數目代表可以使用的最大磁碟空間 (MB)，以及在第一層與第二層的目錄數目。`ufs` 參數不可變更。在預設情況下，`/var/cache/squid` 目錄佔用 100 MB 磁碟空間，而且可以在其中建立 16 個子目錄，每個目錄還各包含 256 個子目錄。當指定要使用的磁碟空間時，請保留足夠的預留磁碟空間。在此指定可用磁碟空間的 50% (最小) 至 80% (最大) 的值最為合理。最後兩個目錄值應該謹慎地增加，因為太多的目錄也有可能導致效能降低。如果您有數個共享快取的磁碟，請輸入數行 `cache_dir`。

`cache_access_log /var/log/squid/access.log` , `cache_log /var/log/squid/cache.log` ,
`cache_store_log /var/log/squid/store.log`

這三個項目指定 Squid 記錄其所有動作的路徑。一般而言，這裏不會有所變更。如果 Squid 負荷過重，則將快取與記錄檔分散到數個磁碟會是一個好辦法。

`emulate_httpd_log off`

如果該項目設為 *on*，就會取得可以讀取的記錄檔。然而有些試用程式無法解譯此檔案。

`client_netmask 255.255.255.255`

使用這個項目時，可以遮罩記錄檔中用戶端的 IP 位址。如果您在這裏輸入 `255.255.255.0`，IP 位址的最後一位數就會設為 0。您可以用這種方式保護用戶端的隱私。

`ftp_user Squid@`

使用這個項目可設定匿名 FTP 登入應該使用的 Squid 密碼。在此也可以指定有效的電子郵件地址，因為某些 FTP 伺服器會檢查這些地址的有效性。

`cache_mgr webmaster`

如果 Squid 意外損毀，Squid 應傳送訊息給此電子郵件地址。預設值為網站管理員。

`logfile_rotate 0`

如果您執行 `squid -k rotate`，則 Squid 會輪換安全的記錄檔。在此程序中會計算檔案的數目，而且在到達指定的值後，就會覆寫最舊的檔案。預

設值為 0，因為歸檔和刪除在 SUSE Linux Enterprise Server 中的記錄檔是由設定在 `/etc/logrotate/squid` 組態檔中的 `cron` 工作所執行。

`append_domain <domain>`

使用 `append_domain`，可在沒有給定網域時，指定要自動附加的網域。通常，可在此處輸入您自己的網域，因此在瀏覽器中輸入 `www` 就可以存取您自己的網頁伺服器。

`forwarded_for on`

如果您將項目設為 `off`，則 Squid 會從 HTTP 要求移除 IP 位址以及用戶端系統名稱。否則，它會在標頭中新增類似下一行

```
X-Forwarded-For: 192.168.0.1
```

`negative_ttl 5 minutes; negative_dns_ttl 5 minutes`

一般而言，您不需要變更這些值。不過，就算您有撥號連線，網際網路有時也可能無法使用。雖然已重新建立網際網路連線，Squid 仍然會記錄失敗的要求，並拒絕發出新的要求。在類似這種情況下，可以將 `minutes` 變更為 `seconds`，然後在瀏覽器中按一下「重新載入」，則幾秒鐘之後就會重新進行撥號程序。

`never_direct allow acl_name`

為了防止 Squid 直接從網際網路接受要求，請使用上述指令以強制連接另一個代理。此指令應該在之前已於 `cache_peer` 中輸入。如果 `all` 是指定為 `acl_name`，請強制將所有的要求直接轉遞至 `parent`。例如，如果您所使用的提供者，嚴格地規定其代理的使用方式或拒絕其防火牆直接存取網際網路，就可能需要執行此動作。

32.4.2 存取控制的選項

Squid 會提供一個詳細系統來控制代理存取。透過執行 ACL，可以輕鬆並完整地設定該系統。這牽涉到列出依序處理之規則的清單。在使用 ACL 前必須先進行定義。某些預設的 ACL，例如 `all` 與 `localhost` 已經存在。然而，僅定義 ACL 並不代表實際上會套用。這只會發生在連接 `http_access` 規則使用時。

`acl <acl_name> <type> <data>`

至少需要三種規格才能定義 ACL。可以任意選擇 `<acl_name>` 的名稱。至於 `<type>` 的部分，可從各種不同的選項中選取(選項位於 `/etc/squid/squid.conf` 檔案中的 `ACCESS CONTROLS` 小節)。`<data>` 的規格取決於個別的

ACL 類型，而且也可以從檔案讀取，例如，透過主機名稱、IP 位址或 URL。下列是一些簡單的範例：

```
acl mysurfers srcdomain .my-domain.com
acl teachers src 192.168.1.0/255.255.255.0
acl students src 192.168.7.0-192.168.9.0/255.255.255.0
acl lunch time MTWTF 12:00-15:00
```

`http_access allow <acl_name>`

http_access 定義哪些人可使用代理，以及哪些人可存取網際網路的哪些內容。因此，必須指定 ACL。已在上文定義的 *localhost* 與 *all*，可透過 *deny* 或 *allow* 拒絕或允許存取。您可以建立包含任何數目之 *http_access* 項目的清單，系統會從上至下處理這些項目，並按照前面優先的原則允許或拒絕存取個別 URL。最後一個項目應該永遠為 *http_access deny all*。在下列範例中，*localhost* 對於每個項目都擁有完整的存取權，而所有其他的主機則完全無法存取。

```
http_access allow localhost
http_access deny all
```

在另一個使用這些規則的範例中，*teachers* 群組永遠具有網際網路的存取權。*students* 群組只能取得在星期一到星期五午休時間的存取權。

```
http_access deny localhost
http_access allow teachers
http_access allow students lunch time
http_access deny all
```

基於可讀性的理由，*http_access* 項目清單，只能在 `/etc/squid/squid.conf` 檔案中的指定位置中輸入。也就是，在文字之間

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

以及最後

```
http_access deny all
```

`redirect_program /usr/bin/squidGuard`

使用此選項，可以指定 *squidGuard* 等重新導向器，用於封鎖不需要的 URL。使用代理驗證以及適當的 ACL，就可以為不同的使用者群組個別地控制網際網路的存取。*squidGuard* 是可以安裝和設定的獨立套件。

`auth_param basic program /usr/sbin/pam_auth`

如果在代理上必須對使用者進行驗證，請設定對應的程式，例如 `pam_auth`。第一次存取 `pam_auth` 時，使用者會看到一個登入視窗，請在此輸入使用者名稱與密碼。除此之外，仍然需要 ACL，因此只有擁有有效登入的用戶端可以使用網際網路：

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

在 `proxy_auth` 之後的 *REQUIRED* 可以使用允許的使用者名稱清單或是到達這類清單的路徑來取代。

`ident_lookup_access allow <acl_name>`

使用這個項目，就會為所有 ACL 定義的用戶端執行 `ident` 要求以尋找每個使用者的身分。如果您將 *all* 套用至 `<acl_name>`，會對所有用戶端生效。另外，`ident` 精靈必須在所有的用戶端上執行。在 Linux 上，請為此用途安裝 `pidntd` 套件。在 Microsoft Windows 上，可以從網際網路下載可用的免費軟體。若要確保只允許 `ident` 查詢為成功的用戶端，請在此定義對應的 ACL：

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

同樣地，請使用允許的使用者名稱清單來取代 *REQUIRED*。使用 `ident` 會大幅增加存取時間，因為每個要求都會重複 `ident` 查詢。

32.5 設定操作順暢的代理

使用代理伺服器的一般方法如下：網頁瀏覽器將要求傳送至代理伺服器的某個連接埠，然後代理伺服器會提供這些所需物件（無論它們是否在快取記憶體中）。使用網路工作時，可能會發生數種狀況：

- 基於安全理由，建議所有的用戶端都使用代理瀏覽網際網路。
- 所有的用戶端都必須使用代理，不論它們是否注意到它。
- 網路上的代理發生變動，但現有的用戶端需要保留其原有的組態。

在所有上述情況下，都可使用透明代理。原則很簡單：代理會攔截和回應網頁瀏覽器的要求，因此網頁瀏覽器不必知道頁面的來源，即可收到要求的頁面。如名稱所示，整個程序會流暢地執行。

32.5.1 在 `/etc/squid/squid.conf` 中的組態選項

若要通知 squid 它將會做為透明代理，請在主要組態檔案 `/etc/squid/squid.conf` 中的 `http_port` 標記處使用 `transparent` 選項。重新啟動 squid 後，唯一要執行的任務就是重新設定防火牆，以將 `http` 連接埠重新指向至 `http_port` 中指定的連接埠。在下面的 squid 組態行中，該指定的埠為埠 3128。

```
http_port 3128 transparent
```

32.5.2 使用 SuSEfirewall2 的防火牆組態

現在，請使用連接埠轉遞規則，透過防火牆將所有的內送要求重新導向至 Squid 埠。若要這麼做，請依照第 15.4.1 節「Configuring the Firewall with YaST」(第 15 章「*Masquerading and Firewalls*」, ↑*Security Guide*) 中所述使用隨附工具 SuSEfirewall2。其組態檔位於 `/etc/sysconfig/SuSEfirewall2`。組態檔由詳細記錄的項目所組成。若要設定操作順暢的代理，您必須設定數個防火牆選項：

- 指向網際網路的設備：`FW_DEV_EXT="eth1"`
- 指向網路的設備：`FW_DEV_INT="eth0"`

在防火牆上，定義供不受信任的 (外部) 網路 (如網際網路) 存取的連接埠與服務 (請參閱 `/etc/services`)。在此範例中，僅提供對外的 Web 服務：

```
FW_SERVICES_EXT_TCP="www"
```

在從安全 (內部) 網路存取的防火牆上，定義埠或服務 (請參閱 `/etc/services`)，兩者都是透過 TCP 與 UDP 服務：

```
FW_SERVICES_INT_TCP="domain www 3128"  
FW_SERVICES_INT_UDP="domain"
```

這裡允許存取 Web 服務與 Squid (其預設埠為 3128)。「domain」服務代表 DNS (網域名稱服務)。這個服務使用非常普遍。否則，請直接將它從上述項目移除，並將下列選項設為 no：

```
FW_SERVICE_DNS="yes"
```

最重要的選項是選項數字 15：

範例 32.1 防火牆組態：選項 15

```
# 15.)
# Which accesses to services should be redirected to a local port on
# the firewall machine?
#
# This option can be used to force all internal users to surf via
# your squid proxy, or transparently redirect incoming webtraffic to
# a secure webserver.
#
# Format:
# list of <source network>[,<destination network>,<protocol>[,dport[:lport]]
# Where protocol is either tcp or udp. dport is the original
# destination port and lport the port on the local machine to
# redirect the traffic to
#
# An exclamation mark in front of source or destination network
# means everything EXCEPT the specified network
#
# Example: "10.0.0.0/8,0/0,tcp,80,3128 0/0,172.20.1.1,tcp,80,8080"
```

上方的註解顯示要遵照的語法。首先，輸入存取代理防火牆之內部網路的 IP 位址與網路遮罩。其次，輸入這些用戶端的要求傳送到的 IP 位址與網路遮罩。如果是網頁瀏覽器，請將網路指定為 0/0，萬用字元表示「可到任何位置」。完成後，輸入這些要求傳送到的原始目的埠，最後，輸入重新導向所有這些要求的目的埠。由於 Squid 支援 HTTP 以外的通訊協定，請將要求從其他連接埠重新導向到代理，例如 FTP (埠 21)、HTTPS、或 SSL (埠 443)。在此範例中，Web 服務 (埠 80) 會重新導向至代理埠 (埠 3128)。如果需要新增更多的網路或服務，必須在各個項目中以空格隔開。

```
FW_REDIRECT="192.168.0.0/16,0/0,tcp,80,3128"
```

若要啟動防火牆並使用它所包含的新組態，請在 /etc/sysconfig/SuSEfirewall12 檔案中變更項目。START_FW 項目必須設為 "yes"。

啟動 Squid，如第 32.3 節「啟動 Squid」[460 頁] 所示。若要確認一切正常，請查看 /var/log/squid/access.log 中的 Squid 記錄。Squid 若要確認是否已正

確設定所有的埠，請從網路之外的任何電腦執行機器上的埠掃描。只應開啟 Web 服務 (埠 80)。若要以 `nmap` 掃描連接埠，指令語法為 `nmap -O IP_address`。

32.6 cachemgr.cgi

快取管理員 (`cachemgr.cgi`) 是一種 CGI 公用程式，用來顯示正在執行之 Squid 處理程序的記憶體使用率統計資料。它也是管理快取和檢視統計資料較方便的方式，因為不需要登入伺服器。

32.6.1 設定

首先，需要在系統上執行網頁伺服器。依第 30 章「*Apache HTTP 伺服器*」[411頁] 中所述方式設定 Apache。若要檢查 Apache 是否已在執行，請以 `root` 的身分輸入 `rcapache status` 指令。如果出現像這類的訊息：

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

表示 Apache 正在機器上執行。否則，請輸入 `rcapache start`，以使用 SUSE Linux Enterprise Server 預設值啟動 Apache。設定 Apache 的最後一個步驟是將 `cachemgr.cgi` 檔案複製到 Apache 的 `cgi-bin` 目錄。對於 32 位元，方式如下：

```
cp /usr/lib/squid/cachemgr.cgi /srv/www/cgi-bin/
```

在 64 位元環境中，檔案 `cachemgr.cgi` 位於 `/usr/lib64/squid/` 之下，若要將其複製到 Apache 目錄，請使用如下指令：

```
cp /usr/lib64/squid/cachemgr.cgi /srv/www/cgi-bin/
```

32.6.2 在 `/etc/squid/squid.conf` 中的快取管理員 ACL

快取管理員需要原始檔案中某些預設的設定值。首先，定義兩個 ACL，然後 `http_access` 選項會使用這些 ACL 來授予 CGI 程序檔對 Squid 的存取權限。第一個 ACL 最重要，因為快取管理員會嘗試透過 `cache_object` 通訊協定與 Squid 通訊。


```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

下列規則會將 Squid 的存取權限授與 Apache：

```
http_access allow manager localhost
http_access deny manager
```

這些規則是假設網頁伺服器與 Squid 在相同的機器上執行。如果快取管理員與 Squid 之間的通訊是源自於另一部電腦上的網頁伺服器，請依 範例 32.2「存取規則」[471頁] 所述包含一個額外的 ACL。

範例 32.2 存取規則

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # webserver IP
```

然後新增 範例 32.3「存取規則」[471頁] 中的規則，以允許從網頁伺服器存取。

範例 32.3 存取規則

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

設定管理員的密碼以存取更多的選項，如遠端關閉快取記憶體或是檢視快取記憶體的詳細資訊。為此，請以管理員的密碼以及要檢視的選項清單設定 `cachemgr_passwd` 項目。這個清單會顯示成 `/etc/squid/squid.conf` 中項目備註的一部份。

每次變更組態檔時，請重新啟動 Squid。使用 `rcsquid reload` 即可輕鬆執行重啟。

32.6.3 檢視統計資料

瀏覽對應的網站——<http://webserver.example.org/cgi-bin/cachemgr.cgi>。按「繼續」，然後瀏覽不同的統計資料。

32.7 squidGuard

本節目的不是說明 squidGuard 的廣泛組態，而是簡單介紹並給予使用上的一些建議。如需更深入的組態問題，請參閱 squidGuard 網站，網址為 <http://www.squidguard.org>。

squidGuard 屬於自由軟體 (GPL)，是一個靈活而快速的過濾器，也是重新導向器以及 Squid 的存取控制器外掛程式。它可讓您在 Squid 快取上，針對不同的使用者群組，使用不同的限制來定義多重存取規則。squidGuard 使用 Squid 的標準重新導向器介面。squidGuard 可以執行下列動作：

- 將某些使用者的 Web 存取權限制為一系列已接受或已知的 Web 伺服器或 URL。
- 針對某些使用者，封鎖某些列示或列為黑名單的網頁伺服器或 URL 的存取權。
- 針對某些使用者，封鎖符合一般運算式或文字清單的 URL。
- 將封鎖的 URL，重新導向至「智慧型」的 CGI 資訊頁面。
- 將未註冊的使用者重新導向至註冊表單。
- 將橫幅重新導向至空白的 GIF。
- 根據時間、星期、日期等，使用不同的存取規則。
- 針對不同的使用者群組，使用不同的規則。

squidGuard 與 Squid 無法用於：

- 編輯、過濾或審查文件內的文字。
- 編輯、過濾或審查 HTML 內嵌的程序檔語言，例如 JavaScript 或 VBscript。

使用前，請先安裝 squidGuard。以 `/etc/squidguard.conf` 提供最小的組態檔。組態範例請見 <http://www.squidguard.org/Doc/examples.html>。稍後請使用較複雜的組態設定值來測試。

接著，如果用戶端要求已列為黑名單的網站，請建立虛擬的「拒絕存取」頁面，或建立一個有點複雜的 CGI 頁面以重新導向 Squid。強烈建議使用 Apache。

現在，請將 Squid 設定為使用 squidGuard。在 `/etc/squid/squid.conf` 檔案中使用下列項目：

```
redirect_program /usr/bin/squidGuard
```

另一個稱為 `redirect_children` 的選項會設定在機器上執行之「重新導向」(在此範例中為 squidGuard) 程序的數量。您設定的程序越多，所需的 RAM 就越多。請先嘗試較小的數字 (例如 4)。

```
redirect_children 4
```

最後，執行 `rcsquid reload`，讓 Squid 載入新的組態。現在，請使用瀏覽器測試您的設定值。

32.8 使用 Calamaris 產生快取報告

Calamaris 是一種 Perl 程序檔，用來產生 ASCII 或 HTML 格式的快取記憶體活動報告。它使用原生的 Squid 存取記錄檔。Calamaris 的首頁網址為 <http://Calamaris.Cord.de/>。此工具不屬於 SUSE Linux Enterprise Server 預設安裝的部分，若想使用，可以安裝 `calamaris` 套件。

以 root 身分登入，然後輸入 `cat access.log | calamaris 選項 > reportfile`。當要傳輸一個以上的記錄檔時，須依時間順序來排列記錄檔，較舊的檔案排在前面。以下是程式的某些選項：

提示：外圍程序與檔案順序

如果您有多個類似的檔案，如 `access.log.1`、`access.log.2`，依此類推，則在列出 `access.log.*` 時，預設外圍程序 `bash` 會以非數字順序對這些檔案排序。若要解決此問題，可以使用語法 `access.log.{1..42}`，產生副檔名為從數字 1 到 42 的檔案清單。

-a

輸出所有可用的報告

-w

以 HTML 報告輸出

-l

在報告標題中包含訊息或標誌

在程式的手冊頁中，使用 `man calamaris` 可以找到各種選項的詳細資訊。

以下是典型的範例：

```
cat access.log.{10..1} access.log | calamaris -a -w \  
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

這會將報告放在網頁伺服器的目錄中。需要有 Apache 才能檢視報告。

32.9 如需更多資訊

請瀏覽 Squid 的首頁，網址為 <http://www.squid-cache.org/>。此處可以找到「Squid 使用者指南」(Squid User Guide) 以及有關 Squid 常見問題集 (FAQ) 的豐富資訊。

安裝後，可以在 `howtoenh` 中找到有關透明代理之簡要操作資訊，檔案名稱為 `/usr/share/doc/howto/en/txt/TransparentProxy.gz`。除此之外，還可以在 squid-users@squid-cache.org 中找到 Squid 的郵件清單。這個的歸檔是位於 <http://www.squid-cache.org/mail-archive/squid-users/>。

透過 SFCB 實作的網路企業管理

33.1 簡介與基本概念

SUSE® Linux Enterprise Server (SLES) 提供一系列基於開放式標準的工具，用於統一管理不同的計算系統和環境。我們的企業解決方案執行 Distributed Management Task Force 所建議的標準。以下段落將介紹其基本元件。

Distributed Management Task Force, Inc (DMTF) 是業內一個引領企業和網際網路環境管理標準開發的組織。該組織的目標是統一管理標準與計劃，並制定整合性更強、更為經濟有效且更具互通性的管理解決方案。DMTF 標準為實施控制和通訊提供了通用的系統管理元件。它們的解決方案與平台和技術無關。*網路企業管理*和 *Common Information Model* 是其重要技術之一。

網路企業管理 (WBEM) 是一套管理和網際網路標準技術。WBEM 的開發目的是為了統一管理企業計算環境。它能夠讓整個行業使用 Web 技術提供一系列整合性極強的管理工具。WBEM 包含以下標準：

- 資料模型：標準的通用資訊模型 (CIM)
- 編碼規格：CIM-XML 編碼規格
- 輸送機制：透過 HTTP 的 CIM 操作

Common Information Model 是一個概念性的資訊模型，對系統管理進行了描述。該模型並非限於某種實作，而且可以實現管理系統、網路、服務與應用程式之間管理資訊的交換。CIM 由兩個部分組成：CIM 規格與 CIM 綱要。

- *CIM* 規格描述語言、命名和中繼綱要。中繼綱要是正式的模型定義。它定義了用來表達此模型的詞彙，以及這些詞彙的使用和語意。中繼綱要包含類別 (class)、內容 (property) 和方法 (method) 這幾個元素。它還允許將指示與關聯做為類別的類型，將參考做為內容的類型。
- *CIM* 綱要提供實際的模型描述。它提供一組類別，這些類別包含的屬性和關聯可提供完整解讀的概念框架，使用者可運用此框架來組織關於受管理環境的可用資訊。

共用資訊模型物件管理員 (Common Information Model Object Manager, CIMOM) 就是 CIM 物件管理員，更詳細說來，就是指根據 CIM 標準管理物件的應用程式。CIMOM 會管理 CIMOM 提供者與 CIM 用戶端之間的通訊，而管理員則會管理系統。

CIMOM 提供者是指透過 CIMOM 來執行用戶端應用程式所要求之特定工作的軟體。每個提供者都會執行 CIMOM 綱要的一項或多項範疇工作。這些提供者會直接與硬體互動。

Standards Based Linux Instrumentation for Manageability (SBLIM) 是為實現網路企業管理 (WBEM) 而設計的一系列工具。SUSE® Linux Enterprise Server 使用 SBLIM 專案 *Small Footprint CIM Broker* 的開放原始碼 CIMOM (或 CIM 伺服器)。

Small Footprint CIM Broker 是一款適用於資源受限或內嵌式環境的 CIM 伺服器，可同時實現模組化與輕量化。它基於開放式標準，並支援 CMPI 提供者、CIM-XML 編碼和受管理物件格式 (MOF)。這款伺服器不僅設定自由度高，而且在提供者當機時仍能穩定運作。此外，它還支援各種傳輸通訊協定 (例如 HTTP、HTTPS、Unix Domain Socket、服務位置通訊協定 (SLP) 和 Java 資料庫連接 (JDBC))，因此存取方便。

33.2 設定 SFCB

若要設定 Small Footprint CIM Broker (SFCB) 環境，請務必在 SUSE Linux Enterprise Server 安裝期間選取 YaST 中的「網路企業管理」模式。或者，也可以選擇將其做為一個元件，安裝於目前正在執行的伺服器上。請確定系統上已安裝下列套件：

cim-schema, Common Information Model (CIM) 綱要

包含 Common Information Model (CIM)。CIM 是描述網路或企業環境內所有管理資訊的模型。CIM 由規格和綱要所組成。其中的規格定義了與其他管理模型整合的詳細資訊。而綱要則會提供實際的模型描述。

cmpi-bindings-pywbem

包含可在 Python 中寫入並執行 CMPI 類型 CIM 提供者的介面卡。

cmpi-pywbem-base

包含基礎系統 CIM 提供者。

cmpi-pywbem-power-management

包含基於 DSP1027 的電源管理提供者。

python-pywbem

包含 Python 模組，用於透過 WBEM 通訊協定進行 CIM 操作呼叫，以查詢及更新受管理物件。

cmpi-provider-register, 與 CIMOM 無關的提供者註冊公用程式

包含一個公用程式，無論 CIMOM 在系統中執行何種操作，都可讓 CMPI 提供者套件進行註冊。

sblim-sfcb, Small Footprint CIM Broker

包含 Small Footprint CIM Broker。這是一個 CIM 伺服器，執行透過 HTTP 通訊協定的 CIM 操作。這款伺服器功能全，資源佔用率低，因此特別適合內嵌式環境以及資源受限的環境。SFCB 允許透過通用管理程式介面 (CMPI) 寫入提供者。

sblim-sfcc

包含 Small Footprint CIM Client Library 執行時期程式庫。

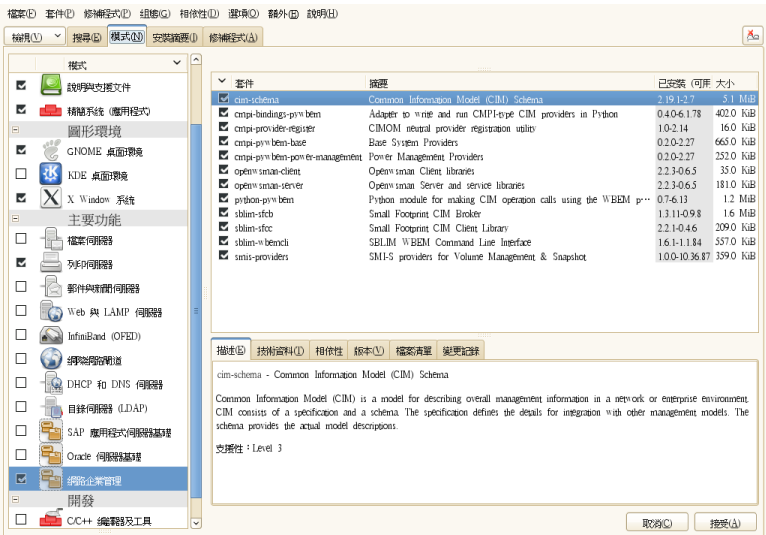
sblim-wbemcli

包含 WBEM 指令行介面。它是一個獨立的指令行 WBEM 用戶端，特別適合基礎系統管理任務。

smis-providers

包含多個提供者，適用於 Linux 檔案系統上的磁碟區和快照。它們均基於 SNIA 的 SMI 磁碟區管理設定檔與複製服務設定檔。

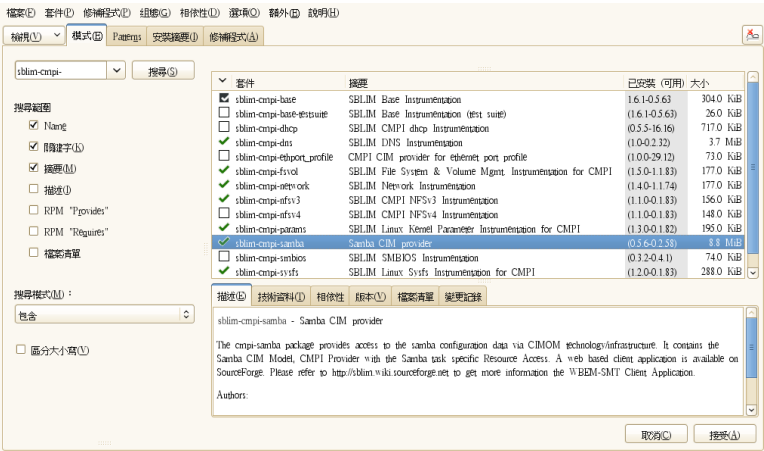
圖形 33.1 網路企業管理模式的套件選擇



33.2.1 安裝其他提供者

SUSE® Linux Enterprise Server 軟體儲存庫包含無法在網路企業管理安裝模式下找到的其他 CIM 提供者。您可以透過在 YaST 軟體安裝模組中搜尋模式 `sblim-cmpi-`，輕鬆獲得這些提供者的清單與安裝狀態。這些提供者能夠完成各種系統管理任務，例如 `dhcp`、`NFS` 或核心參數設定。安裝要與 `SFCB` 搭配使用的提供者很有必要。

圖形 33.2 其他 CIM 提供者的套件選擇



33.2.2 開始、停止和檢查 SFCB 的狀態

CIM 伺服器 sfcbd 精靈隨網路企業管理軟體一起安裝，並且預設會在系統啟動時啟動。下表將說明如何啟動、停止和檢查 sfcbd 的狀態。

表格 33.1 管理 sfcbd 的指令

任務	Linux指令
啟動 sfcbd	以 root 身分在指令行中輸入 rcsfcb start。
停止 sfcbd	以 root 身分在指令行中輸入 rcsfcb start。
檢查 sfcbd 狀態	以 root 身分在指令行中輸入 rcsfcb status。

33.2.3 確保安全的存取

SFCB 的預設設定相當安全。不過，仍須檢查 SFCB 元件存取的安全級別是否符合您組織的要求。

33.2.3.1 憑證

安全通訊端層 (SSL) 傳輸必須使用證書，才能執行安全的通訊服務。安裝 SFCB 時，會產生自行簽署的證書。

您可以變更 `/etc/sfcb/sfcb.cfg` 中的 `sslCertificateFilePath`：路徑_檔名設定，以商業證書或自行簽署證書的路徑取代預設證書的路徑。該檔案必須為 PEM 格式。

預設產生的伺服器證書會存放在以下位置：

```
/etc/sfcb/server.pem
```

注意：SSL 證書的路徑

預設產生的證書檔案 `servercert.pem` 與 `serverkey.pem` 會儲存於 `/etc/ssl/servercerts` 目錄。檔案 `/etc/sfcb/client.pem`、`/etc/sfcb/file.pem` 和 `/etc/sfcb/server.pem` 為上述檔案的符號連結。

若要產生新證書，請以 `root` 身分在指令行中輸入以下指令：

```
tux@mercury:~> sh /usr/share/sfcb/genSslCert.sh
Generating SSL certificates in .
Generating a 2048 bit RSA private key
.....+++
.+++
writing new private key to '/var/tmp/sfcb.0Bjt69/key.pem'
-----
```

預設情況下，程序檔會在目前的工作目錄下產生證書 `client.pem`、`file.pem` 和 `server.pem`。若要讓程序檔在 `/etc/sfcb` 目錄中產生證書，則需要在指令中附加該路徑。如果這些檔案已存在，系統只會顯示警告訊息，不會覆寫舊證書。

```
tux@mercury:~> sh /usr/share/sfcb/genSslCert.sh /etc/sfcb
Generating SSL certificates in .
WARNING: server.pem SSL Certificate file already exists.
```

```
old file will be kept intact.  
WARNING: client.pem SSL Certificate trust store already exists.  
old file will be kept intact.
```

必須從檔案系統中移除舊證書，然後再次執行指令。

若要變更 SFCB 使用證書的方式，請參閱第 33.2.3.3 節「驗證」[481頁]。

33.2.3.2 埠

預設情況下，SFCB 設定為接受所有透過安全連接埠 5989 傳輸的通訊。以下段落將介紹通訊連接埠設定以及建議的組態。

連接埠 5989 (安全)

SFCB 通訊使用的安全連接埠，提供 HTTPS 服務。這是預設值。如果使用這項設定，當透過網際網路在伺服器和工作站之間傳送時，所有 CIMOM 和用戶端應用程式之間的通訊都會進行加密。使用者必須使用用戶端應用程式進行驗證才能連接 SFCB 伺服器。建議您保留此設定。如果用戶端應用程式和受監控的節點之間存在路由器和防火牆，則必須在這些路由器和防火牆上開啟此連接埠，以便 SFCB CIMOM 可以與必要的應用程式進行通訊。

連接埠 5988 (不安全)

SFCB 通訊使用的非安全連接埠，提供 HTTP 服務。這項設定已預設為停用。使用這項設定時，所有 CIMOM 和用戶端應用程式之間的通訊，在透過網際網路在伺服器和工作站之間傳送時都會開放，任何人無須經過任何驗證即可檢視。建議您只在嘗試為 CIMOM 相關問題除錯時使用這項設定。一旦問題解決，請再次停用不安全連接埠選項。如果 SFCB CIMOM 要與需要進行不安全存取的必要應用程式進行通訊，則必須在用戶端應用程式與受監控節點之間的路由器和防火牆上開啟此連接埠。

如果您要變更預設的埠指定，請參閱第 33.2.3.2 節「埠」[481頁]。

33.2.3.3 驗證

SFCB 支援 HTTP 基本驗證和基於用戶端證書的驗證 (HTTP over SSL 連線)。在 SFCB 組態檔案 (預設為 `/etc/sfcb/sfcb.cfg`) 中指定 `doBasicAuth=true`，可啟用基本 HTTP 驗證。SFCB 的 SUSE® Linux Enterprise Server 安裝支援可插入驗證模組 (PAM) 方法，因此本地 root 使用者可以使用本地 root 使用者身分證明向 SFCB CIMOM 進行驗證。

如果 `sslClientCertificate` 組態內容設為 *accept* 或 *require*，則 SFCB HTTP 介面卡會在用戶端透過 HTTP over SSL (HTTPS) 連接時要求其提供證書。如果指定 *require*，則用戶端必須提供有效的證書 (依據透過 `sslClientTrustStore` 指定的用戶端信任儲存區)。如果用戶端無法提供有效證書，CIM 伺服器會拒絕連線。

`sslClientCertificate=accept` 設定產生的作用可能並不明顯。不過，當要同時允許基本驗證與用戶端證書驗證時，此設定非常有用。如果用戶端能夠提供有效的證書，HTTPS 連線便會建立，並且不再執行基本驗證程序。如果此功能無法驗證該證書，則會執行 HTTP 基本驗證。

33.3 SFCB CIMOM 組態

SFCB 是 CIM 伺服器的輕量化實作，但設定的自由度很高。有多個選項可控制其行為。控制 SFCB 伺服器的方法主要有三種：

- 設定相應的環境變數
- 使用指令行選項
- 變更其組態檔案

33.3.1 環境變數

有多個環境變數會直接影響 SFCB 的行為。您需要透過 `rcsfcb restart` 重新啟動 SFCB 精靈，才能讓上述變更生效。

`PATH`

指定 `sfcdb` 精靈及公用程式的路徑。

`LD_LIBRARY_PATH`

指定 `sfcdb` 執行時期程式庫的路徑。或者，您也可以將此路徑新增至系統層級的動態載入程式組態檔案 `/etc/ld.so.conf`。

`SFCB_PAUSE_PROVIDER`

指定提供者名稱。SFCB 伺服器會在首次載入提供者後暫停。此時，您可以將執行時期除錯程式附加至提供者的程序，以進行除錯。

SFCB_PAUSE_CODEC

指定 SFCB 轉碼器的名稱 (目前僅支援 http)。SFCB 伺服器會在首次載入轉碼器後暫停。此時，您可以將執行時期除錯程式附加至程序。

SFCB_TRACE

為 SFCB 指定除錯訊息的等級。有效值為 0 (無除錯訊息)，或 1 (重要除錯訊息) 至 4 (所有除錯訊息)。預設值為 1。

SFCB_TRACE_FILE

SFCB 預設會將其除錯訊息輸出至標準錯誤輸出 (STDERR)。若要將除錯訊息改寫到指定的檔案，可以設定此變數。

SBLIM_TRACE

為 SBLIM 提供者指定除錯訊息的等級。有效值為 0 (無除錯訊息)，或 1 (重要除錯訊息) 至 4 (所有除錯訊息)。

SBLIM_TRACE_FILE

SBLIM 提供者預設會將其追蹤訊息輸出至 STDERR。若要將追蹤訊息改寫到指定的檔案，可以設定此變數。

33.3.2 指令行選項

SFCB 精靈 `sfcbd` 有多個指令行選項，可開啟或關閉特定的執行時期功能。請在 SFCB 精靈啟動時輸入這些選項。

`-c`、`--config-file=檔案`

SFCB 精靈啟動時，預設會從 `/etc/sfcb/sfcb.cfg` 中讀取組態。借助此選項，可以指定替代的組態檔案。

`-d`、`--daemon`

強制 `sfcbd` 及其子程序在背景執行。

`-s`、`--collect-stats`

開啟執行時期的統計資料收集。各種 `sfcbd` 執行時期統計資料將被寫入到目前工作目錄下的 `sfcbStat` 檔案。預設情況下，不會收集任何統計資料。

`-l`、`--syslog-level=記錄層級`

指定 `syslog` 的詳細層級。記錄層級可以是 `LOG_INFO`、`LOG_DEBUG` 或 `LOG_ERR`，預設為 `LOG_ERR`。

-k、--color-trace=記錄層級

使用不同的色彩列印各程序的追蹤輸出，以方便您除錯。

-t、--trace-components=數字

啟動元件層級的訊息追蹤，其中數字為使用OR指定的位元遮罩整數，用於定義要追蹤的元件。如果指定 -t ?，會列出所有元件及其關聯的整數位元遮罩：

```
tux@mercury:~> sfcdbd -t ?
---   Traceable Components:      Int      Hex
---   providerMgr:                1 0x0000001
---   providerDrv:                2 0x0000002
---   cimxmlProc:                 4 0x0000004
---   httpDaemon:                 8 0x0000008
---   upCalls:                    16 0x0000010
---   encCalls:                   32 0x0000020
---   ProviderInstMgr:            64 0x0000040
---   providerAssocMgr:          128 0x0000080
---   providers:                  256 0x0000100
---   indProvider:                512 0x0000200
---   internalProvider:          1024 0x0000400
---   objectImpl:                 2048 0x0000800
---   xmlIn:                       4096 0x0001000
---   xmlOut:                      8192 0x0002000
---   sockets:                    16384 0x0004000
---   memoryMgr:                   32768 0x0008000
---   msgQueue:                    65536 0x0010000
---   xmlParsing:                  131072 0x0020000
---   responseTiming:             262144 0x0040000
---   dbpdaemon:                   524288 0x0080000
---   slp:                         1048576 0x0100000
```

-t 2019 會顯示 sfcdbd 的內部函數，但不會產生過多訊息，因此很有用。

33.3.3 SFCB 組態檔案

SFCB 會在啟動後從組態檔案 /etc/sfcb/sfcb.cfg 讀取其執行時期組態。若想覆寫啟動時的這一行為，可以使用 -c 選項。

組態檔案包含多組 option: 值，每行一組。變更此檔案時，可以使用以所用環境原生格式儲存檔案的任何文字編輯器。

如果設定中包含以數字符號 (#) 設為備註的選項，則該設定會使用預設設定。

下面的選項清單可能不完整。如需完整的清單，請參閱 `/etc/sfcb/sfcb.cfg` 和 `/usr/share/doc/packages/sblim-sfcb/README` 中的相關內容。

33.3.3.1 httpPort

目的、用途

指定 `sfcbd` 監聽來自 CIM 用戶端之 HTTP (不安全) 請求的本地連接埠值。預設值為 5988。

語法

`httpPort`: 埠號

33.3.3.2 enableHttp

目的、用途

指定 SFCB 是否應接受 HTTP 用戶端連線。預設值為 `false`。

語法

`enableHttp`: 選項

選項	描述
<code>true</code>	啟用 HTTP 連線。
<code>false</code>	停用 HTTP 連線。

33.3.3.3 httpProcs

目的、用途

指定可同時建立之 HTTP 用戶端連線的最大數目。達到該數目後，所有新的內送 HTTP 請求都將遭到阻擋。預設值為 8。

語法

`httpProcs`: 最大連線數

33.3.3.4 httpUserSFCB、httpUser

目的、用途

這些選項可控制 http 伺服器將以何使用者的身分執行。如果 `httpUserSFCB` 為 `true`，http 將以 SFCB 主程序所用的相同使用者身分執行。如果為 `false`，將使用為 `httpUser` 指定的使用者名稱。此設定用於 http 和 https 兩種伺服器。若 `httpUserSFCB` 設定為 `false`，就必須指定 `httpUser`。預設值為 `true`。

語法

`httpUserSFCB`: *true*

33.3.3.5 httpLocalOnly

目的、用途

指定是否將 HTTP 要求局限於本地主機。預設值為 `false`。

語法

`httpLocalOnly`: *false*

33.3.3.6 httpsPort

目的、用途

指定 `sfcdb` 監聽來自 CIM 用戶端之 HTTPS 請求的本地連接埠值。預設值為 5989。

語法

`httpsPort`: 埠號

33.3.3.7 enableHttps

目的、用途

指定 SFCB 是否接受 HTTPS 用戶端連線。預設值為 `true`。

語法

`enableHttps`: 選項

選項	描述
<code>true</code>	啟用 HTTPS 連線。
<code>false</code>	停用 HTTPS 連線。

33.3.3.8 httpsProcs

目的、用途

指定可同時建立之 HTTPS 用戶端連線的最大數目。達到該數目後，所有新的內送 HTTPS 請求都將遭到阻擋。預設值為 8。

語法

`httpsProcs`: 最大連線數

33.3.3.9 enableInterOp

目的、用途

指定 SFCB 是否提供 *interop* 名稱空間，用於指示支援。預設值為 `true`。

語法

`enableInterOp`: 選項

選項	描述
true	啟用 interop 名稱空間。
false	停用 interop 名稱空間。

33.3.3.10 provProcs

目的、用途

指定可同時執行之提供者程序的最大數目。達到該數目之後，如果有新的內送請求要求載入新提供者，則會先自動卸載某個現有的提供者。預設值為 32。

語法

provProcs: 最大程序數

33.3.3.11 doBasicAuth

目的、用途

接受請求之前，依據用戶端使用者識別碼開啟或關閉基本驗證。預設值為 true，表示系統會執行基本用戶端驗證。

語法

doBasicAuth: 選項

選項	描述
true	啟用基本驗證。
false	停用基本驗證。

33.3.3.12 basicAuthLib

目的、用途

指定本地程式庫名稱。SFCB 伺服器會載入程式庫，以驗證用戶端使用者識別碼。預設值為 `sfcBasicPAMAuthentication`。

語法

`provProcs`: 最大程序數

33.3.3.13 useChunking

目的、用途

此選項可啟用或停用 HTTP/HTTPS 區塊化功能。如果啟用，伺服器會將大量回應資料以較小的「區塊」傳回到用戶端，而不是採用緩衝資料，然後以一個區塊全部送回的方式。預設值為 `true`。

語法

`useChunking`: 選項

選項	描述
<code>true</code>	啟用 HTTP/HTTPS 資料區塊化功能。
<code>false</code>	停用 HTTP/HTTPS 資料區塊化功能。

33.3.3.14 keepaliveTimeout

目的、用途

指定 SFCB HTTP 程序在同一個連線上兩次請求間的最長等待時間 (秒)。達到此時間後，程序將終止。如果將其設定為 0，則會停用 HTTP 保持連線功能。預設值為 0。

語法

`keepaliveTimeout`: 秒數

33.3.3.15 keepaliveMaxRequest

目的、用途

指定一個連線上連續請求的最大數目。如果將其設定為 0，則會停用 HTTP 保持連線功能。預設值為 10。

語法

`keepaliveMaxRequest`: 連線數

33.3.3.16 registrationDir

目的、用途

指定註冊目錄，其中包含提供者註冊資料、階段區域和靜態儲存庫。預設值為 `/var/lib/sfcb/registration`。

語法

`registrationDir`: 目錄

33.3.3.17 providerDirs

目的、用途

指定 SFCB 從中搜尋提供者程式庫的目錄清單，以空格分隔。預設值為 /usr/lib64 /usr/lib64 /usr/lib64/cmpi。

語法

providerDirs: 目錄

33.3.3.18 providerSampleInterval

目的、用途

指定提供者管理員檢查閒置提供者的間隔 (秒)。預設值為 30。

語法

providerSampleInterval: 秒數

33.3.3.19 providerTimeoutInterval

目的、用途

指定提供者在閒置多少時間 (秒) 後由提供者管理員卸載。預設值為 60。

語法

providerTimeoutInterval: 秒數

33.3.3.20 providerAutoGroup

目的、用途

如果提供者註冊檔案未指定其他任何群組，並且該選項設定為 *true*，則同一個共享程式庫中的所有提供者都會在同一個程序中執行。

語法

`providerAutoGroup`: 選項

選項	描述
<code>true</code>	啟用提供者分組。
<code>false</code>	停用提供者分組。

33.3.3.21 sslCertificateFilePath

目的、用途

指定包含伺服器證書的檔案名稱。檔案必須為 **PEM** (隱私增強郵件，採用 **RFC 1421** 與 **RFC 1424** 標準) 格式。不過，此檔案僅在 `enableHttps` 設定為 `true` 時才要求使用。預設值為 `/etc/sfcb/server.pem`。

語法

`sslCertificateFilePath`: 路徑

33.3.3.22 sslKeyFilePath

目的、用途

指定包含伺服器證書之私密金鑰的檔案名稱。該檔案必須為 **PEM** 格式，可以不含密碼片語保護。不過，此檔案僅在 `enableHttps` 設定為 `true` 時才要求使用。預設值為 `/etc/sfcb/file.pem`。

語法

`sslKeyFilePath`: 路徑

33.3.3.23 sslClientTrustStore

目的、用途

指定包含 CA 或自行簽署之客戶端證書的檔案名稱。此檔必須為 PEM 格式，不過僅在 `sslClientCertificate` 設定為 `accept` 或 `require` 時才要求使用。預設值為 `/etc/sfcb/client.pem`。

語法

`sslClientTrustStore`: 路徑

33.3.3.24 sslClientCertificate

目的、用途

指定 SFCB 處理用戶端證書驗證的方式。如果設定為 `ignore`，則不會要求用戶端提供證書。如果設定為 `accept`，則會要求用戶端提供證書，不過即使用戶端不提供，操作也不會失敗。如果設定為 `require`，則會在客戶端不提供證書時拒絕客戶端連線。預設值為 `ignore`。

語法

`sslClientCertificate`: 選項

選項	描述
<code>ignore</code>	停用用戶端證書的請求。
<code>接受</code>	停用用戶端證書的請求。 即使不提供證書，也不會失敗。

選項	描述
require	如果沒有有效的證書，便拒絕用戶端連線。

33.3.3.25 certificateAuthLib

目的、用途

指定本地程式庫的名稱，以便請求基於用戶端證書的使用者驗證。僅當 `sslClientCertificate` 未設定為 `ignore` 時才需要指定。預設值為 `sfcCertificateAuthentication`。

語法

`certificateAuthLib`: 檔案

33.3.3.26 traceLevel

目的、用途

指定 SFCB 的追蹤層級。您可以透過設定環境變數 `SFCB_TRACE_LEVEL` 的方式對其進行覆寫。預設值為 0。

語法

`traceLevel`: 層級數

33.3.3.27 traceMask

目的、用途

指定 SFCB 的追蹤遮罩。您可以透過指令行選項 `--trace-components` 對其進行覆寫。預設值為 0。

語法

traceMask: 遮罩

33.3.3.28 traceFile

目的、用途

指定 SFCB 的追蹤檔案。您可以透過設定環境變數 SFCB_TRACE_FILE 的方式對其進行覆寫。預設值為 stderr (標準錯誤輸出)。

語法

traceFile: 輸出

33.4 進階 SFCB 任務

本章介紹有關 SFCB 使用的更多進階主題。為了便於理解，您需要先掌握 Linux 檔案系統的基本知識，並具備 Linux 指令行的操作經驗。本章包括以下任務：

- 安裝 CMPI 提供者
- 測試 SFCB
- 使用 wbemcli CIM 用戶端

33.4.1 安裝 CMPI 提供者

若要安裝 CMPI 提供者，需要確定其共享程式庫複製到 providerDirs 組態選項指定的其中一個目錄，請參閱第 33.3.3.17 節「providerDirs」[491 頁]。還必須使用 sfcbstage 與 sfcbrepos 指令正確註冊提供者。

系統通常會為 SFCB 準備提供者套件，以便安裝程序能夠正確進行註冊。此外，還為 SFCB 準備了大多數 SBLIM 提供者。

33.4.1.1 類別儲存庫

類別儲存庫是 SFCB 儲存 CIM 類別之相關資訊的位置。它通常包含一個由名稱空間元件所組成的目錄樹。常見的 CIM 名稱空間為 `root/cimv2` 或 `root/interop`，它們會分別轉譯為檔案系統上的類別儲存庫目錄路徑

```
/var/lib/sfcb/registration/repository/root/cimv2
```

和

```
/var/lib/sfcb/registration/repository/root/interop
```

每個名稱空間目錄都包含檔案 `classSchemas`。該檔案內有所有在該名稱空間下註冊之 CIM 類別的編譯二進位表示。同時還包含有關其 CIM 超類別的必要資訊。

此外，每個名稱空間目錄可能會包含檔案 `qualifiers`，內有該命名空間的所有修飾詞。Sfcbd 重新啟動時，類別提供者會掃描目錄 `/var/lib/sfcb/registration/repository/` 及其所有子目錄，以確定註冊的名稱空間。然後解碼 `classSchemas` 檔案，並建立每個名稱空間的類別階層。

33.4.1.2 新增類別

SFCB 無法執行線上 CIM 類別操作。您需要在離線模式下新增、變更或移除類別，然後使用 `rcsfcb restart` 重新啟動 SFCB 服務以註冊變更。

儲存提供者類別和註冊資訊時，SFCB 會使用一個稱為階段區域的位置。在 SUSE® Linux Enterprise Server 系統中，即 `/var/lib/sfcb/stage/` 下的目錄結構。

若要新增提供者，需要：

- 將提供者類別定義檔案複製到階段區域目錄(`/var/lib/sfcb/stage/mofs`)下的 `./mofs` 子目錄。
- 將包含類別名稱或提供者類型，以及可執行程式庫檔案名稱的註冊檔案複製到 `./regs` 子目錄。

階段目錄中有兩個預設「mof」(類別定義)檔案：indication.mof 與 interop.mof。執行 sfcbrepos 指令後，根階段目錄 /var/lib/sfcb/stage/mofs 下的 MOF 檔案將複製到每個名稱空間中。interop.mof 只會編譯至 *interop* 名稱空間。

目錄配置可能如下例所示：

```
tux@mercury:~> ls /var/lib/sfcb/stage
default.reg  mofs  regs

tux@mercury:~> ls /var/lib/sfcb/stage/mofs
indication.mof  root

tux@mercury:~> ls /var/lib/sfcb/stage/mofs/root
cimv2  interop  suse  virt

tux@mercury:~> ls -l /var/lib/sfcb/stage/mofs/root/cimv2 | less
Linux_ABIPParameter.mof
Linux_BaseIndication.mof
Linux_Base.mof
Linux_DHCPElementConformsToProfile.mof
Linux_DHCPEntity.mof
[...]
OMC_StorageSettingWithHints.mof
OMC_StorageVolumeDevice.mof
OMC_StorageVolume.mof
OMC_StorageVolumeStorageSynchronized.mof
OMC_SystemStorageCapabilities.mof

tux@mercury:~> ls -l /var/lib/sfcb/stage/mofs/root/interop
ComputerSystem.mof
ElementConformsToProfile.mof
HostSystem.mof
interop.mof
Linux_DHCPElementConformsToProfile.mof
[...]
OMC_SMIElementSoftwareIdentity.mof
OMC_SMISubProfileRequiresProfile.mof
OMC_SMIVolumeManagementSoftware.mof
ReferencedProfile.mof
RegisteredProfile.mof

tux@mercury:~> ls -l /var/lib/sfcb/stage/regs
AllocationCapabilities.reg
Linux_ABIPParameter.reg
Linux_BaseIndication.reg
Linux_DHCPGlobal.reg
Linux_DHCPRegisteredProfile.reg
[...]
OMC_Base.sfcb.reg
OMC_CopyServices.sfcb.reg
OMC_PowerManagement.sfcb.reg
```

```

OMC_Server.sfcf.reg
RegisteredProfile.reg

tux@mercury:~> cat /var/lib/sfcf/stage/regs/Linux_DHCPRegisteredProfile.reg
[Linux_DHCPRegisteredProfile]
    provider: Linux_DHCPRegisteredProfileProvider
    location: cmpiLinux_DHCPRegisteredProfile
    type: instance
    namespace: root/interop
#
[Linux_DHCPElementConformsToProfile]
    provider: Linux_DHCPElementConformsToProfileProvider
    location: cmpiLinux_DHCPElementConformsToProfile
    type: instance association
    namespace: root/cimv2
#
[Linux_DHCPElementConformsToProfile]
    provider: Linux_DHCPElementConformsToProfileProvider
    location: cmpiLinux_DHCPElementConformsToProfile
    type: instance association
    namespace: root/interop

```

SFCB 會對每個提供者使用一個自定的提供者註冊檔案。

注意：SBLIM 提供者註冊檔案

SBLIM 網站上的所有 SBLIM 提供者都已包含用於產生 SFCB 之 .reg 檔案的註冊檔案。

SFCB 註冊檔案的格式如下：

```

[<class-name>]
    provider: <provide-name>
    location: <library-name>
    type: [instance] [association] [method] [indication]
    group: <group-name>
    unload: never
    namespace: <namespace-for-class> ...

```

其中，

<類別名稱>

CIM 類別名稱 (必要)

<provider-name>

CMPI 提供者名稱 (必要)

<location-name>

提供者程式庫名稱 (必要)

type

提供者類型 (必要) 可以是 instance、association、method 或 indication 的任意組合。

<group-name>

可以將多個提供者組合在一起，在單一程序下執行，以便進一步減少對執行時期資源的佔用。在相同 <group-name> 下註冊的所有提供者會在同一程序下執行。預設情況下，每個提供者會做為獨立的程序執行。

unload

指定提供者的卸載規則。目前唯一支援的選項為 never，即不監控提供者的閒置時間，也不卸載提供者。預設情況下，當提供者的閒置時間超過組態檔案中指定的值時，就會被卸載。

namespace

可以執行此提供者之名稱空間的清單。這是必要選項，雖然對大多數提供者而言，此值均為 *root/cimv2*。

在階段區域中儲存所有類別定義和提供者註冊檔案後，需要使用指令 `sfcbrepos -f` 重建 SFCB 類別儲存庫。

您可以使用此方式新增、變更或移除類別。重建類別儲存庫後，使用指令 `rcsfcb restart` 重新啟動 SFCB。

此外，SFCB 套件還包含一個公用程式，會將提供者類別 `mof` 檔案和註冊檔案複製到階段區域中的正確位置。

```
sfcbstage -r [provider.reg] [class1.mof] [class2.mof] ...
```

執行此指令行後，仍需重建類別儲存庫並重新啟動 SFCB 服務。

33.4.2 測試 SFCB

SFCB 套件包含兩個測試程序檔：`wbemcat` 和 `xmltest`。

wbemcat 會透過 HTTP 通訊協定將原始 CIM-XML 資料傳送至在連接埠 5988 上監聽的指定 SFCB 主機(預設為 localhost)。然後顯示傳回的結果。以下檔案包含標準 EnumerateClasses 請求的 CIM-XML 表示：

```
<?xml version="1.0" encoding="utf-8"?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
  <MESSAGE ID="4711" PROTOCOLVERSION="1.0">
    <SIMPLEREQ>
      <IMETHODCALL NAME="EnumerateClasses">
        <LOCALNAMESPACEPATH>
          <NAMESPACE NAME="root"/>
          <NAMESPACE NAME="cimv2"/>
        </LOCALNAMESPACEPATH>
        <IPARAMVALUE NAME="ClassName">
          <CLASSNAME NAME=""/>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="DeepInheritance">
          <VALUE>TRUE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="LocalOnly">
          <VALUE>FALSE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="IncludeQualifiers">
          <VALUE>FALSE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="IncludeClassOrigin">
          <VALUE>TRUE</VALUE>
        </IPARAMVALUE>
      </IMETHODCALL>
    </CIM></SIMPLEREQ>
  </MESSAGE>
</CIM>
```

將此請求傳送至 SFCB CIMOM 會傳回有註冊提供者之所有支援類別的清單。假設將檔案儲存為 cim_xml_test.xml。

```
tux@mercury:~> wbemcat cim_xml_test.xml | less
HTTP/1.1 200 OK
Content-Type: application/xml; charset="utf-8"
Content-Length: 337565
Cache-Control: no-cache
CIMOperation: MethodResponse

<?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
  <MESSAGE ID="4711" PROTOCOLVERSION="1.0">
    <SIMPLERSP>
      <IMETHODRESPONSE NAME="EnumerateClasses">
        [...]
        <CLASS NAME="Linux_DHCPPParamsForEntity" SUPERCLASS="CIM_Component">
          <PROPERTY.REFERENCE NAME="GroupComponent" REFERENCECLASS="Linux_DHCPEntity">
            </PROPERTY.REFERENCE>
```

```

<PROPERTY.REFERENCE NAME="PartComponent" REFERENCECLASS="Linux_DHCPParams">
</PROPERTY.REFERENCE>
</CLASS>
</IRETURNVALUE>
</IMETHODRESPONSE>
</SIMPLERSP>
</MESSAGE>
</CIM>

```

列出的類別會視系統上安裝的提供者而有所不同。

第二個程序檔 `xmltest` 也用於將原始 CIM-XML 測試檔案傳送至 SFCB CIMOM。傳送之後，它會將傳回的結果與之前儲存的「OK」結果檔案進行比較。如果不存在對應的「OK」檔案，則會予以建立，供後續使用。

```

tux@mercury:~> xmltest cim_xml_test.xml
Running test cim_xml_test.xml ... OK
Saving response as cim_xml_test.OK
tux@mercury:~> xmltest cim_xml_test.xml
Running test cim_xml_test.xml ... Passed

```

33.4.3 指令行 CIM 用戶端：wbemcli

除了 `wbemcat` 與 `xmltest` 外，SBLIM 專案還包含更進階的指令行 CIM 用戶端 `wbemcli`。該用戶端用於向 SFCB 伺服器傳送 CIM 請求，並顯示傳回的結果。它不依賴 CIMOM 程式庫，並可用於所有與 WBEM 相容的實作。

例如，如果需要列出由註冊到您 SFCB 的 SBLIM 提供者執行的所有類別，可向 SFCB 傳送「EnumerateClasses」(ec) 要求：

```

tux@mercury:~> wbemcli -dx ec http://localhost/root/cimv2
To server: <?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0"><SIMPLEREQ><IMETHODCALL \
  NAME="EnumerateClasses"><LOCALNAMESPACEPATH><NAMESPACE NAME="root"> \
    </NAMESPACE><NAMESPACE NAME="cimv2"></NAMESPACE> \
  </LOCALNAMESPACEPATH>
<IPARAMVALUE NAME="DeepInheritance"><VALUE>TRUE</VALUE> \
  </IPARAMVALUE>
<IPARAMVALUE NAME="LocalOnly"><VALUE>FALSE</VALUE></IPARAMVALUE>
<IPARAMVALUE NAME="IncludeQualifiers"><VALUE>FALSE</VALUE> \
  </IPARAMVALUE>
<IPARAMVALUE NAME="IncludeClassOrigin"><VALUE>TRUE</VALUE> \
  </IPARAMVALUE>
</IMETHODCALL></SIMPLEREQ>
</MESSAGE></CIM>
From server: Content-Type: application/xml; charset="utf-8"
From server: Content-Length: 337565

```

```

From server: Cache-Control: no-cache
From server: CIMOperation: MethodResponse
From server: <?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0">
<SIMPLERSP>
<IMETHODRESPONSE NAME="EnumerateClasses">
<IRETURNVALUE>
<CLASS NAME="CIM_ResourcePool" SUPERCLASS="CIM_LogicalElement">
<PROPERTY NAME="Generation" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="ElementName" TYPE="string">
</PROPERTY>
<PROPERTY NAME="Description" TYPE="string">
</PROPERTY>
<PROPERTY NAME="Caption" TYPE="string">
</PROPERTY>
<PROPERTY NAME="InstallDate" TYPE="datetime">
</PROPERTY>
[... ]
<CLASS NAME="Linux_ReiserFileSystem" SUPERCLASS="CIM_UnixLocalFileSystem">
<PROPERTY NAME="FSReservedCapacity" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="TotalInodes" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="FreeInodes" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="ResizeIncrement" TYPE="uint64">
<VALUE>0</VALUE>
</PROPERTY>
<PROPERTY NAME="IsFixedSize" TYPE="uint16">
<VALUE>0</VALUE>
</PROPERTY>
[... ]

```

-dx 選項會顯示由 wbemcli 傳送至 SFCB 的實際 XML，以及實際收到的 XML。在上例中，傳回的第一個類別是 CIM_ResourcePool，然後是 Linux_ReiserFileSystem。所有其他註冊類別也會顯示類似的項目。

如果省略 -dx 選項，則 wbemcli 只會顯示傳回資料的精簡表示：

```

tux@mercury:~> wbemcli ec http://localhost/root/cimv2
localhost:5988/root/cimv2:CIM_ResourcePool Generation=,ElementName=, \
    Description=,Caption=,InstallDate=,Name=,OperationalStatus=, \
    StatusDescriptions=,Status=,HealthStates=,PrimaryStatus=, \
    DetailedStatus=,OperatingStatus=,CommunicationStatus=,InstanceID=, \
    PoolID=,Primordial=,Capacity=,Reserved=,ResourceType=, \
    OtherResourceType=,ResourceSubType=, \AllocationUnits=
localhost:5988/root/cimv2:Linux_ReiserFileSystem FSReservedCapacity=, \
    TotalInodes=,FreeInodes=,ResizeIncrement=,IsFixedSize=,NumberOfFiles=, \
    OtherPersistenceType=,PersistenceType=,FileSystemType=,ClusterSize=, \

```



```
MaxFileNameLength=,CodeSet=,CasePreserved=,CaseSensitive=, \
CompressionMethod=,EncryptionMethod=,ReadOnly=,AvailableSpace=, \
FileSystemSize=,BlockSize=,Root=,Name=,CreationClassName=,CSName=, \
CSCreationClassName=,Generation=,ElementName=,Description=,Caption=, \
InstanceID=,InstallDate=,OperationalStatus=,StatusDescriptions=, \
Status=,HealthState=,PrimaryStatus=,DetailedStatus=,OperatingStatus= \
,CommunicationStatus=,EnabledState=,OtherEnabledState=,RequestedState= \
,EnabledDefault=,TimeOfLastStateChange=,AvailableRequestedStates=, \
TransitioningToState=,PercentageSpaceUse=
[...]
```

33.5 如需更多資訊

如需有關 **WBEM** 和 **SFCB** 的詳細資料，請參閱以下來源：

<http://www.dmtf.org>

Distributed Management Task Force 網站

<http://www.dmtf.org/standards/wbem/>

網路企業管理 (WBEM) 網站

<http://www.dmtf.org/standards/cim/>

Common Information Model (CIM) 網站

<http://sblim.wiki.sourceforge.net/>

Standards Based Linux Instrumentation (SBLIM) 網站

<http://sblim.wiki.sourceforge.net/Sfcb>

Small Footprint CIM Broker (SFCB) 網站

<http://sblim.wiki.sourceforge.net/Providers>

SBLIM 提供者套件

V. 疑難排解

說明和文件

SUSE® Linux Enterprise Server 隨附了各種來源的資訊和文件，其中有許多已整合到安裝的系統中。

`/usr/share/doc` 中的文件

這是傳統的說明目錄，包含系統的各種文件檔案及版本說明。子目錄 `packages` 中還提供了所安裝套件的相關資訊。如需詳細資訊，請參閱第 34.1 節「文件目錄」[508頁]。

外圍程序指令的 `man` 頁面與資訊頁

使用外圍程序時，不需要記住指令的選項。一般而言，外圍程序會以 `man` 頁面與資訊頁的方式提供整合式說明。如需詳細資訊，請參閱第 34.2 節「線上文件」[510頁] 與第 34.3 節「Info 頁面」[511頁]。

桌面說明中心

從 KDE 桌面的說明中心 (KDE help center) 與 GNOME 桌面的說明中心 (Yelp)，您可以透過搜尋的方式存取系統中大多數最重要的文件資源。這些資源包括已安裝之應用程式的線上說明、`man` 頁面、資訊頁以及產品隨附的 Novell/SUSE 手冊。

某些應用程式的獨立說明套件

使用 YaST 安裝新軟體時，通常會自動安裝軟體文件，而且多半會顯示在桌面系統的求助中心內。不過，有些應用程式 (例如 GIMP) 可能具有不同的線上說明套件，它們可以使用 YaST 獨立安裝，但不會整合到說明中心內。

34.1 文件目錄

安裝 Linux 系統後，可以在 `/usr/share/doc` 這個傳統目錄中找到文件。該目錄通常包含系統上已安裝之套件的相關資訊，以及版本說明和手冊等。

注意：內容取決於已安裝的套件

在 Linux 系統中，有許多手冊及其他類型的文件都可以像軟體一樣，以套件的形式獲取。`/usr/share/docs` 中包含的資訊量和類型也取決於所安裝的(文件) 套件。如果找不到此處提及的子目錄，請檢查您的系統中是否已安裝相應的套件，並根據需要使用 YaST 予以新增。

34.1.1 Novell/SUSE 手冊

我們提供不同語言的 HTML 和 PDF 版手冊。在 `manual` 子目錄下，可以找到您產品適用的大多數 HTML 版 Novell/SUSE 手冊。如需您產品適用的所有文件的綜覽，請參閱手冊的序。

如果安裝了多種語言，`/usr/share/doc/manual` 可能會包含不同語言版本的手冊。HTML 版本的 Novell/SUSE 手冊也可以在桌面系統的求助中心內找到。若想瞭解 PDF 和 HTML 版手冊在安裝媒體上的位置，請參閱 SUSE Linux Enterprise Server 的版本說明。這些手冊位於所安裝系統的 `/usr/share/doc/release-notes/` 目錄內，也可以在 <http://www.suse.com/doc/> 中產品特定的網頁內找到其線上版本。

34.1.2 HOWTO

如果您的系統中安裝了 `howto` 套件，`/usr/share/doc` 內還會存放 `howto` 子目錄，包含許多與 Linux 軟體設定及操作相關之任務的其他文件。

34.1.3 套件文件

在 `packages` 下面，可找到系統上已安裝之軟體套件中所包含的文件。系統會為每個套件建立一個子目錄 `/usr/share/doc/packages/ 套件名稱`。其中通常包含套件的讀我檔案，有時還包含範例、組態檔案或其他程序檔。以下清單

介紹了 `/usr/share/doc/packages` 下包含的一般檔案。每個項目不一定存在，許多套件可能只包含其中的一小部分。

AUTHORS

主要開發者清單。

BUGS

已知錯誤或異常狀況。可能還包含 **Bugzilla** 網頁的連結，透過該網頁可以搜尋所有錯誤。

CHANGES , ChangeLog

版本之間的變更摘要。因為它非常詳盡，所以對於開發人員而言通常很有幫助。

COPYING , LICENSE

授權資訊。

FAQ

自郵寄清單或新聞群組所收集的問題與解答。

INSTALL

在系統上安裝此套件的方法。由於在您讀取此檔案時已安裝套件，因此可以安心地忽略此檔案的內容。

README、README.*

有關軟體的一般資訊。例如用途和使用方法。

TODO

尚未執行但可能會在未來執行的項目。

MANIFEST

具有簡短摘要的檔案清單。

NEWS

說明此版本的新功能。

34.2 線上文件

man 頁面 Linux 系統的重要部分。它們提供指令用法以及所有可用選項與參數的說明。man 頁面可以使用man後接指令名稱的方式進行存取，例如man ls。

man 頁面會直接在外圍程序中顯示。若要導覽這些頁面，請使用 Page ↑ 和 Page ↓ 上移和下移。使用 Home 和 End，在文件的開頭和結尾之間移動。按 Q 結束此檢視模式。使用 man man，可詳細瞭解 man 指令本身的資訊。如 表格 34.1 「man 頁面 — 類別和說明」 [510頁] (取自 man 本身的 man 頁面) 所示，man 頁面會依類別儲存。

表格 34.1 man 頁面 — 類別和說明

數字	描述
1	執行程式或外圍程序指令
2	系統呼叫 (核心提供的功能)
3	程式庫呼叫 (程式庫中的函數)
4	特殊檔案 (通常位於 /dev 中)
5	檔案格式和慣例 (/etc/fstab)
6	遊戲
7	其他 (包括巨集套件與慣例)，例如，man(7)、groff(7)
8	系統管理指令 (通常只適用於 root)
9	核心常式 (非標準)

每一個線上文件由標籤為 *NAME*、*SYNOPSIS*、*DESCRIPTION*、*SEE ALSO*、*LICENSING* 以及 *AUTHOR* 等的許多部份組成。視指令的類型，可能還包括其他可用區段。

34.3 Info 頁面

Info 頁面是您系統上另一個重要的資訊來源。它們所提供的資訊通常比 `man` 頁面更為詳盡。若要檢視特定指令的資訊頁面，請輸入 `info`，後接指令名稱，例如 `info ls`。您可以直接在外圍程序中使用檢視器瀏覽資訊頁面，並可顯示不同的區段（稱為「節點」）。使用 `Space` 可以向前移動，使用 `<—` 可以向後移動。在節點內，您也可以使用 `Page ↑` 和 `Page ↓` 進行瀏覽，但要前往上一個或下一個節點，只能使用 `Space` 和 `<—`。按 `Q` 可以結束檢視模式。並不是所有 `man` 頁面都隨附資訊頁面，反之亦然。

34.4 線上資源

除了 `/usr/share/doc` 下所安裝之 Novell 手冊的線上版本外，您還可以在網站上存取產品專屬的手冊與文件。如需有關 SUSE Linux Enterprise Server 所有可用文件的綜覽，請查看產品專屬文件網頁 <http://www.novell.com/documentation/>。

如果您要搜尋其他產品相關的資訊，也可以造訪下列網站：

Novell 技術支援知識庫

<http://www.novell.com/support/> 上提供了 Novell 技術支援知識庫。該知識庫包含為解決 SUSE Linux Enterprise Server 的技術問題而撰寫的文章。

Novell 論壇

Novell 提供了多個論壇，您可以在其中深入研究有關 Novell 產品的各項討論。請參閱 <http://forums.novell.com/> 以取得論壇清單。

Cool Solutions

一個線上社群，提供可下載的文章、提示、問答集以及免費工具，網址為：
<http://www.novell.com/communities/coolsolutions>

KDE 文件

如需尋找有關 KDE 各方面資訊且適用對象為使用者和管理員的文件，請造訪 <http://www.kde.org/documentation/>。

GNOME 文件

<http://library.gnome.org/> 上提供了適用於 GNOME 使用者、管理員以及開發人員的文件。

The Linux Documentation Project

The Linux Documentation Project (TLDP) 由志願者組成的團體運營，該團體負責撰寫 Linux 相關文件 (請參閱 <http://www.tldp.org>)。TLDP 或許是能夠提供最全面的 Linux 相關文件的資源了。這組文件包含入門者的教學課程，但主要是針對有經驗的使用者和專業系統管理員。TLDP 已免費公開發行 HOWTO、常見問題集以及指南 (手冊)。SUSE Linux Enterprise Server 中也隨附了一部分來自 TLDP 的文件

您可能還想嘗試用於搜尋一般資訊的搜尋引擎。例如，如果燒錄 CD 或進行 LibreOffice 檔案轉換時遇到問題，可以搜尋「Linux CD-RW 說明」或「OpenOffice 檔案轉換問題」片語。Google™ 也提供專門針對 Linux 的搜尋引擎 (<http://www.google.com/linux>)，可能對您有幫助。

一般問題和解決方案

本章節介紹一些可能會發生的問題及其解決方案。即使這裡沒有與您完全相同的情況，或許可以從類似情況中獲得一些提示，來解決您遇到的問題。

35.1 尋找並收集資訊

Linux 會非常詳細地報告事件。當系統發生問題時，可以從幾個地方查看相關資訊，主要是 Linux 系統的標準記錄檔，也有與 SUSE Linux Enterprise Server 系統相關的記錄檔。大部分記錄檔都可以透過 YaST (「其他」>「檢視開機記錄」) 進行檢視。

YaST 可讓您收集支援團隊所需的所有系統資訊。請使用「其他」>「支援」，然後選取問題類別。在收集到所有資訊之後，將此份資訊連結到您的支援要求。

以下是最常查看的記錄檔案清單，以及它們各自的一般用途。包含 ~ 的路徑表示目前使用者的主目錄。

表格 35.1 記錄檔案

Log File	描述
<code>~/.xsession-errors</code>	來自目前執行中桌上應用程式的訊息。
<code>/var/log/apparmor/</code>	來自 AppArmor 的記錄檔案，請參閱第 IV 部分「Confining Privileges」

Log File	描述
	with AppArmor」(↑ <i>Security Guide</i>) 以獲得詳細資訊。
/var/log/audit/audit.log	來自 Audit 的記錄檔案，可追蹤對 檔案、目錄或系統資源的存取，並 追蹤系統呼叫。
/var/log/boot.msg	開機程序期間報告的來自核心的訊 息。
/var/log/mail.*	來自郵件系統的訊息。
/var/log/messages	執行時來自核心與系統記錄精靈的 即時訊息。
/var/log/NetworkManager	NetworkManager 中的記錄檔，用於 收集網路連接性的問題
/var/log/samba/	目錄包含 Samba 伺服器和用戶端記 錄訊息。
/var/log/SaX.log	來自 SaX 顯示器與 KVM 系統的硬 體訊息。
/var/log/warn	來自核心和系統記錄精靈的所有訊 息，均為「警告」或以上等級。
/var/log/wtmp	二進位檔案包含使用者對於目前機 器工作階段的登入記錄。請以 last 檢視。
/var/log/Xorg.*.log	來自 X Window System 的多種啟動 和執行時期記錄。對於 X 啟動失敗 的除錯非常實用。
/var/log/YaST2/	目錄包含 YaST 的動作與結果。

Log File	描述
<code>/var/log/zypper.log</code>	zypper 的記錄檔案。

與記錄檔不同的是，您的機器亦提供您執行中系統的資訊。請參閱表格 35.2: `/proc` 檔案系統的系統資訊

表格 35.2 `/proc` 檔案系統的系統資訊

檔案	描述
<code>/proc/cpuinfo</code>	包含處理器資訊，如類型、廠商、型號與效能。
<code>/proc/dma</code>	顯示目前使用的 DMA 頻道。
<code>/proc/interrupts</code>	顯示使用中的岔斷，以及每種岔斷正在使用的數量。
<code>/proc/iomem</code>	顯示 I/O (輸入/輸出) 記憶體的状态。
<code>/proc/ioports</code>	顯示此時正在使用的 I/O 連接埠。
<code>/proc/meminfo</code>	顯示記憶體状态。
<code>/proc/modules</code>	顯示個別模組。
<code>/proc/mounts</code>	顯示目前掛接的設備。
<code>/proc/partitions</code>	顯示所有硬碟的分割區。
<code>/proc/version</code>	顯示目前的 Linux 版本。

除了 `/proc` 檔案系統，Linux 核心還會輸出 `sysfs` 模組 (記憶體內檔案系統) 的相關資訊。此模組代表核心物件及其屬性和關係。如需有關 `sysfs` 的詳細資訊，請參閱第 14 章「使用 `udev` 進行動態核心設備管理」[167頁] 中 `udev` 的相關內容。表格 35.3 提供了 `/sys` 下最常用目錄的綜覽。

表格 35.3 /sys 檔案系統的系統資訊

檔案	描述
/sys/block	包含系統中探查到之每個區塊設備的子目錄。一般情況下，大部分設備都是磁碟類型的設備。
/sys/bus	包含每種實體匯流排類型的子目錄。
/sys/class	包含組合為功能型設備(如圖形、網路和印表機等)的多個子目錄
/sys/device	包含全域設備階層。

Linux 隨附多種工具可進行系統分析和監控。請參閱 第 2 章「*System Monitoring Utilities*」(↑系統分析與調整指南) 以取得用於系統診斷最重要的選項。

下面的每種情境所採用的編排順序是，先在標題中描述問題，隨後用一兩個段落提供建議的解決方案、詳細解決方案的參考資料，以及對其他相關情境的交叉參照。

35.2 安裝問題

安裝問題是安裝機器時失敗的一個狀況。可能是徹底失敗，也可能是無法啟動圖形安裝程式。本節重點介紹了您可能會遭遇的一般性問題，並對這些狀況提供了可能的解決方案或處理方式。

35.2.1 檢查媒體

若您在使用 SUSE Linux Enterprise Server 安裝媒體時遇到問題，請使用「軟體」>「媒體檢查」檢查安裝媒體的完整性。出現媒體問題可能性較大的是您自己燒錄的媒體。若要檢查 SUSE Linux Enterprise Server 媒體，請將其插入磁碟機，並按一下 YaST「媒體檢查」畫面中的「開始檢查」。這可能會花費幾分鐘。如果偵測到錯誤，請勿使用此媒體來進行安裝。

圖形 35.1 檢查媒體

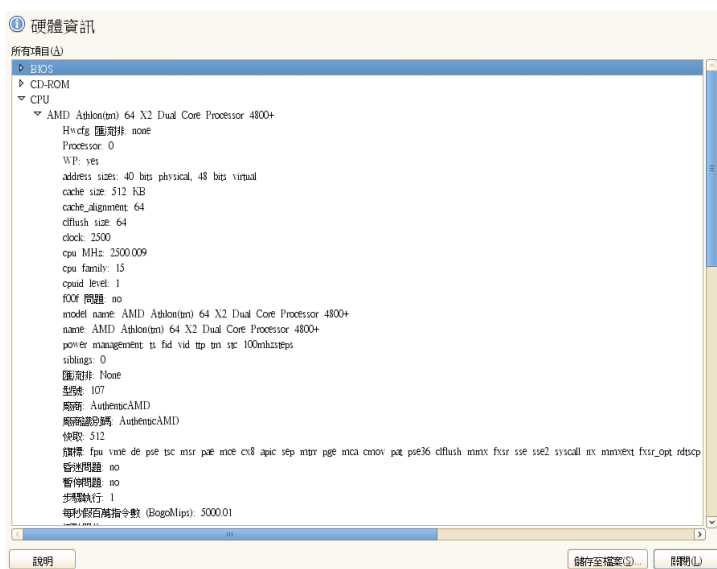


35.2.2 硬體資訊

使用「**硬體**」>「**硬體資訊**」顯示偵測到的硬碟和技術資料。按一下樹狀結構的任何節點，取得關於設備的更多資訊。提交需要提供硬體資訊的支援請求時，這個模組特別有用。

按一下「**儲存至檔案**」將顯示的硬體資訊儲存至檔案。選取想要的目錄和檔案名稱，然後按一下「**儲存**」來建立檔案。

圖形 35.2 顯示硬體資訊



35.2.3 無可用的可開機 DVD 磁碟機

如果您的電腦沒有可開機的 DVD-ROM 磁碟機，或是 Linux 不支援您的磁碟機，可以利用幾個選項在不使用內建 DVD 磁碟機的情況下安裝機器：

從磁片開機

建立開機磁片並從磁片而非 DVD 開機。

使用外接開機設備

如果 BIOS 和安裝核心支援，您可以從外接 DVD 磁碟機開機。

透過 PXE 以網路開機

如果機器沒有 DVD 磁碟機，但提供可用的乙太網路連線，則可採用全網路式安裝。請參閱第 14.1.3 節「透過 VNC 進行的遠端安裝—PXE 開機和網路喚醒功能」(第 14 章「遠端安裝」, ↑部署指南)和第 14.1.6 節「透過 SSH 進行的遠端安裝—PXE 開機和網路喚醒功能」(第 14 章「遠端安裝」, ↑部署指南)以取得詳細資料。

35.2.3.1 從磁片 (SYSLINUX) 開機

在某些舊型電腦上，沒有可用的可開機 DVD 磁碟機，只有軟碟機。若要在這類系統上安裝，請建立開機磁片並以此開機。

開機磁片包括 SYSLINUX 載入程式與 `linuxrc` 程式。SYSLINUX 允許在啟動程序選取核心以及硬體需要的任何參數。`linuxrc` 程式可以為您的硬體載入核心模組，然後開始安裝。

從開機磁片開機時，會由 SYSLINUX 載入器 (`syslinux` 套件) 起始開機程序。系統啟動時，SYSLINUX 會執行最小的硬體偵測，主要包括以下步驟：

1. 程式檢查 BIOS 是否提供 VESA 2.0—相容的框架緩衝區支援，然後啟動核心。
2. 讀取監視器資料 (DDC 資訊)。
3. 開機載入程式設定時，會讀取第一個硬碟的第一個區塊 (MBR)，將 BIOS ID 對應至 Linux 設備名稱。程式嘗試透過 BIOS 的 `lba32` 功能讀取區塊，判斷 BIOS 是否支援這些功能。

如果啟動 SYSLINUX 時，您一直按住 Shift，會略過所有這些步驟。基於疑難排解用途，請插入以下一行文字

```
verbose 1
```

於 `syslinux.cfg`，讓啟動載入器顯示目前執行的動作。

如果機器未從磁片開機，您可能需要將 BIOS 的啟動順序變更成 A, C, CDROM。

35.2.3.2 外接開機設備

Linux 支援大部分現有的 DVD 磁碟機。如果系統既沒有 DVD 磁碟機也沒有軟碟機，仍然可以使用 USB、FireWire 或 SCSI 來連接外接式 DVD 磁碟機，以執行系統開機。這操作主要依賴 BIOS 與所用硬體之間的互動。如果您遭遇到問題，有時更新 BIOS 可能會有幫助。

35.2.4 從安裝媒體開機失敗

機器無法開機安裝媒體的一個原因可能是 BIOS 中的開機順序設定不正確。在 BIOS 開機順序中，必須將 DVD 磁碟機設為開機的第一項。否則機器會嘗試從其他媒體開機，一般會從硬碟開機。有關變更 BIOS 開機順序的指導，可參閱隨主機板提供的文件，也可參閱下文段落。

BIOS 是提供電腦最基本功能的軟體。主機板供應商會針對自己的硬體提供特製的 BIOS。通常，BIOS 設定只可在特定時間 (機器開機時) 進行存取。在這個啟始化階段，機器會執行一些硬體診斷測試。其中之一是記憶體檢查，由記憶體計數器指示。當計數器出現時，請尋找指示按下按鍵來存取 BIOS 設定的一行文字，通常在計數器下方或底端某個位置。要按的鍵通常是 Del、F1 或 Esc 中的一個。請按住這個按鍵，直到 BIOS 設定畫面出現為止。

過程 35.1 變更 BIOS 開機順序

- 1 使用開機常式所宣告的正確按鍵進入 BIOS，等待 BIOS 畫面出現。
- 2 要變更 AWARD BIOS 中的開機順序，請尋找「*BIOS FEATURES SETUP*」(BIOS 功能設定) 項目。其他製造商可能使用不同的名稱，例如「*ADVANCED CMOS SETUP*」(進階 CMOS 設定)。當您找到該項目後，請選取並按 Enter 確認。
- 3 在隨後開啟的畫面中，找到「*BOOTSEQUENCE*」或「*BOOTORDER*」(開機順序) 子項目。開機順序通常顯示為 C, A 或 A, C。在前一種情況，機器首先搜尋硬碟 (C)，然後是軟碟機 (A) 來尋找可開機媒體。請按 PgUp 或 PgDown 鍵來變更設定，直到順序改成 A, CDROM, C 為止。
- 4 請按 Esc 來離開 BIOS 設定畫面。若要儲存變更，請選取「*SAVE & EXIT SETUP*」(儲存並結束設定)，或者按 F10。要確認儲存設定，請按 Y。

過程 35.2 在 *SCSI BIOS (Adaptec 主機介面卡)* 中變更開機順序

- 1 按 **Ctrl + A** 開啟設定。
- 2 選取「**磁碟公用程式**」。連接的硬體元件隨即顯示。
記下您 DVD 磁碟機的 SCSI ID。
- 3 使用 **Esc** 離開功能表。
- 4 開啟「*Configure Adapter Settings*」(設定介面卡設定)。在「*Additional Options*」(其他選項)下，請選取「*Boot Device Options*」(開機設備選項)，然後按 **Enter**。
- 5 輸入 DVD 磁碟機的 ID，然後再按 **Enter**。
- 6 按兩下 **Esc** 回到 SCSI BIOS 的開始畫面。
- 7 退出這個畫面，接著按「**Yes**」(是)來啟動電腦。

不管您最終安裝使用的語言和鍵盤配置為何，大部分的 BIOS 組態均使用美國鍵盤配置，如下圖所示：

圖形 35.3 美國鍵盤配置



35.2.5 無法開機

有些硬體類型 (多半是極舊或極新的機型) 無法安裝。在許多情況中，發生此狀況的原因是安裝核心不支援此類型的硬體，或是此核心中包含的某些功能 (如 ACPI) 會對一些硬體造成問題。

若您的系統無法使用標準「安裝」模式，從第一個安裝開機畫面安裝的話，請嘗試下列方法：

- 1 使用尚留在磁碟機中的 DVD，以 Ctrl + Alt + Del 或硬體重設按鈕重新開機。
- 2 出現開機畫面時按 F5，並使用鍵盤上的方向鍵導覽至「無 ACPI」，然後按 Enter 啟動開機與安裝程序。此選項會停用 ACPI 電源管理技術的支援。
- 3 如第 6 章「使用 YaST 安裝」(↑部署指南) 所述，繼續安裝。

如果失敗，請仍按上述步驟執行，但改選「安全設定」。此選項會停用 ACPI 和 DMA 支援。大部分硬體將以此選項開機。

若這些選項都失敗的話，請使用開機選項提示，將支援此類硬體所需的其他參數傳送到安裝核心。如需關於可做為開機選項之參數的詳細資訊，請參閱位於 `/usr/src/linux/Documentation/kernel-parameters.txt` 的核心文件。

提示：取得核心文件

安裝 `kernel-source` 套件以檢視核心文件。

其中有許多其他的 ACPI 相關參數，可讓您在開機前的開機提示中輸入，以進行安裝：

`acpi=off`

此參數會關閉電腦的所有 ACPI 子系統。如果您的電腦根本無法處理 ACPI 或者您認為電腦的 ACPI 造成問題，此參數會很有幫助。

`acpi=force`

永遠啟用 ACPI，即使電腦的 BIOS 出廠日期是在 2000 年以前。若沒有使用 `acpi=off`，設定此參數也會啟用 ACPI。

`acpi=noirq`

不將 ACPI 用於 IRQ 路由。

`acpi=ht`

只執行足夠啟用超執行緒的 ACPI。

`acpi=strict`

降低對不完全與 ACPI 規格相容之平台的容忍度。

`pci=noacpi`

停用新 ACPI 系統的 PCI IRQ 路由。

`pnpacpi=off`

當您的 BIOS 設定中包含錯誤的岔斷或連接埠時，可透過此選項解決序列或平行問題。

`notsc`

停用時戳計數器。可使用此選項解決系統中的計時問題。這是一項新功能。如果您發現機器上出現效能衰退，特別是越到最後，效能越低，甚至完全當機，不妨嘗試此選項。

`nohz=off`

停用 `nohz` 功能。如果您的機器當機，使用此選項可能會有所幫助。其他情況下則毫無用處。

一旦您判斷出正確的參數組合，YaST 就會自動將其寫入開機載入程式組態，以確定系統下次可正確開機。

如果核心載入或者安裝時發生不明錯誤，選取開機功能表的「記憶體測試」，檢查記憶體。若「記憶體測試」傳回錯誤，則通常會是硬體錯誤。

35.2.6 無法啟動圖形安裝程式

將媒體插入磁碟機並將系統重新開機後，會出現安裝畫面，但在選取「安裝」之後，圖形安裝程式並未啟動。

有許多方法可以解決此狀況：

- 嘗試選取安裝對話方塊的其他螢幕解析度。
- 選取「文字模式」進行安裝。
- 透過 VNC，使用圖形安裝程式進行遠端安裝。

過程 35.3 變更安裝的畫面解析度

- 1 開機以進行安裝。
- 2 按 F3 開啟功能表，從中選取較低解析度進行安裝。
- 3 選取「安裝」並如第 6 章「使用 YaST 安裝」(↑部署指南) 所述繼續安裝。

過程 35.4 在文字模式下安裝

- 1 開機以進行安裝。
- 2 按下 F3 並選取「文字模式」。
- 3 選取「安裝」並如第 6 章「使用 YaST 安裝」(↑部署指南) 所述繼續安裝。

過程 35.5 安裝 VNC

- 1 開機以進行安裝。
- 2 在開機選項提示中輸入下列文字：

```
vnc=1 vncpassword=some_password
```

以 VNC 安裝所使用的密碼取代 *some_password*。

- 3 選取「安裝」，然後按 Enter 啟動安裝。

這樣不會直接啟動圖形安裝常式，系統會繼續以文字模式執行，然後終止，顯示含有 IP 位址與連接埠號碼的訊息，根據此訊息便可以透過瀏覽器介面或 VNC 檢視器應用程式找到安裝程式。

- 4 如果使用瀏覽器來存取安裝程式，則啟動瀏覽器並輸入 SUSE Linux Enterprise Server 機器安裝常式所提供的位址資訊，並按 Enter：

```
http://ip_address_of_machine:5801
```

瀏覽器視窗中會開啟一個對話方塊，提示您輸入 VNC 密碼。輸入密碼，並如第 6 章「使用 YaST 安裝」(↑部署指南) 所述繼續安裝。

重要

若要在任何作業系統下、使用任何瀏覽器、透過 VNC 工作，首先必須啟用 Java 支援。

出現提示時，提供 VNC 檢視器的 IP 位址和密碼。會開啟一個視窗，顯示安裝對話。請如一般方式繼續安裝。

35.2.7 只有極簡開機畫面被啟動

將媒體插入磁碟機後，BIOS 常式結束，但系統未啟動圖形開機畫面。而是啟動一個非常簡化的文字介面。若機器無法提供足夠的圖形記憶體以轉譯圖形開機畫面，就可能發生此狀況。

雖然文字開機畫面看起來簡化，但其提供的功能幾乎與圖形介面一樣：

開機選項

與圖形介面不同的是，這裡無法以鍵盤游標選取開機選項。文字模式開機畫面的開機功能表，會在開機提示時提供一些可輸入的關鍵字。這些關鍵字對映到圖形版本所提供的選項。輸入您的選擇並按一下 **Enter** 以啟動開機程序。

自定開機選項

選取開機選項之後，在開機提示中輸入適當的關鍵字，或如第 35.2.5 節「無法開機」[521 頁]所述輸入自定開機選項。若要啟動安裝程序，請按下 **Enter**。

螢幕解析度

使用 **F** 鍵決定安裝時的螢幕解析度。若您需要以文字模式開機，請選擇 **F3**。

35.3 開機問題

開機問題指的是您的系統無法正常開機的狀況(無法開機到預期的執行層級和登入畫面)。

35.3.1 無法載入 GRUB 開機載入程式

若硬體運作正常，則可能是開機載入程式已損毀，Linux 無法在機器上啟動。若是這樣的話，必須重新安裝開機載入程式。若要重新安裝開機載入程式，請執行下列步驟：

- 1 將安裝媒體插入光碟機中。
- 2 重新開機。
- 3 從開機功能表選取「安裝」。
- 4 選擇語言。
- 5 接受授權合約。
- 6 在「安裝模式」螢幕中，選取「修復已安裝的系統」。
- 7 進入 YaST 系統修復模組後，選取「進階工具」，然後選取「安裝新開機載入程式」。
- 8 還原原始設定並重新安裝開機載入程式。
- 9 結束 YaST 系統修復並重新啟動系統。

另一個機器無法開機的原因可能跟 BIOS 有關：

BIOS 設定

檢查與您硬碟相關的 BIOS 設定。若在目前的 BIOS 設定下找不到硬碟本身，則可能只是未啟動 GRUB。

BIOS 開機順序

檢查您系統的開機順序是否包含硬碟。若未啟用硬碟選項，您的系統可能已正確安裝，但在需要存取硬碟時無法開機。

35.3.2 沒有圖形登入

若可開機，但未開機到圖形登入管理員，可能的問題不是出在預設的執行層級選擇，就是在於 X Window System 組態。若要檢查執行層級組態，請以根使用

者的身份登入，檢查機器是否設定為開機至執行層級 5 (圖形桌面)。有個方法可以快速檢查此設定，就是檢驗 `/etc/inittab` 的內容，如下：

```
tux@mercury:~> grep "id:" /etc/inittab
id:5:initdefault:
```

傳回的行指示機器的預設執行層級 (`initdefault`) 設為 5，且應開機至圖形桌面。若執行層級設為其他數字，請使用 YaST 執行層級編輯器模組將它設為 5。

重要

請勿手動編輯執行層級組態。否則 `SUSEconfig` (由 YaST 所執行) 會在下次執行時覆寫這些變更。若您需要在此進行手動變更，請在 `/etc/sysconfig/suseconfig` 中，將 `CHECK_INITTAB` 設定為 `no`。

若執行層級設為 5，可能是您的桌面或 X Windows 軟體設定錯誤或已損毀。請檢查 `/var/log/Xorg.*.log` 中的記錄檔，以瞭解 X 伺服器嘗試啟動時的訊息。若啟動時桌面出現故障，系統可能會將錯誤訊息記錄至 `/var/log/messages`。若這些錯誤訊息指出 X 伺服器中有組態問題，請嘗試修復這些問題。若仍然未出現圖形系統，請考慮重新安裝圖形桌面。

提示：手動啟動 X Window System

快速測試：若使用者目前已登入主控台中，則 `startx` 指令可強制 X Window System 以預設的組態啟動。若這樣沒有作用的話，會將錯誤記錄至主控台。

35.4 登入問題

登入問題是指，您的機器已確實開機並進入歡迎畫面或收到登入提示，但不接受使用者名稱或密碼，或是接受後運作不正常 (無法啟動圖形桌面、產生錯誤、出現指令行等等)。

35.4.1 有效的使用者名稱和密碼組合失敗

這種情形常發生於系統設定為使用網路驗證或目錄服務時，且基於某些原因，會無法從其所設定的伺服器取得結果。身為唯一的本地使用者，根使用者是唯一

一仍可登入這些機器的使用者。下面是機器看似運作良好卻無法正確執行登入的一些常見原因：

- 網路未作用。如須對此情況的進一步指示，請參閱第 35.5 節「網路問題」 [534頁]。
- DNS 此時未運作 (這樣會阻礙 GNOME 或 KDE 運作，也會妨礙系統驗證安全伺服器的要求)。若機器花費過久的時間回應任何動作的話，表示可能是這種情況。如需此主題的詳細資訊，請參閱第 35.5 節「網路問題」 [534頁]。
- 若系統設定為使用 Kerberos，則系統的本地時間有可能超過了 Kerberos 伺服器時間所容許的時間差 (一般為 300 秒)。若 NTP (網路時間協定) 未正確運作，或本地 NTP 伺服器未運作，則 Kerberos 驗證會停止作用，因為它必須仰賴網路上同步的共同時脈才可運作。
- 系統的驗證組態設定錯誤。請檢查 PAM 組態檔案是否有錯字或指示詞順序錯誤。如需關於 PAM 和所包含組態檔案語法的其他背景資料，請參閱第 2 章「*Authentication with PAM*」 (↑*Security Guide*)。
- 主分割區已加密。如需此主題的詳細資訊，請參閱第 35.4.3 節「無法登入加密的主分割區」 [531頁]。

對於所有非外部網路造成的問題，解決方案就是重新開機進入單一使用者模式，並修復組態後再次開機進入操作模式，以嘗試重新登入。若要開機進入單一使用者模式：

- 1 重新啟動系統。會出現開機畫面及提示。
- 2 在開機提示中輸入 1，讓系統開機進入單一使用者模式。
- 3 輸入根的使用者名稱與密碼。
- 4 進行必要的所有變更。
- 5 在指令行中輸入 `telinit 5`，開機進入完整多使用者及網路模式。

35.4.2 有效的使用者名稱和密碼不被接受

這顯然是使用者最常遇到的問題，其發生的原因有很多。根據您使用本地使用者管理和驗證，或使用網路驗證，會有不同原因造成登入失敗。

本地使用者管理可能因為下列原因而失敗：

- 使用者輸入的密碼有誤。
- 使用者包含桌面組態檔的主目錄損毀或有防寫保護。
- **X Window System** 可能無法驗證此特定使用者，尤其是在安裝目前版本的 **Linux** 之前，此使用者的主目錄已用於其他 **Linux** 版本的情況下。

若要找出本地登入失敗的原因，請執行下列步驟：

- 1 開始進行整個驗證機制的偵錯之前，先確認使用者可以正確記住密碼。若使用者無法正確記住密碼，請使用 **YaST** 使用者管理模組變更使用者的密碼。請注意 **Caps Lock** 鍵的使用，並根據需要進行切換。
- 2 以根使用者登入，並檢查 `/var/log/messages` 中有沒有登入程序和 **PAM** 的錯誤訊息。
- 3 嘗試從主控台登入 (使用 **Ctrl + Alt + F1**)。如果成功，表示問題不在 **PAM**，因為它能夠在此機器上驗證此使用者。嘗試找出 **X Window System** 或桌面系統 (**GNOME** 或 **KDE**) 的任何問題。如需詳細資訊，請參閱第 35.4.4 節「登入成功但 **GNOME** 桌面失敗」[532頁] 和第 35.4.5 節「登入成功但 **KDE** 桌面失敗」[532頁]。
- 4 若使用者的主目錄已由其他 **Linux** 版本使用，請移除使用者主目錄中的 `Xauthority` 檔案。使用主控台透過 **Ctrl + Alt + F1** 登入，並以此使用者身份執行 `rm .Xauthority`。這樣應可排除此使用者的 **X** 驗證問題。重新嘗試圖形登入。
- 5 若仍無法進行圖形登入，請以 **Ctrl + Alt + F1** 執行主控台登入。嘗試在其他畫面啟動 **X** 工作階段—第一個 (`:0`) 已被使用：

```
startx -- :1
```

這樣應可出現圖形畫面與您的桌面。若沒有的話，請檢查 **X Window System** 的記錄檔案 (`/var/log/Xorg.displaynumber.log`)，或您桌面應用程式的登入檔案 (位於使用者主目錄中的 `.xsession-errors`)，以得知是否有任何異常。

- 6 若由於組態檔案損毀導致桌面無法啟動，請繼續執行第 35.4.4 節「登入成功但 **GNOME** 桌面失敗」[532頁] 或第 35.4.5 節「登入成功但 **KDE** 桌面失敗」[532頁]。

以下是特定使用者在特定機器上網路驗證失敗的一些常見原因：

- 使用者輸入的密碼有誤。
- 機器的本地驗證檔案中已存在使用者名稱，但網路驗證系統也提供了，兩者產生了衝突。
- 主目錄是存在的，但損毀或無法使用。或許此目錄設為防止寫入，或位於此時無法存取的伺服器上。
- 使用者沒有登入驗證系統特定主機的許可。
- 機器的主機名稱已因某種原因而變更，而使用者沒有登入該主機的許可。
- 機器無法聯繫驗證伺服器，或是含有使用者資訊的目錄伺服器。
- X Window System 可能無法驗證此特定使用者，尤其是在安裝目前版本的 Linux 之前，此使用者的主目錄已用於其他 Linux 版本的情況下。

若要找出登入發生網路驗證失敗的原因，請執行下列步驟：

- 1 進行整個驗證機制的除錯之前，請先確認使用者所記的密碼正確無誤。
- 2 確定機器賴以進行驗證的目錄伺服器，並確定該伺服器已啟動且正在執行，而且能夠與其他機器正常進行通訊。
- 3 確定使用者的使用者名稱和密碼可以在其他機器上使用，以確定其驗證資料存在，而且已正確配送。
- 4 再看看在運作不正常的機器上，可否讓其他使用者登入。若其他使用者可以正常登入，或根使用者可以登入的話，請登入並檢驗 `/var/log/messages` 檔案。找出嘗試登入所對應的時間戳記，並判斷 PAM 是否已產生任何錯誤訊息。
- 5 嘗試從主控台登入 (使用 `Ctrl + Alt + F1`)。若是成功，說明問題不是出在 PAM 或使用者主目錄所在的目錄伺服器，因為能夠在此機器上驗證此使用者。嘗試找出 X Window System 或桌面系統 (GNOME 或 KDE) 的任何問題。如需詳細資訊，請參閱第 35.4.4 節「登入成功但 GNOME 桌面失敗」[532頁] 和第 35.4.5 節「登入成功但 KDE 桌面失敗」[532頁]。

- 6 若使用者的主目錄已由其他 Linux 版本使用，請移除使用者主目錄中的 `Xauthority` 檔案。使用主控台透過 **Ctrl + Alt + F1** 登入，並以此使用者身份執行 `rm .Xauthority`。這樣應可排除此使用者的 X 驗證問題。重新嘗試圖形登入。
- 7 若仍無法進行圖形登入，請以 **Ctrl + Alt + F1** 執行主控台登入。嘗試在其他畫面啟動 X 工作階段—第一個 (:0) 已被使用：

```
startx -- :1
```

這樣應可出現圖形畫面與您的桌面。若沒有的話，請檢查 X Window System 的記錄檔案 (`/var/log/Xorg.displaynumber.log`)，或您桌面應用程式的登入檔案 (位於使用者主目錄中的 `.xsession-errors`)，以得知是否有任何異常。

- 8 若由於組態檔案損毀導致桌面無法啟動，請繼續執行第 35.4.4 節「登入成功但 GNOME 桌面失敗」[532頁] 或第 35.4.5 節「登入成功但 KDE 桌面失敗」[532頁]。

35.4.3 無法登入加密的主分割區

建議對筆記型電腦使用加密的主分割區。如果無法登入您的筆記型電腦，通常只是因為無法解除鎖定您的分割區。

開機期間，您必須輸入密碼片語以解除鎖定加密的分割區。如果不輸入密碼片語，則開機程序會繼續，但分割區將處於鎖定狀態。

若要解除鎖定加密的分割區，請執行以下步驟：

- 1 按 **Ctrl + Alt + F1** 切換到文字主控台。
- 2 以 `root` 使用者身分登入。
- 3 使用以下指令重新啟動解除鎖定程序：

```
/etc/init.d/boot.cryptot restart
```

- 4 輸入可解除鎖定加密分割區的密碼片語。
- 5 按 **Alt + F7** 離開文字主控台並切換回登入畫面。

6 像往常一樣登入。

35.4.4 登入成功但 GNOME 桌面失敗

若出現此狀況，可能是 GNOME 組態檔案已損毀。其他症狀還包括鍵盤無法工作、畫面幾何錯亂，甚至畫面呈現空白的灰色區塊。此問題最重要的區隔是，若其他使用者可以登入，則此機器是正常運作的。此類問題或許可以較快解決，只要將使用者的 GNOME 組態目錄移到新的位置，讓 GNOME 啟始化新的組態目錄即可。雖然這樣算是強制使用者重新設定 GNOME，但並沒有資料因此遺失。

1 按Ctrl + Alt + F1切換到文字主控台。

2 使用您的使用者名稱登入。

3 將使用者的 GNOME 組態目錄移到一個暫時位置：

```
mv .gconf .gconf-ORIG-RECOVER
mv .gnome2 .gnome2-ORIG-RECOVER
```

4 登出。

5 再次登入，勿執行任何應用程式。

6 依照下列方式將 ~/.gconf-ORIG-RECOVER/apps/ 目錄複製回新的 ~/.gconf 目錄，修復您的個別應用程式組態資料 (包括 Evolution 電子郵件用戶端資料)：

```
cp -a .gconf-ORIG-RECOVER/apps .gconf/
```

若這樣導致登入問題，請嘗試僅修復重要的應用程式資料，並重新設定其他的應用程式。

35.4.5 登入成功但 KDE 桌面失敗

KDE 桌面無法讓使用者登入有幾個原因。快取資料損毀以及 KDE 桌面組態檔案損毀，均可能導致登入問題。

快取檔案可用於增進桌面啟動的效能。若此資料損毀的話，啟動速度會變慢或完全故障。請將其移除，並強制桌面啟動常式重新開始啟動。這樣會比正常啟動的時間久，但將不會損害資料的保存並讓使用者登入。

若要移除 KDE 桌面的快取檔案，請以根使用者身份發出以下指令：

```
rm -rf /tmp/kde-user /tmp/ksocket-user
```

以使用者名稱取代 *user*。移除這兩個目錄只會移除損毀的快取檔案，過程中並不會傷害到真正的資料。

我們永遠可以使用初始組態檔案取代損毀的桌面組態檔案。若您希望復原使用者的調整值，請在以預設組態值還原組態之後，小心地將調整值從暫存位置複製回原來位置。

若要以初始組態值取代損毀的桌面組態，請執行下列步驟：

- 1 按Ctrl + Alt + F1切換到文字主控台。
- 2 以此使用者名稱登入。
- 3 將 KDE 組態目錄和 *.skel* 檔案移動到暫時位置：

- 對 KDE3 使用以下指令：

```
mv .kde .kde-ORIG-RECOVER  
mv .skel .skel-ORIG-RECOVER
```

- 對 KDE4 使用以下指令：

```
mv .kde4 .kde4-ORIG-RECOVER  
mv .skel .skel-ORIG-RECOVER
```

- 4 登出。
- 5 再次登入。
- 6 成功啟動桌面後，將使用者自己的組態複製回原位：

```
cp -a KDEDIR/share .kde/share
```

使用步驟 3 [533頁] 中的目錄取代 *KDEDIR*。

重要

若使用者自己的調整值導致登入失敗，且一再重複，請重做以上步驟，但不要複製 `.kde/share` 目錄。

35.5 網路問題

您系統的許多問題可能都與網路有關，但可能一開始看不出來。例如，系統不允許使用者登入，可能就是某種網路問題所致。本節會介紹簡單的檢查清單，可讓您用來辨識所遇到網路問題的原因。

過程 35.6 如何識別網路問題

檢查機器網路連線時，請如下執行：

- 1 若使用乙太網路連線，請先檢查硬體。確認您的網路線正確插在電腦和路由器 (或集線器等) 上。正常情況下，乙太網路接頭旁的兩個控制燈都會亮起。

若連接失敗，請檢查網路線在其他機器上可否使用。若可以的話，就是您的網路卡造成的問題。若您的網路設定中包含集線器或交換器，也可能是這些設備的問題。

- 2 若使用無線連接的話，請檢查可否由其他機器建立無線連結。若無法建立，請聯絡無線網路管理員。
- 3 檢查完基本網路連線之後，請嘗試找出未回應的服務為何。收集您設定中所需所有網路伺服器的位址資訊。您可在適當的 YaST 模組中查詢，或詢問您的系統管理員。下列清單提供了設定中所包含的一些基本的網路伺服器，以及其故障的症狀。

DNS (名稱服務)

名稱服務損壞或故障會從許多方面影響網路的運作。若本地網路仰賴網路伺服器進行驗證，而因為名稱解析問題而找不到這些伺服器的話，使用者就無法登入了。故障名稱伺服器所管理的機器將無法「看到」彼此並進行通訊。

NTP (時間服務)

NTP 服務的損壞或完全故障會影響 Kerberos 驗證以及 X 伺服器的功能。

NFS (檔案服務)

若應用程式所需的資料儲存於掛接 NFS 的目錄中，萬一此服務關閉或設定錯誤，該應用程式將無法啟動或無法正常運作。最糟糕的情況是，如果因 NFS 伺服器出現故障，而找不到包含 `.gconf` 或 `.kde` 子目錄的使用者主目錄，則使用者的個人桌面組態將無法起作用。

Samba (檔案服務)

若應用程式所需的資料儲存於出現故障之 Samba 伺服器的目錄中，該應用程式將無法啟動或無法正常運作。

NIS (使用者管理)

若您的 SUSE Linux Enterprise Server 系統仰賴出現故障之 NIS 伺服器提供使用者資料，使用者將無法登入這部機器。

LDAP (使用者管理)

若您的 SUSE Linux Enterprise Server 系統仰賴出現故障之 LDAP 伺服器提供使用者資料，使用者將無法登入這部機器。

Kerberos (驗證)

不進行驗證，也無法登入任何機器。

CUPS (網路列印)

使用者無法列印。

4 請檢查網路伺服器是否運作，且您的網路設定可否讓您建立連接：

重要

下述偵錯程序只適用於不涉及任何內部路由的簡易網路伺服器/用戶端設定。假設伺服器和用戶端都是相同子網路的成員，不需要其他路由。

- 4a** 使用 `ping IP 位址` 或 `主機名稱` (以伺服器的主機名稱取代主機名稱)，檢查各部機器是否開啟，以及能否回應網路。若此指令成功的話，就會告知您的主機您正在尋找並執行它，且您網路的名稱服務設定是正確的。

若 `ping` 的結果失敗且傳回 `destination host unreachable` (無法聯繫目的地主機)，則您的系統或想找的伺服器可能設定錯誤或故障。從其他機器執行 `ping IP 位址` 或您的主機名稱，檢查是否可連

接您的系統。如果您可以從另一台機器存取您的機器，可能是伺服器完全未執行或設定錯誤。

若 `ping` 失敗且傳回 `unknown host` (未知主機)，則是名稱服務設定錯誤，或使用的主機名稱不正確。如須對此問題做進一步檢查，請參閱步驟 4b [536 頁]。若 `ping` 仍然失敗，則是您的網路卡未設定正確，或網路硬體故障。

- 4b** 使用 `host hostname` 指令，檢查您嘗試連接的伺服器主機名稱是否正確轉譯為 IP 位址，反之亦然。若此指令傳回主機的 IP 位址，則名稱服務是啟動且執行中的。如果 `host` 指令失敗，請在您的主機上檢查所有與名稱及位址解析有關的網路組態檔案：

`/etc/resolv.conf`

此檔案用於追蹤您目前使用的名稱伺服器與領域。您可以手動修改此檔案，或以 YaST 或 DHCP 自動調整。建議您採用自動調整。然而，請確定此檔案的結構如下，且所有的網路位址與領域名稱均正確：

```
search fully_qualified_domain_name
nameserver ipaddress_of_nameserver
```

此檔案會包含多個名稱伺服器位址，其中至少有一個必須是正確的，才能為您的主機提供名稱解析。需要時，請使用 YaST 網路設定模組 (「主機名稱」/「DNS」索引標籤) 調整此檔案。

若您是透過 DHCP 處理網路連線，請在 YaST DNS 和主機名稱模組中選取「透過 DHCP 變更主機名稱」和「透過 DHCP 更新名稱伺服器搜尋清單」，以啟用 DHCP 來變更主機名稱與名稱服務資訊。

`/etc/nsswitch.conf`

此檔案會告知 Linux 何處可找到名稱服務資訊。檔案外觀如下：

```
...
hosts: files dns
networks: files dns
...
```

`dns` 項目是必備的。這會告訴 Linux 使用外部名稱伺服器。正常情況下，YaST 會自動管理這些項目，但檢查很謹慎。

若主機上所有相關的項目都正確的話，請要求您的系統管理員檢查 DNS 伺服器組態是否具備正確的時區資訊。如需關於 DNS 的詳細資訊，請參閱第 24 章「網域名稱系統」[315頁]。若您確定主機和 DNS 伺服器的 DNS 組態正確物誤，請繼續檢查網路組態和網路設備。

- 4c** 若您的系統無法建立與網路伺服器的連線，且您已經從問題可能原因清單中排除名稱服務的問題，則請檢查網路卡的組態。

使用指令 `ifconfig network_device` (以根使用者身份執行) 來檢查設備是否正確設定。請確認 `inet address` 和 `Mask` 均已設定正確。IP 位址有錯誤或網路遮罩有位元遺失的話，都可能造成網路組態無法使用。必要的話，請一併於伺服器上執行此檢查。

- 4d** 如果名稱服務與網路硬體均設定正確且在執行中，但仍有些外部網路連線逾時或完全失敗，請使用 `traceroute fully_qualified_domain_name` (以根使用者身份執行) 來追蹤這些要求所採用的網路路由。此指令會列出請求從您機器傳送到其目的地所經的所有閘道 (躍程)。其會列出各躍程的回應時間，以及是否能取得此躍程。請使用 `traceroute` 加上 `ping` 找出問題的原因，並告知管理員。

一旦您辨識出網路問題的原因，就可以自己解決 (若問題發生在您機器上的話)，或將您的發現告訴網路系統管理員，讓他們可以重新設定服務，或修復必要的系統。

35.5.1 NetworkManager 問題

若您有網路連線的問題，請依過程 35.6, “如何識別網路問題” [534頁] 所述將範圍調窄。若 NetworkManager 似乎有問題，請執行下列步驟，取得 NetworkManager 故障原因的提示記錄：

- 1 開啟外圍程序並以 `root` 身份登入。
- 2 重新啟動 NetworkManager：

```
rcnetwork restart -o nm
```

- 3 以一般使用者身份開啟網頁，例如 <http://www.opensuse.org>，看看是否可以連接。
- 4 在 `/var/log/NetworkManager` 中收集 `NetworkManager` 狀態的所有相關資訊。

如需關於 `NetworkManager` 的詳細資訊，請參閱第 26 章「使用 *NetworkManager*」[355頁]。

35.6 資料問題

資料問題是指，機器或許可以 (或無法) 正確開機，但系統上有著明顯的資料損毀，且需要修復。遇到這些情況時，需要用到您重要資料的備份檔案，以讓您的系統回復到故障前的狀態。`SUSE Linux Enterprise Server` 提供了專用的 `YaST` 模組，用於系統備份與還原，並提供了一個救援系統，可從外部復原損毀的系統。

35.6.1 管理分割區影像

有時，您需要對整個分割區甚至是硬碟執行備份。`Linux` 附帶 `dd` 工具，可為磁碟建立完全一致的副本。結合 `gzip`，還能為您節省一些空間。

過程 35.7 備份和還原硬碟

- 1 以 `root` 使用者身分啟動外圍程序。
- 2 選取來源設備。一般類似 `/dev/sda` (標示為 *SOURCE*)。
- 3 決定要儲存影像 (標示為 *BACKUP_PATH*) 的位置。此位置必須不同於來源設備的位置。換言之，如果您對 `/dev/sda` 進行備份，就不能將影像檔案儲存在 `/dev/sda` 下。
- 4 執行以下指令建立壓縮影像檔：

```
dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
```

- 5 使用以下指令還原硬碟：

```
gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
```

如果您只需備份分割區，請使用各個分割區取代指令中預留的 *SOURCE*。如此，您的影像檔便會存放於同一個硬碟的不同分割區中。

35.6.2 備份重要資料

使用 YaST 系統備份模組，可輕鬆管理系統備份：

- 1 以根使用者身份啟動 YaST，並選取「系統 / 、」 > 「系統備份」。
 - 2 建立持有備份所需所有細節、歸檔檔名、範圍和備份類型等資訊的備份設定檔：
 - 2a 選取「設定檔管理」 > 「新增」。
 - 2b 輸入歸檔的名稱。
 - 2c 若您希望將備份保存於本地，請輸入備份的路徑與位置。若您要將備份歸檔於網路伺服器 (透過 NFS)，請輸入要存放歸檔的 IP 位址或伺服器名稱和目錄。
 - 2d 決定歸檔類型，並按一下「下一步」。
 - 2e 決定要使用的備份選項，如不隸屬任何套件的檔案是否要備份，以及建立歸檔前是否要先顯示檔案清單。同時也要決定是否要使用耗時的 MD5 機制，辨識檔案是否已變更過。

使用「進階」進入備份整個硬碟區域的對話。此選項目前只適用於 Ext2 檔案系統。

 - 2f 最後，請設定搜尋限制，以將不需備份的特定系統區域從備份區域中排除，如所定的檔案或是快取檔案。新增、編輯或刪除項目，直到符合您的需求為止，再按「確定」離開。
- 3 完成設定檔設定之後，您就可以立即使用「開始」開始備份，或設定自動備份。您亦可針對其他不同目的，建立其他設定檔。

若要為已知設定檔設定自動備份，請如下操作：

- 1 從「設定檔管理」中選取「自動備份」功能表。

- 2 選取「*開始自動備份*」。
- 3 決定備份的頻率。選擇「*每日*」、「*每週*」或「*每月*」。
- 4 決定備份開始時間。這些設定會根據所選取的備份頻率而定。
- 5 決定是否保留舊的備份，以及要保留多少。若要收到自動產生的備份程序狀態訊息，請按一下「*傳送摘要郵件給使用者 root*」。
- 6 按一下「*確定*」套用您的設定，並於指定的時間啟動第一次備份。

35.6.3 還原系統備份

使用 YaST 系統還原模組，從備份還原系統組態。您可還原整個備份，或選取特定損毀而需要重設置舊狀態的元件。

- 1 啟動「YaST」>「系統」>「系統還原」。
- 2 輸入備份檔案的位置。可以是本地檔案、掛載於網路的檔案，或是軟碟或 DVD 等抽取式設備中的檔案。然後按「*下一步*」。

下列對話方塊會顯示歸檔內容的摘要，如檔案名稱、建立日期、備份類型和選用的註解。
- 3 按一下「*歸檔內容*」檢視歸檔的內容。按一下「*確定*」返回「*歸檔內容*」對話方塊。
- 4 會開啟「*進階選項*」對話方塊，讓您微調還原程序。按一下「*確定*」即可回到「*歸檔內容*」對話。
- 5 按一下「*下一步*」開啟要還原的套件檢視畫面。按「*接受*」還原歸檔中的所有檔案，或使用各式各樣的「*全選*」、「*取消全選*」和「*選取檔案*」按鈕，微調您的選擇。只有當 RPM 資料庫損毀或已刪除，而且此檔案包含於備份中時，才使用「*還原 RPM 資料庫*」選項。
- 6 按一下「*接受*」之後，就會還原備份。備份程序完成後，請按一下「*結束*」離開模組。

35.6.4 修復損毀的系統

系統無法啟動並正常運作的原因可能有幾種。最常見的原因是系統當機後檔案系統損毀、組態檔案損毀，或開機載入程式組態損毀。

SUSE Linux Enterprise Server 提供了兩種不同的方法來解決這些情況。您可以使用 YaST 系統修復功能，或啟動救援系統。下面幾節會介紹這兩種系統修復方法。

35.6.4.1 使用 YaST 系統修復

注意：鍵盤與語言設定

如果您在開機後變更了語言設定，鍵盤也會相應調整。

啟動 YaST 的「系統修復」模組前，請判定要使用哪種模式執行，以符合您的需求。根據嚴重性與系統故障的原因 (以及您的技術水準)，有三種不同的模式可以選擇：

自動修復

若您的系統會因為未知的原因故障，而您基本上不知道系統的哪個部分導致故障，請使用「*自動修復*」。這會對所安裝系統的所有元件進行大規模的自動檢查。如需此程序的詳細描述，請參閱章節「自動修復」[542頁]。

自定修復

若您的系統故障，且您已經知道哪個元件造成故障，請將系統分析的範圍限制在那些元件上，停止「*自動修復*」冗長的系統檢查。例如，若故障前的系統訊息指示套件資料庫有錯誤，則您可將分析與修復程序限定於檢查並復原系統的這一部份。如需此程序的詳細描述，請參閱章節「自定修復」[543頁]。

進階工具

如果您已經清楚瞭解發生故障的元件，且知道該如何修復，則可略過分析步驟，直接套用修復相關元件所需的工具。如需詳細資訊，請參閱章節「進階工具」[544頁]。

如上所述選擇修復模式之一，並如以下章節所述繼續進行系統修復。

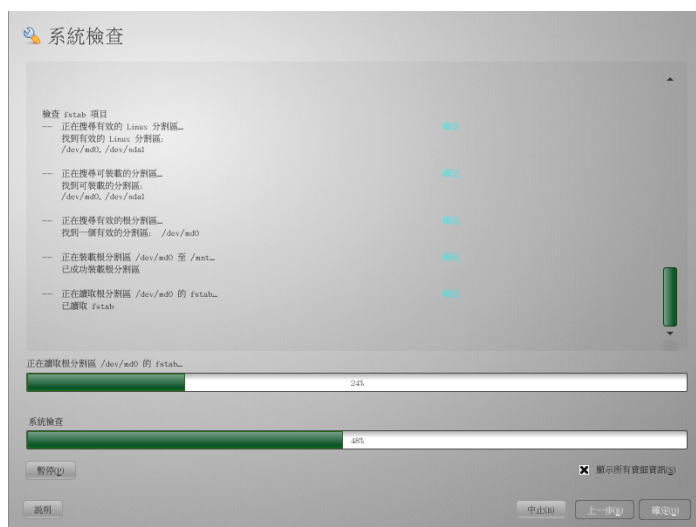
自動修復

若要啟動「YaST 系統修復」的自動修復模式，請如下執行：

- 1 將 SUSE Linux Enterprise Server 的安裝媒體插入 DVD 光碟機。
- 2 重新啟動系統。
- 3 在開機畫面中，選取「修復已安裝的系統」。
- 4 確認授權合約並按一下「下一步」。
- 5 選擇「自動修復」。

YaST 會立即啟動已安裝系統的大規模分析。程序的進度會以畫面底部的兩個進度列顯示。上面的進度列顯示目前執行測試的進度。下面的進度列顯示分析程序的整體進度。上方區段的記錄視窗會追蹤目前執行中的測試及其結果。請參閱圖形 35.4 「自動修復模式」[542頁]。

圖形 35.4 自動修復模式



每次執行時都會執行下列主測試執行。其中包括一些個別的子測試：

檢查分割區表

對所有偵測到之硬碟的分割區表，進行有效性和連貫性的檢查。

檢查交換區域

對所安裝系統的交換分割區進行偵測、測試，並提議啟用(若適用)。您應接受此提議，以便達到更高的系統修復速度。

檢查檔案系統

所有偵測到的檔案系統都會進行檔案系統的特定檢查。

檢查 fstab 項目

針對檔案中的項目進行完整性和一致性的檢查。所有有效分割區都會進行裝載。

檢查套件資料庫

檢查是否具有最小安裝作業所需的所有套件。雖然您也可以選擇分析基礎套件，但這很耗時，因為套件的數量十分龐大。

檢查開機載入器組態

針對已安裝系統(GRUB 或 LILO)的開機載入程式組態，檢查其完整性和一致性。這時會檢查開機和 root 設備，並檢查 initrd 模組的可用性。

- 6 發生錯誤時，程序會停止，並開啟對話方塊，說明詳細資訊及可能的解決方法。

請仔細閱讀畫面訊息，再接受建議的修復動作。若您決定拒絕建議的解決方案，系統會保留不變。

- 7 修復程序成功完成之後，請按一下「確定」和「完成」，並移除安裝媒體。這樣系統就會自動重新開機。

自定修復

若要啟動「自定修復」模式，並選擇性檢查已安裝系統的特定元件，請依照下列步驟執行：

- 1 將 SUSE Linux Enterprise Server 的安裝媒體插入 DVD 光碟機。
- 2 重新啟動系統。
- 3 在開機畫面中，選取「修復已安裝的系統」。

4 確認授權合約並按一下「*下一步*」。

5 選擇「*自定修復*」。

選擇「*自定修復*」會顯示測試執行清單，這些測試執行最初都會標記為執行。測試的整個範圍會與自動修復相符。如果您已經知道系統沒有受損，請取消相對應測試的標記。按一下「*下一步*」，然後啟動範圍較小的測試程序，它所需的執行時間可能短的多。

不是所有測試群組都可以個別套用。檔案系統的檢驗一定會結合 `fstab` 項目的分析，包括現有的交換分割區。YaST 會選擇必要測試的最小執行數量，自動解析這樣的相依性。YaST 不支援加密分割區。如果您有加密分割區，YaST 會通知您這一情況。

6 發生錯誤時，程序會停止，並開啟對話方塊，說明詳細資訊及可能的解決方法。

請仔細閱讀畫面訊息，再接受建議的修復動作。若您決定拒絕建議的解決方案，系統會保留不變。

7 修復程序成功完成之後，請按一下「*確定*」和「*完成*」，並移除安裝媒體。這樣系統就會自動重新開機。

進階工具

如果您瞭解 SUSE Linux Enterprise Server，而且清楚知道需要修復系統中的哪些元件，請略過系統分析，直接套用工具。

若要使用「YaST 系統修復」模組的「*進階工具*」功能，請依照下列步驟執行：

1 將 SUSE Linux Enterprise Server 的安裝媒體插入 DVD 光碟機。

2 重新啟動系統。

3 在開機畫面中，選取「*修復已安裝的系統*」。

4 確認授權合約並按一下「*下一步*」。

5 選取「*進階工具*」，然後選擇一個修復選項。

- 6 修復程序成功完成之後，請按一下「確定」和「完成」，並移除安裝媒體。這樣系統就會自動重新開機。

「進階工具」可提供下列選項來修復故障系統：

「安裝新的開機載入程式」

這會啟動 YaST 開機載入程式組態模組。如需詳細資訊，請參閱第 10.2 節「使用 YaST 設定開機載入程式」[119頁]。

「將已安裝的系統開機」

嘗試將已安裝的 Linux 系統開機。

「啟動磁碟分割工具」

這會啟動 YaST 裡的進階分割工具。

「修復檔案系統」

這會檢查您已安裝系統中的檔案系統。系統會先提供所有偵測到之分割區的選單，供您選擇一個來進行檢查。

「復原遺失的分割區」

您可以嘗試重建受損的分割區表。首先會提供所偵測到的硬碟清單，供您選擇。按一下「確定」，啟動檢查。這可能需要一些時間，具體視電腦速度及硬碟的大小和速度而定。

重要：「重建分割區表」

重建分割區表有些麻煩。YaST 會分析硬碟的資料磁區，嘗試辨識遺失的分割區。辨識之後，會將遺失的分割區新增至重新建好的分割區表。不過，這個方法並不一定適用於每個所想得到的例子。

「將系統設定儲存至軟碟」

這個選項將重要的系統檔案儲存至軟碟。如果這些檔案中有一個受損，就可以從磁碟還原。

「驗證安裝的軟體」

這會檢查套件資料庫的一致性，和最重要套件的可用性。任何已安裝套件在受損時都可以使用這個工具重新安裝。

35.6.4.2 使用救援系統

SUSE Linux Enterprise Server 包含一個救援系統。救援系統是一個小型的 Linux 系統，可以載入到 RAM 磁碟上並裝載為根目錄檔案系統，好讓您從外部存取 Linux 分割區。藉由此救援系統，您可以復原或修改任何重要的系統項目：

- 操作任何類型的組態檔案。
- 檢查檔案系統有無缺失並啟動自動修復程序。
- 在「變更根目錄」環境中存取已安裝的系統。
- 檢查、修改和重新安裝開機載入程式設定。
- 從錯誤安裝的設備驅動程式或無法使用的核心復原。
- 使用 Parted 指令來調整分割區大小。如需此工具的詳細資訊，請造訪 GNU Parted 網站 <http://www.gnu.org/software/parted/parted.html>。

救援系統可以從各種來源與位置載入。最簡單的方法就是從原始安裝媒體將救援系統開機：

- 1 將安裝媒體插入 DVD 光碟機。
- 2 重新啟動系統。
- 3 在開機畫面中按 F4，然後選擇「*DVD-ROM*」。之後從主功能表中選擇「救援系統」。
- 4 在 Rescue: 提示輸入 root。無須輸入密碼。

如果硬體安裝內容不包括 DVD 磁碟機，您可以從網路來源 啟動救援系統。以下範例適用於遠端開機情境 — 如果使用其他開機媒體 (例如 DVD)，請相應修改 info 檔案，並按照一般安裝方式開機。

- 1 輸入 PXE 開機設定的組態，然後新增下列行：
`install=protocol://instsource` 和 `rescue=1`。如果需要啟動系統修復，請使用 `repair=1`。正如一般安裝的情況，`protocol` 代表任何支援的網路通訊協定 (NFS、HTTP、FTP 等等)，而 `instsource` 代表網路安裝來源的路徑。

- 2 依照第 14.3.7 節「區域網路喚醒」(第 14 章「遠端安裝」,↑部署指南)中的說明,使用「網路喚醒」啟動系統。
- 3 在 Rescue: 提示輸入 root。無須輸入密碼。

一旦進入救援系統後,您可以利用 Alt + F1 至 Alt + F6 來使用虛擬主控台。

/bin 目錄中提供外圍程序以及其他許多有用的公用程式,例如 mount 程式。sbin 目錄中包含重要的檔案與網路公用程式,以便檢視及修復檔案系統。此目錄中也包含最重要的二進位系統維護程式,例如 fdisk、mkfs、mkswap、mount、mount、init 及 shutdown,還有維護網路的 ifconfig、ip、route 以及 netstat。目錄 /usr/bin 包含 vi 編輯器、find、less 以及 ssh。

若要檢視系統訊息,請使用指令 dmesg 或檢視檔案 /var/log/messages。

檢查和操作組態檔案

為了舉例說明使用救援系統如何修正組態檔案,請想像系統由於組態檔案損毀而無法正常開機。您可以使用救援系統來解決這個問題。

若要操作組態檔案,請執行下列步驟:

- 1 使用上述的其中一個方法啟動救援系統。
- 2 若要將 /dev/sda6 下的開機檔案系統裝載到救援系統,請使用下列指令:

```
mount /dev/sda6 /mnt
```

系統的所有目錄現在都存放在 /mnt 中

- 3 將此目錄變更到裝載的開機檔案系統中:

```
cd /mnt
```

- 4 在 vi 編輯器中開啟有問題的組態檔案。調整並儲存設定。
- 5 從救援系統解除裝載開機檔案系統:

```
umount /mnt
```

- 6 重新開機。

修復和檢查檔案系統

一般而言，檔案系統無法在執行中的系統上修復。如果發生了嚴重的問題，您可能甚至無法裝載開機檔案，而且系統可能會因為「核心異常」而無法開機。在此情況下，唯一的方法就是從外部修復系統。強烈建議您使用 YaST 系統修復來執行這項任務 (如需詳細資料，請參閱第 35.6.4.1 節「使用 YaST 系統修復」[541頁])。不過，如果您需要執行手動檔案系統檢查或修復，請啟動救援系統。其中包含的公用程式可檢查和修復 btrfs、ext2、ext3、ext4、reiserfs、xfs、dosfs 以及 vfat 檔案系統。

存取已安裝的系統

如果需要從救援系統存取已安裝的系統，您需要在變更根目錄環境中執行此操作。例如，若要修改開機載入程式組態或執行硬體組態公用程式。

若要根據已安裝的系統設定變更根目錄環境，請執行下列步驟：

- 1 首先，從已安裝系統與設備檔案系統掛接根分割區 (將設備名稱變更為目前設定)：

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

- 2 現在您可以「變更根目錄」至新環境：

```
chroot /mnt
```

- 3 接著裝載 /proc and /sys：

```
mount /proc
mount /sys
```

- 4 最後，從已安裝的系統裝載其餘分割區：

```
mount -a
```

- 5 現在您可以存取已安裝的系統。重新啟動系統之前，請先使用 `umount -a` 來解除裝載分割區，並以 `exit` 離開「變更根」目錄環境。

警告：限制

雖然您可以完全存取已安裝系統的檔案和應用程式，但必須遵守某些限制。執行中的核心是使用救援系統啟動的核心，而不是使用變更根目錄環境啟動的核心。它只支援基本硬體，而且無法從已安裝系統新增核心模組，除非核心版本完全一致。一律使用 `uname -r` 檢查目前執行的 (救援) 核心，然後確定變更根目錄環境的 `/lib/modules` 目錄中是否有相符的子目錄。如果有，您便可以使用已安裝的模組，否則，需要在其他媒體 (例如 USB 隨身碟) 上提供模組的正確版本。多數情況下，救援核心版本與已安裝的版本並不相同，因此，舉例來說，您便不能像平常一樣存取聲卡。您也無法啟動圖形使用者介面。

另外請注意，當您使用 `Alt + F1` 至 `Alt + F6` 來切換主控台時，將會離開「變更根」目錄環境。

修改和重新安裝開機載入程式

有時候系統無法開機是因為開機載入程式組態已損毀。譬如說，開機載入程式若未執行，啟動常式便無法將實體磁碟機轉譯為 Linux 檔案系統中的實際位置。

若要檢查開機載入程式組態和重新安裝開機載入程式，請執行下列步驟：

- 1 執行存取已安裝系統所需的必要步驟，如章節「存取已安裝的系統」[548頁]所述。
- 2 根據第 10 章「開機載入程式 *GRUB*」[109頁]中概述的 GRUB 組態原則，檢查下列檔案是否正確設定，並在必要時加以修正。

- `/etc/grub.conf`
- `/boot/grub/device.map`
- `/boot/grub/menu.lst`
- `/etc/sysconfig/bootloader`

- 3 依序使用下列指令來重新安裝開機載入程式：

```
grub --batch < /etc/grub.conf
```

4 解除裝載分割區，從「變更根目錄」環境登出，並重新啟動系統：

```
umount -a  
exit  
reboot
```

修正核心安裝

核心更新可能會帶來新的錯誤，進而會影響系統作業。例如，系統中某個硬體的驅動程式可能有錯誤，致使您無法存取和使用系統。在這種情況下，請復原至上回正常運作的核心(如果系統中提供的話)，或者從安裝媒體安裝原始核心。

提示：如何在更新後保留之前的核心

為了防止在錯誤的核心更新後無法開機，請使用核心多版本功能，並告知 libzypp 您要在更新後保留哪些核心。

例如，若要永遠保留最後兩個核心和目前執行中的核心，請新增

```
multiversion.kernels = latest,latest-1,running
```

至 `/etc/zypp/zypp.conf` 檔案。

另一個類似的情況是，當您需要重新安裝或更新 SUSE Linux Enterprise Server 不支援之設備的已損毀驅動程式時。例如，當硬體廠商使用特定設備時，比如使用硬體 RAID 控制器，這就要求作業系統能夠識別二進位驅動程式。廠商一般會發行「驅動程式更新磁碟」，內含所需驅動程式的修正或更新版本。

在這兩種情況下，您都需要以救援模式存取安裝的系統，並修正與核心相關的問題，否則系統可能無法正常開機：

- 1 從 SUSE Linux Enterprise Server 安裝媒體開機。
- 2 如果您要在錯誤的核心更新之後復原，請跳過此步驟。如果需要使用驅動程式更新磁碟(DUD)，請在開機功能表出現之後按 **F6** 以載入驅動程式更新，並選擇驅動程式更新的路徑或 URL，然後按一下「是」確認。
- 3 從開機功能表中選擇「救援系統」，然後按 **Enter**。如果您之前選擇使用 DUD，系統將會要求您指定儲存驅動程式更新的位置。
- 4 在 **Rescue:** 提示輸入 `root`。無須輸入密碼。

- 5 手動將目標系統和「變更根目錄」掛接至新環境：如需詳細資訊，請參閱章節「存取已安裝的系統」[548頁]。
- 6 如果要使用 DUD，請安裝/重新安裝/更新錯誤的設備驅動程式套件。請務必確定已安裝的核心版本與要安裝的驅動程式版本完全相符。

如果要修正錯誤的核心更新安裝，可以按照以下程序從安裝媒體安裝原始核心。

- 6a 使用 `hwinfo --cdrom` 識別 DVD 設備，並使用 `mount /dev/sr0 /mnt` 掛接設備。
 - 6b 導覽到 DVD 上儲存核心檔案的目錄，例如 `cd /mnt/suse/x86_64/`。
 - 6c 使用 `rpm -i` 指令安裝您的產品類別所需的 `kernel-*`、`kernel-*-base` 以及 `kernel-*-extra` 套件。
 - 6d 安裝完成之後，檢查與新安裝核心相關的新功能表項目是否已新增至開機載入程式組態檔 (grub 對應的組態檔為 `/boot/grub/menu.lst`)。
- 7 根據需要更新組態檔，然後重新啟動開機載入程式。如需詳細資訊，請參閱章節「修改和重新安裝開機載入程式」[549頁]。
 - 8 從系統磁碟機中取出任何可開機的媒體，然後重新開機。

35.7 IBM System z: 使用 initrd 做為救援系統

如果升級或修改 IBM System z 的 SUSE® Linux Enterprise Server 核心，可能會意外以不一致的狀態重新啟動系統，使得對已安裝系統執行 IPL 的標準程序失敗。在已經安裝新的或更新的 SUSE Linux Enterprise Server 核心，但尚未執行 `zipl` 程式來更新 IPL 記錄時，最容易發生這種意外。在此狀況下，請使用標準安裝套件做為救援系統，可在其中執行 `zipl` 程式以更新 IPL 記錄。

35.7.1 IPL 救援系統

重要：提供使用安裝資料

若要使用這種方法，必須取得適用於 IBM System z 的 SUSE Linux Enterprise Server 的安裝資料。如需詳細資訊，請參閱第 4.2.1 節「提供使用安裝資料」（第 4 章「在 IBM System z 上安裝」，↑部署指南）。除此之外，您需要設備的通道號碼和包含 SUSE Linux Enterprise Server 安裝的根目錄檔案系統的設備內分割區數目。

首先，對適用於 IBM System z 的 SUSE Linux Enterprise Server 安裝系統執行 IPL，如第 4.2 節「準備安裝」（第 4 章「在 IBM System z 上安裝」，↑部署指南）中所述。然後會出現使用的網路介面卡選項清單。

選取「啟動安裝或系統」，然後選取「啟動救援系統」以啟動救援系統。視安裝環境而定，您現在必須指定網路介面卡的參數和安裝來源。救援系統便會載入，且結尾會顯示下列登入提示：

```
Skipped services in runlevel 3:  nfs nfsboot
```

```
Rescue login:
```

現在可以使用 root 身份登入，無需密碼。

35.7.2 設定磁碟

在此狀態下，尚未設定任何磁碟。您必須先設定磁碟，才能繼續。

過程 35.8 設定 DASD

1 使用下列指令來設定 DASD：

```
dasd_configure 0.0.0150 1 0
```

0.0.0150 是連接 DASD 的通道。1 表示啟用磁碟（此處的 0 會停用磁碟）。0 表示磁碟的「無 DIAG 模式」（此處的 1 會啟用磁碟的 DAIG 存取）。

2 現在 DASD 已經上線（請使用 `cat /proc/partitions` 來檢查），而且可以用於後續指令。

過程 35.9 設定 zFCP 磁碟

- 1 若要設定 zFCP 磁碟，您必須先設定 zFCP 介面卡。使用下列指令來執行此動作：

```
zfcplib_configure 0.0.4000 1
```

0.0.4000 是連接介面卡的通道，而 1 表示啟動 (此處的 0 會停用介面卡)。

- 2 啟用介面卡之後，便可以設定磁碟。使用下列指令來執行此動作：

```
zfcplib_disk_configure 0.0.4000 1234567887654321 8765432100000000 1
```

0.0.4000 是之前使用的通道 ID，1234567887654321 是 WWPN (全球連接埠號碼)，而 8765432100000000 則是 LUN (邏輯單元編號)。1 表示啟用磁碟 (此處的 0 會停用磁碟)。

- 3 現在 zFCP 磁碟已經上線 (請使用 `cat /proc/partitions` 來檢查)，而且可以用於後續指令。

35.7.3 裝載根設備

如果所有所需磁碟均已上線，您現在就應該能夠裝載根設備。假設根設備位於 DASD 設備的第二分割區 (/dev/dasda2)，對應的指令為 `mount /dev/dasda2 /mnt`。

重要：檔案系統一致性

如果安裝的系統未正確關閉，建議在裝載之前檢查檔案系統一致性。如此可避免意外遺失資料。使用此範例，發出指令 `fsck /dev/dasda2` 以確定檔案系統處於一致的狀態。

僅需發出指令 `mount`，便可以檢查檔案系統是否已正確裝載。

範例 35.1 裝載指令的輸出

```
SuSE Instsys suse:/ # mount
shmfs on /newroot type shm (rw,nr_inodes=10240)
devpts on /dev/pts type devpts (rw)
virtual-proc-filessystem on /proc type proc (rw)
/dev/dasda2 on /mnt type reiserfs (rw)
```

35.7.4 變更至已裝載的檔案系統

`zipl` 指令可從安裝的系統之根設備讀取組態檔，而非從救援設備，可使用 `chroot` 指令來變更安裝系統的根設備：

範例 35.2 `chroot` 至已裝載的檔案系統

```
SuSE Instsys suse:/ # cd /mnt
SuSE Instsys suse:/mnt # chroot /mnt
```

35.7.5 執行 `zipl`

現在執行 `zipl` 將正確值重新寫入 IPL 記錄：

範例 35.3 使用 `zipl` 安裝 IPL 記錄

```
sh-2.05b# zipl
building bootmap : /boot/zipl/bootmap
adding Kernel Image : /boot/kernel/image located at 0x00010000
adding Ramdisk : /boot/initrd located at 0x00800000
adding Parmline : /boot/zipl/parmfile located at 0x00001000
Bootloader for ECKD type devices with z/OS compatible layout installed.
Syncing disks....
...done
```

35.7.6 結束救援系統

若要結束救援系統，首先以 `chroot` 指令和 `exit` 讓外圍程序保持開啟。若要防止資料遺失，請將所有未寫入的緩衝區以 `sync` 指令沖洗至磁碟。現在變更救援系統的根目錄，並解除裝載適用於 IBM System z 的 SUSE Linux Enterprise Server 安裝的根設備。

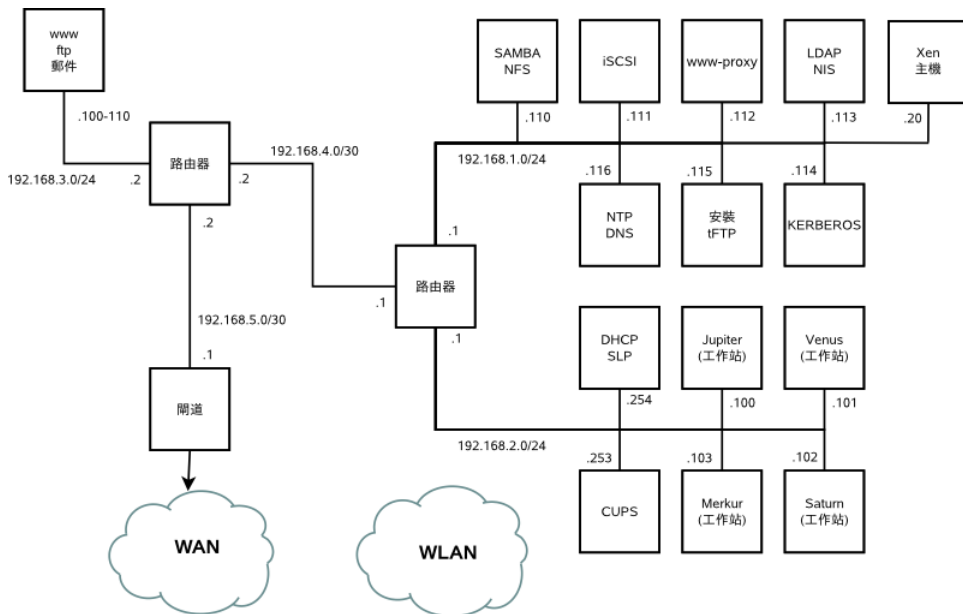
範例 35.4 解除裝載檔案系統

```
SuSE Instsys suse:/mnt # cd /
SuSE Instsys suse:/ # umount /mnt
```

最後，以 `halt` 指令停止救援系統。現在可以如第 6.15.1 節「IBM System z：對安裝的系統執行 IPL」（第 6 章「使用 *YaST* 安裝」，↑部署指南）所述對 SUSE Linux Enterprise Server 系統執行 IPL。

網路範例

此網路範例用於 SUSE® Linux Enterprise Server 文件中所有與網路相關的章節。





GNU Licenses

This appendix contains the GNU Free Documentation License version 1.2.

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D Preserve all the copyright notices of the Document.
- E Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

