Red Hat Linux 7.0

Das Offizielle Red Hat Linux Referenzhandbuch

ISBN: —

Red Hat, Inc.
2600 Meridian Parkway Durham NC 27713 US 919-547-0012 1-888-733-4281 919-547-0024
docs@redhat.com 13588 Research Triangle Park NC 27709

RefGuide(DE)-7.0-Print-RHI (2000-07-24T10:53-0400)

Printed in Canada, Ireland, and Japan

Inhalt

Red Hat Linux 7.0

Einführung

Willkommen

Willkommen beim *Offiziellen Red Hat Linux Referenzhandbuch*.

Das *Offizielle Red Hat Linux Referenzhandbuch* enthält nützliche Informationen über Ihr Red Hat Linux System. Sie können die meisten Informationen, die Sie hier finden, auf fast alle Linux-Distributionen anwenden. Es wäre ganz in unserem Sinne, wenn sich dieses Buch für Sie zu einem wertvollen Nachschlagewerk entwickeln würde. Von der Verwendung von RPM über Gnome-RPM bis hin zu spezifischen Detailinformationen zur Festplattenpartitionierung erhalten Sie in ihm eine Vielzahl nützlicher Informationen.

Wenn Sie ein wenig mehr über die Funktionsweise Ihres Red Hat Linux Systems erfahren möchten, ist dieses Buch genau das Richtige für Sie. Es werden unter anderem folgende Themen behandelt:

- Partitionierungskonzepte — eine Einführung in Plattenpartitionen und in die Strategien, die bei der Installation mehrerer Betriebssysteme auf einer Festplatte eine Rolle spielen.
- Installation im Textmodus — Obwohl bei Red Hat Linux jetzt auch ein Installationsprogramm mit grafischer Benutzeroberfläche zur Verfügung steht, können Sie weiterhin eine Installation im Textmodus durchführen. In diesem Abschnitt erfahren Sie alles Wissenswerte zu diesem Thema.
- RPM — Vom Gnome-RPM-Frontend bis zur Verwendung von RPM an der Konsole.
- RAID-Konzepte — Nehmen Sie eine Festplatte, fügen Sie eine zweite, eine dritte hinzu… Fassen Sie sie zu einer einzelnen logischen Einheit zusammen, und Ihnen stehen Speicherkapazität und Leistung zur Verfügung.
- Konfiguration nach der Installation — Möchten Sie das System nach der Installation ein wenig feinabstimmen? Hier wird beschrieben, an welcher Stelle Sie ansetzen können.

So finden Sie die richtige Dokumentation

Auch wenn Sie in Ihrem *Offiziellen Red Hat Linux Referenzhandbuch* schon ziemlich detaillierte Informationen zu Ihrem Red Hat Linux System finden, ist es dennoch wichtig, dass Sie sich die Dokumentation beschaffen, die für Ihren Kenntnisstand in Sachen Linux geeignet ist. Unabhängig von den Erfahrungen, die Sie bereits mit Linux gemacht haben, können Sie sich ohne die richtige Dokumentation schnell überfordert fühlen.

Schauen wir uns doch einfach die drei Kategorien von Red Hat Linux Benutzern an, um etwas genauer sagen zu können, welche Dokumentation am besten für Sie geeignet ist. Zunächst sollten Sie sich klar werden, wie umfangreich Ihre Vorkenntnisse sind. Hier sind die drei grundlegenden Kategorien:

Linux-Neuling

Dieser Benutzertyp hat bislang noch kein Linux-Betriebssystem (oder von Linux abgeleitetes Betriebssystem) verwendet oder verfügt nur über geringe Kenntnisse in Linux. Möglicherweise sind bereits gewisse Kenntnisse im Umgang mit anderen Betriebssystemen vorhanden (beispielsweise Windows). Trifft das auf Sie zu? In diesem Fall sollten Sie sich *Dokumentation für Linux-Neulinge* durchlesen.

Gewisse Erfahrung mit Linux

Dieser Benutzertyp hat Linux (allerdings nicht Red Hat Linux) bereits zuvor erfolgreich installiert und verwendet. Er verfügt unter Umständen auch über vergleichbare Erfahrungen mit anderen Betriebssystemen, die Linux ähneln. Trifft das auf Sie zu? In diesem Fall sollten Sie sich *Dokumentation für erfahrene Linux-Benutzer* durchlesen.

Alter Hase

Dieser Benutzertyp hat Red Hat Linux bereits zuvor erfolgreich installiert und verwendet. Sind Sie ein alter Hase in Sachen Linux? In diesem Fall sollten Sie sich *Dokumentation für Linux-Experten* durchlesen.

Dokumentation für Linux-Neulinge

Auch der längste Fluss beginnt irgendwo seinen Lauf. Dieses alte Sprichwort gilt auch für das Erlernen des Red Hat Linux Systems. Das gründliche Einarbeiten in Linux ist ein langer, aber lohnender Weg, bei dem Sie feststellen werden, dass Ihnen Linux Möglichkeiten eröffnet, von denen die Benutzer anderer Betriebssysteme nur träumen können. Sie müssen nur erst einmal den ersten Schritt dieses langen Wegs wagen - und im Folgenden erfahren Sie, wie Sie hierzu vorgehen müssen.

Der erste Schritt besteht im Allgemeinen darin, sich die nötige Dokumentation zu besorgen. Die Wichtigkeit dieses Schritts kann gar nicht oft genug betont werden, da Sie ohne die erforderlichen Informationen Ihr Red Hat Linux System nicht nach Ihren Wünschen einrichten können und sich möglicherweise rasch wieder von Linux abwenden werden.

Nachstehend wird beschrieben, nach welchen Kriterien Sie Ihre Dokumentation auswählen sollten:

- Eine kurze Geschichte der Entwicklung von Linux — Viele Aspekte von Linux lassen sich durch die historische Entwicklung dieses Betriebssystems besser verstehen. Es gibt sogar so etwas wie eine Linux-Kultur, die wiederum eng mit dieser Geschichte verbunden ist. Wenn Sie sich zumindest ein bisschen mit der Entstehungsgeschichte von Linux auskennen, kommt Ihnen das auch beim Gedankenaustausch mit erfahreneren Linux-Benutzern im Internet zugute.
- Eine Erklärung der Funktionsweise von Linux — Auch wenn es sicher nicht nötig ist, sich mit den exotischsten Fragestellungen hinsichtlich des Linux-Kernels auseinanderzusetzen, ist doch ein grundlegendes Verständnis der Funktionsweise von Linux sehr hilfreich. Diese Kenntnisse sind vor allem dann wichtig, wenn Sie sich bereits mit anderen Betriebssystemen auskennen. Einige der Konzepte dieser Betriebsysteme können möglicherweise nicht direkt auf Linux übertragen werden. Ein paar Kapitel mit Anmerkungen zur Funktionsweise von Linux (und vor allem zu Unterschieden zwischen Ihrem gewohnten Betriebssystem und Linux) leisten einen unverzichtbaren Beitrag zum erfolgreichen Start mit Ihrem Red Hat Linux System.

- Eine einführende Befehlsübersicht (mit Beispielen) — Dies ist vielleicht der wichtigste Punkt bei Ihrer Suche nach geeigneter Linux-Dokumentation. Die grundlegende Philosophie hinter Linux besteht darin, dass die Kombination "kleiner" Befehle mit eingeschränktem Funktionsumfang der Verwendung einiger weniger "großer" und somit komplexer Befehle vorzuziehen ist. Die Verarbeitung der Daten erfolgt somit schrittweise und nicht in einem großen Arbeitsschritt, wie es bei komplexen Befehlen der Fall wäre. Wenn Sie sich nicht anhand von Beispielen mit dem von Linux vertretenen Ansatz für das Erledigen von Aufgaben vertraut machen, kann es sein, dass Sie von der Vielzahl der auf Ihrem Red Hat Linux System zur Verfügung stehenden Befehle schier überwältigt werden.

Im Folgenden erhalten Sie einige Hinweise, welche Art von Dokumentation Ihren Anforderungen vermutlich am besten gerecht wird:

- Bücher — *Linux for Dummies* von John "maddog" Hall, erschienen bei IDG; *Using Linux* von William H. Ball, erschienen bei Que; *Running Linux* von Matt Welsh und Lar Kaufman, erschienen bei O'Reilly & Associates; *Red Hat Linux Secrets* von Naba Barkakati, erschienen bei IDG.
- Die Red Hat Website — Auf unserer eigenen Website (http://www.redhat.de) finden Sie Links zum Linux Documentation Project (LDP), dem *Offiziellen Red Hat Linux Installationshandbuch*, dem *Offiziellen Red Hat Linux Handbuch Erste Schritte*, den FAQs (häufig gestellten Fragen), der Datenbank für die Suche nach einer Linux-Benutzergruppe in Ihrer Nähe und einer weiteren Datenbank mit Wissenswertem zu Linux und mehr. Kurzum, auf unserer Website finden Sie alle Informationen, die Sie für Ihre ersten Schritte mit Linux benötigen.
- Newsgroups — Es gibt wohl kein anderes Betriebssystem, bei dem Neulinge so umfassende Unterstützung durch erfahrene Benutzer erhalten wie bei Linux. Im Usenet finden Sie Dutzende von Newsgroups zu Linux, darunter die folgenden Newsgroups, die bei einer Suche mit Deja News (http://www.deja.com) angegeben wurden:
  - linux.help
  - linux.redhat
  - linux.redhat.digest

- linux.redhat.misc
- linux.redhat.rpm

Auf der Website Deja.com haben Sie auch die Möglichkeit, nach bestimmten Informationen in Linux Newsgroups zu suchen.

Im nächsten Abschnitt erfahren Sie, welche Art von Dokumentation Sie dann heranziehen können.

Dokumentation für erfahrene Linux-Benutzer

Wenn Sie bereits andere Linux-Distributionen verwendet haben, sind Ihnen vermutlich bereits die am häufigsten verwendeten Befehle geläufig. Möglicherweise haben Sie ein eigenes Linux-System installiert und sogar Software aus dem Internet heruntergeladen und installiert. Welche Informationen benötigen Sie nun?

- Aufgabenorientierte Informationen — Häufig möchten Sie Ihr Red Hat Linux System auf eine bestimmte Weise konfigurieren, wissen aber nicht genau, wie Sie damit beginnen sollen. In diesem Fall ist es oft eine große Hilfe, wenn Sie wissen, wie andere Benutzer hierzu vorgegangen sind. Hier kann das Linux Documentation Project (auch als LDP bekannt) sehr nützlich sein. In jedem HOWTO-Dokument wird ein bestimmter Aspekt von Linux besprochen - von den Geheimnissen des Kernels bis hin zur Verwendung von Linux für einen Amateur-Radiosender.

  Wenn Sie eines der verschiedenen Pakete mit `HOWTO` -Dateien bei der Installation von Red Hat Linux ausgewählt haben, finden Sie die HOWTOs auf Ihrem System unter `/usr/share/doc/HOWTO`.

Dokumentation für Linux-Experten

Wenn Sie Red Hat Linux schon seit langem verwenden, haben Sie bei der Suche nach Dokumentation sicher auch bislang folgendes Motto berücksichtigt:

Immer erst die Quelle lesen!

Mitunter ist es schon völlig ausreichend, die Quelle zu lesen, um komplizierte Sachverhalte plötzlich zu begreifen. Und da Linux völlig frei verfügbar ist, stellt auch das Beschaffen dieser Quellen überhaupt kein Problem dar. Das eigentliche Problem liegt eher in deren Verständlichkeit…

Das ist für die Zukunft geplant...

Das *Offizielle Red Hat Linux Referenzhandbuch* ist Bestandteil des ständig wachsenden Engagements von Red Hat, Red Hat Linux Benutzer zum richtigen Zeitpunkt durch nützliche Informationen zu unterstützen. In den künftigen Ausgaben werden Sie erweiterte Informationen über Systemadministration, Konsolentools und weitere Ressourcen finden, damit Sie Ihr Red Hat Linux System — noch besser nutzen können.

Hierfür ist auch Ihr Beitrag von großer Bedeutung.

Teilen Sie uns Ihre Meinung mit

Wenn Sie Vorschläge zum *Offiziellen Red Hat Linux Referenzhandbuch* machen möchten, teilen Sie uns bitte die Kennung dieses Handbuchs mit:

RefGuide(DE)-7.0-Print-RHI (2000-07-24T10:53-0400)

Sie können Ihre E-Mails an folgende Adresse senden:

`docs@redhat.com`

Lassen Sie sich registrieren, um den Support nutzen zu können

Wenn Sie eine offizielle Ausgabe von Red Hat Linux 7.0 besitzen, denken Sie bitte daran, sich registrieren zu lassen, damit Sie in den Genuss der Vorteile kommen, auf die Sie als Red Hat Kunde Anspruch haben.

In Abhängigkeit davon, welches offizielle Red Hat Linux Produkt Sie erworben haben, können Sie einen oder alle der folgenden Vorteile nutzen:

- Offizieller Support durch Red Hat — Das Team für technischen Support von Red Hat, Inc. unterstützt Sie bei Installationsfragen.
- Vorrangiger FTP-Zugriff — Keine Besuche mehr auf hoffnungslos überlasteten Mirror Sites spät in der Nacht. Die Besitzer von Red Hat Linux 7.0 erhalten kostenlosen Zugriff auf priority.redhat.com, dem FTP-Dienst von Red Hat für alle registrierten Kunden. Dieser Server gewährleistet rund um die Uhr hohe Übertragungsraten.

- Red Hat Update Agent — Sie erhalten E-Mails direkt von Red Hat, sobald aktualisierte RPM-Dateien zur Verfügung stehen. Verwenden Sie Filter für Update Agent, um über aktualisierte Pakete zu Themen informiert zu werden, die für Sie von Interesse sind, und um diese schnell herunterzuladen. Darüber hinaus können Sie auch Updates für den Kernel und sicherheitsrelevante Bereiche sowie weitere Pakete automatisch erhalten.
- Under the Brim: Der offizielle Red Hat E-Newsletter — Sie erhalten die neuesten Nachrichten und Produktinformationen jeden Monat direkt von Red Hat.

Wenn Sie sich registrieren lassen möchten, stellen Sie eine Verbindung mit folgender Adresse her: http://www.redhat.com/now. Sie finden Ihre **persönliche Produkt-ID** auf einer rotweißen Karte in Ihrer offiziellen Red Hat Linux Packung.

Im Anhang des Offiziellen Red Hat Linux Installationshandbuchs finden Sie weitere Informationen über den technischen Support für das offizielle Red Hat Linux.

Und nun viel Erfolg bei der Arbeit mit Linux! Vielen Dank, dass Sie sich für Red Hat Linux entschieden haben!

Das Red Hat Dokumentationsteam

Teil I Systembezogene Referenzinformationen

1 Red Hat Linux 7.0 Neue Funktionsmerkmale

In diesem Kapitel werden die neuen Funktionen von Red Hat Linux 7.0 beschrieben.

1.1 Verbesserungen beim Installationsvorgang

Das Installationsprogramm von Red Hat Linux 7.0 enthält eine Reihe neuer Funktionsmerkmale. Weitere Informationen dazu finden Sie im *Offiziellen Red Hat Linux Installationshandbuch*.

1.2 Systembezogene neue Funktionsmerkmale

Red Hat Linux 7.0 bietet viele neue Funktionsmerkmale, die nicht Teil des Installationsvorgangs sind. So stehen Ihnen neue Tools und Anwendungen sowie neue Versionen des Kernels und der Desktop-Umgebungen zur Verfügung. Die nachfolgende Liste informiert Sie darüber, welche neuen Funktionen Ihnen in Red Hat Linux 7.0 zur Verfügung stehen, sobald Sie das Betriebssystem verwenden.

Linux-Kernel 2.2.4:

Red Hat Linux 7.0 enthält die neueste stabile Version des Linux-Kernels 2.2.*x*.

Verbesserte Kickstart-Installationen

Es stehen Ihnen verbesserte Kickstart-Installationen zur Verfügung dank neuer Befehle und einer verbesserten Partitionierung.

XFree86 **Version 4.0.1:**

Red Hat Linux 7.0 enthält die neueste Version von XFree86 (die Version 4.0.1 unterstützt viele neue Treiber).

Verbesserter Update Agent

Red Hat bietet nun eine benutzerdefinierbare Möglichkeit, Updates der Linux-Technologie zu erhalten. Durch den Update Agent und die Produktregistrierung ermöglicht Red Hat es Ihnen nun, jederzeit über die neuesten Hardware-

Treiber und Sicherheitsfunktionen zu verfügen, die automatische Benachrichtigung über Updates zu aktivieren etc. Weitere Informationen hierzu finden Sie unter http://www.redhat.com/now.

GNOME 1.2

Red Hat Linux 7.0 enthält jetzt GNOME 1.2.

Sawfish Windowmanager jetzt enthalten:

Der sawfish-Windowmanager ist jetzt als Standard-Windowmanager für GNOME in Red Hat Linux 7.0 enthalten. sawmill basiert auf einer Lisp-ähnlichen Sprache und ist erweiterbar und GNOME-kompatibel.

KDE 2.0

Red Hat Linux 7.0 enthält jetzt KDE 2.0.

GCC Compiler 2.9.6

Der GCC Compiler 2.9.6 ermöglicht das Schreiben eines schnelleren optimierten Codes und bietet umfassendere C++-Unterstützung.

Änderungen bei der Verschlüsselung:

Aufgrund der Lockerung der US-amerikanischen Verschlüsselungsgesetze wurden an den folgenden Paketen Änderungen hinsichtlich der Verschlüsselung vorgenommen:

- DieKerberos-Authentifizierung wurde dem Installationsprogramm hinzugefügt.
- Die LDAP-Authentifizierung wurde dem Installationsprogramm hinzugefügt.
- Red Hat Linux 7.0 enthält jetzt OpenSSH-Verschlüsselungstools, die Remote-Anmeldungen bei Ihrem System ermöglichen.
- Red Hat Linux 7.0 enthält die Kryptographie-Bibliothek OpenSSL, die sichere Transaktionen für Mail-, Web- und FTP-Kommunikation ermöglicht.

2 Systemadministration

In diesem Kapitel erhalten Sie einen Überblick über das Red Hat Linux System. Dieser Überblick soll dazu dienen, Sie mit einigen Aspekten von Red Hat Linux vertraut zu machen, die Sie möglicherweise noch nicht kennen. Außerdem erläutert dieses Kapitel einige der Unterschiede zwischen Red Hat Linux und anderen UNIX-Systemen.

2.1 Struktur des Dateisystems

Red Hat ist dem **Filesystem Hierarchy Standard** (**FHS**) verpflichtet. Dabei handelt es sich um ein gemeinsam mit anderen Institutionen erarbeitetes Dokument, in dem die Namen und Speicherorte vieler Dateien und Verzeichnisse festgelegt sind. Unser Unternehmen wird sich auch weiterhin nach diesem Standard richten, damit Red Hat Linux auch in Zukunft diesen Standard erfüllt.

Das aktuelle FHS-Dokument ist die maßgebende Referenz für alle FHS-konformen Dateisysteme. In diesem Abschnitt geben wir Ihnen einen Überblick über den Standard sowie eine Beschreibung jener Teile des Dateisystems, die vom Standard nicht beschrieben werden.

Den vollständigen Standard finden Sie unter:

http://www.pathname.com/fhs/

Die Konformität mit diesem Standard beinhaltet sehr viele Aspekte. Die beiden wichtigsten Aspekte sind jedoch die Kompatibilität mit anderen Systemen und die Möglichkeit, die Partition `/usr` als schreibgeschützte Partition zu mounten (da sie gemeinsam genutzte ausführbare Dateien enthält und keine Änderungen durch den Benutzer vorgesehen sind). Da `/usr` schreibgeschützt gemountet werden kann, besteht die Möglichkeit, `/usr` über die CD-ROM oder über ein schreibgeschütztes NFS-System von einem anderen Rechner aus zu mounten.

2.1.1 Überblick über den Dateisystemstandard (FHS)

Die hier beschriebenen Verzeichnisse und Dateien stellen nur eine kleine Teilmenge von den im Dokument zum Dateisystemstandard angegebenen Verzeichnissen und

Dateien dar. Die umfassendsten Informationen finden Sie im neuesten Dokument zum Dateisystemstandard FHS.

Das Verzeichnis /dev

Das Verzeichnis `/dev` enthält Dateisystemeinträge, die die an das System angeschlossenen Geräte repräsentieren. Diese Dateien sind für das richtige Funktionieren des Systems unerlässlich.

Das Verzeichnis /etc

Das Verzeichnis `/etc` ist für lokale Konfigurationsdateien reserviert. In `/etc` dürfen keine Binärdateien abgelegt werden. Sämtliche Binärdateien, die zu einem früheren Zeitpunkt in `/etc` abgelegt wurden, müssen jetzt nach `/sbin` oder - wenn möglich - nach `/bin` verschoben werden.

Die Verzeichnisse `X11` und `skel` müssen Unterverzeichnisse von `/etc` sein:

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

Im Verzeichnis `X11` werden X11-Konfigurationsdateien wie `XF86Config` abgelegt. Im Verzeichnis `skel` werden Benutzerdateien-"Gerippe" abgelegt; wenn ein neuer Benutzer erstellt wird, dienen sie dazu, ein Home-Verzeichnis zu füllen.

Das Verzeichnis /lib

Das Verzeichnis `/lib` sollte nur jene Bibliotheken enthalten, die für das Ausführen der Binärdateien in `/bin` und `/sbin` gebraucht werden.

Das Verzeichnis /proc

Das Verzeichnis `/proc` enthält spezielle Dateien, die Informationen mit dem Kernel austauschen. `/proc` ermöglicht es Ihnen, mit Hilfe des Befehls `cat` auf einfache Weise auf Informationen über das Betriebssystem zuzugreifen.

Das Verzeichnis /sbin

Das Verzeichnis `/sbin` enthält ausführbare Dateien, die nur vom Root-Benutzer verwendet werden. Die ausführbaren Dateien im Verzeichnis `/sbin` werden nur dazu verwendet, `/usr` zu booten und zu mounten und Vorgänge zur Systemwiederherstellung auszuführen. Laut Dateisystemstandard FHS gilt:

> "Zusätzlich zu den Binärdateien in `/bin` sind in `/sbin` in der Regel Dateien enthalten, die für den Systemstart notwendig sind. Alle Programme, die nach dem erfolgreichen Mounten von `/usr` ausgeführt werden (falls keine Probleme aufgetreten sind), sollten in `/usr/sbin` abgelegt werden. Binärdateien für die ausschließlich lokale Systemadministration sollten in `/usr/local/sbin` abgelegt werden."

`/sbin` sollte mindestens die folgenden Programme enthalten:

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

Das Verzeichnis `/usr`

Im Verzeichnis `/usr` werden Dateien abgelegt, die allen Benutzern auf einer Site zur Verfügung gestellt werden. Für das Verzeichnis `/usr` wird in der Regel eine eigene Partition angelegt. Es sollte möglich sein, diese Partition schreibgeschützt zu mounten. `/usr` muss die folgenden Unterverzeichnisse enthalten:

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

Das Verzeichnis X11R6 ist für das X Window System gedacht (XFree86 in Red Hat Linux), bin enthält ausführbare Dateien, doc enthält Dokumentation, die nicht in Form von man-Seiten vorliegt, etc enthält Konfigurationsdateien für die gesamte Site, games ist für Spiele reserviert, include enthält C-Header-Dateien, lib enthält Bibliotheken, libexec enthält kleinere Hilfsprogramme, die von anderen Programmen aufgerufen werden, sbin enthält die Binärdateien für die Systemadministration (solche Binärdateien, die nicht zu /sbin gehören), share enthält Dateien, die nicht architekturspezifisch sind und src ist für den Quellcode reserviert.

Das Verzeichnis /usr/local

Laut Dateisystemstandard FHS gilt:

> "Die Hierarchie /usr/local kann vom Systemadministrator für die Installation lokaler Software benutzt werden. Bei der Aktualisierung der System-Software muss ein Überschreiben ausgeschlossen werden. Das Verzeichnis kann für Programme und Daten verwendet werden, auf die innerhalb einer Gruppe von Computern zugegriffen werden kann und die nicht in /usr abgelegt sind."

Das Verzeichnis /usr/local hat eine ähnliche Struktur wie das Verzeichnis /usr. Es enthält die folgenden Unterverzeichnisse, deren Verwendungszweck jeweils dem der Unterverzeichnisse im Verzeichnis /usr ähnlich ist:

```
/usr/local
       |- bin
       |- doc
       |- etc
       |- games
       |- info
       |- lib
       |- man
       |- sbin
       +- src
```

Das Verzeichnis /var

Der Dateisystemstandard FHS erfordert, dass das Mounten von /usr im Read-Only-Modus möglich sein soll. Daher sollten Programme, die Protokolldateien schreiben oder spool- bzw. lock-Verzeichnisse benötigen, am besten in das Verzeichnis /var schreiben. Laut Dateistandardsystem FHS enthält /var:

> "…variable Datendateien. Dazu gehören Spool-Verzeichnisse und Spool-Dateien, Systemverwaltungs- und Protokollierungsdaten sowie zwischengespeicherte Dateien."

`/var` muss die folgenden Unterverzeichnisse enthalten:

```
/var
  |- cache
  |- db
  |- ftp
  |- gdm
  |- lib
  |- local
  |- lock
  |- log
  |- named
  |- nis
  |- opt
  |- preserve
  |- run
  +- spool
       |- anacron
       |- at
       |- cron
       |- fax
       |- lpd
       |- mail
       |- mqueue
       +- news
       |- rwho
       |- samba
       |- slrnpull
       |- squid
       |- up2date
       |- uucp
       |- uucppublic
       |- vbox
       |- voice
  |- tmp
  |- yp
```

Systemprotokolldateien wie `wtmp` und `lastlog` werden im Verzeichnis `/var/log` abgelegt. Das Verzeichnis `/var/lib` enthält auch die RPM-Systemdatenbanken. Sperrdateien werden in `/var/lock` abgelegt. Das Verzeichnis

`/var/spool` enthält Unterverzeichnisse, in denen verschiedene Systeme Datendateien speichern können.

2.1.2 `/usr/local` in Red Hat Linux

Der Verwendungszweck des Verzeichnisses `/usr/local` unterscheidet sich in Red Hat Linux geringfügig von der im Dateisystemstandard FHS definierten Verwendung. Laut Dateistandard soll in `/usr/local` Software abgelegt werden, die bei Aktualisierungen der System-Software geschützt werden soll. Das Aktualisieren von Red Hat mit dem RPM-System und Gnome-RPM ist sicher, was das Überschreiben angeht. Es ist daher nicht nötig, Dateien dadurch zu schützen, dass Sie sie im Verzeichnis `/usr/local` ablegen. Stattdessen wird empfohlen, `/usr/local` für lokal verwendete Software zu nutzen.

Angenommen, Sie haben z.B. `/usr` über NFS schreibgeschützt von *beavis* gemountet. Wenn Sie ein bestimmtes Paket oder Programm installieren möchten, auf *beavis* aber nicht schreibend zugreifen können, sollten Sie es unter `/usr/local` installieren. Falls es Ihnen irgendwann gelingen sollte, den Systemadministrator von *beavis* dazu zu bringen, das Programm auf `/usr` zu installieren, können Sie es von `/usr/local` wieder deinstallieren.

2.2 Spezielle Speicherorte von Dateien bei Red Hat

Neben den Dateien des RPM-Systems, die im Verzeichnis `/var/lib/rpm` abgelegt sind (weitere Informationen zu RPM finden Sie in Kapitel 5, *Paketverwaltung mit RPM*), gibt es zwei weitere spezielle Speicherorte, die für die Konfiguration und den Betrieb von Red Hat Linux reserviert sind.

Das Control Panel und dazugehörige Tools legen in`/usr/lib/rhs` viele Skripten, Bitmaps und Textdateien ab. Es ist unwahrscheinlich, dass Sie in diesem Verzeichnis Dateien bearbeiten müssen.

In `/etc/sysconfig` werden Konfigurationsinformationen gespeichert. Die Dateien in diesem Verzeichnis werden hauptsächlich von den Skripten verwendet, die beim Systemstart ablaufen. Sie können zwar von Hand bearbeitet werden, es ist jedoch empfehlenswert, das entsprechende Tool im Control Panel zu verwenden.

2.3 Benutzer, Gruppen und benutzereigene Gruppen

Die Verwaltung von Benutzern und Gruppen ist schon immer ziemlich mühsam gewesen. Red Hat Linux bietet hier einige Tools und Konventionen, mit denen Sie Benutzer und Gruppen leichter verwalten können.

Am besten lassen sich Benutzer und Gruppen mit linuxconf verwalten (siehe Kapitel 3, *Systemkonfiguration*). Sie können aber auch den Befehl `useradd` verwenden, um von der Befehlszeile aus einen neuen Benutzer zu erstellen.

Als Nächstes wollen wir die grundlegenden Prinzipien bei der Verwaltung von Benutzern und Gruppen näher betrachten.

2.3.1 Standardbenutzer

Tabelle 2–1, *Standardbenutzer* zeigt die Standardbenutzer, die während des Installationsvorgangs eingerichtet werden (entspricht im Prinzip dem Inhalt der Datei `/etc/passwd`). Die **Gruppen-ID** (GID) in der Tabelle gibt die *Hauptgruppe* des Benutzers an. Nähere Einzelheiten über die Verwendung von Gruppen finden Sie in Abschnitt 2.3.3, *Benutzereigene Gruppen*.

Tabelle 2–1 Standardbenutzer

Benutzer	UID	GID	Home-Verzeichnis	Shell
root	0	0	`/root`	`/bin/bash`
bin	1	1	`/bin`	
daemon	2	2	`/sbin`	
adm	3	4	`/var/adm`	
lp	4	7	`/var/spool/lpd`	
sync	5	0	`/sbin`	`/bin/sync`
shutdown	6	0	`/sbin`	`/sbin/shutdown`
halt	7	0	`/sbin`	`/sbin/halt`
mail	8	12	`/var/spool/mail`	

Benutzer	UID	GID	Home-Verzeichnis	Shell
news	9	13	`/var/spool/news`	
uucp	10	14	`/var/spool/uucp`	
operator	11	0	`/root`	
games	12	100	`/usr/games`	
gopher	13	30	`/usr/lib/gopher-data`	
ftp	14	50	`/var/ftp`	
nobody	99	99	`/`	

2.3.2 Standardgruppen

Tabelle 2–2, *Standardgruppen* zeigt die Standardgruppen, die während des Installationsvorgangs eingerichtet werden (entspricht im Prinzip dem Inhalt der Datei `/etc/group`).

Tabelle 2–2 Standardgruppen

Gruppe	GID	Mitglieder
root	0	root
bin	1	root, bin, daemon
daemon	2	root, bin, daemon
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	
disk	6	root
lp	7	daemon, lp
mem	8	

Gruppe	GID	Mitglieder
kmem	9	
wheel	10	root
mail	12	mail
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	
nobody	99	
users	100	

2.3.3 Benutzereigene Gruppen

Red Hat Linux verwendet **benutzereigene Gruppen** (UPG, User Private Groups). Damit wird die Benutzung von Unix-Gruppen wesentlich vereinfacht. UPG bringt keine Zusätze oder Änderungen in Bezug auf die standardmäßige Behandlung von Gruppen unter Unix. Vielmehr wird eine neue Konvention für die Handhabung von Gruppen eingeführt. Bei jedem Erstellen eines neuen Benutzers wird diesem standardmäßig eine eigene Gruppe zugeordnet. Hier das Prinzip:

Benutzereigene Gruppen

Jeder Benutzer hat seine eigene Hauptgruppe, in der er das einzige Mitglied ist.

umask = 002

Die herkömmliche Unix-umask ist 022. Damit wird verhindert, dass andere Benutzer *und andere Mitglieder der Hauptgruppe eines Benutzers* die Dateien eines Benutzers bearbeiten. Bei UPG hat jeder Benutzer seine eigene Gruppe, und daher wird solch ein "Gruppenschutz" nicht mehr benötigt. Damit Benutzer nicht die privaten Dateien anderer Benutzer bearbeiten können, wird in `/etc/profile` die umask auf 002 gesetzt.

setgid-Bit für Verzeichnisse

Wenn Sie das setgid-Bit für ein Verzeichnis setzen (mit `chmod g+s` *`Verzeichnisname`*), werden die in diesem Verzeichnis erstellten Dateien der Gruppe des Verzeichnisses zugeordnet.

Meistens wird in einer EDV-Abteilung für jedes größere Projekt eine Gruppe erstellt, und den entsprechenden Gruppen werden dann die Benutzer zugeordnet. Trotzdem war die Dateiverwaltung oft problematisch, denn wenn ein Benutzer eine Datei erstellt, wird die Hauptgruppe des Erstellers zum Eigentümer dieser Datei. Wenn ein einzelner Benutzer an mehreren Projekten arbeitet, ist es nicht einfach, die mit dem Projekt verbundene Gruppe zum Eigentümer der Dateien zu machen. Bei UPG werden Gruppen entsprechend dem jeweiligen Projekt automatisch mit Dateien verknüpft. Dadurch wird die Verwaltung von Gruppenprojekten sehr einfach.

Angenommen, Sie haben ein großes Projekt namens *entwicklung*, bei dem viele Benutzer die Dateien im Verzeichnis `entwicklung` bearbeiten. Erstellen Sie eine Gruppe mit der Bezeichnung `entwicklung`, fügen Sie das Verzeichnis `entwicklung` (`chgrp entwicklung`) und alle Benutzer des Projekts der Gruppe `entwicklung` hinzu. Jetzt können alle Benutzer des Projekts die Dateien im Verzeichnis `entwicklung` bearbeiten und neue Dateien erstellen. Diese Dateien sind dauerhaft der Gruppe `entwicklung` zugeordnet und können daher jederzeit von anderen Benutzern desselben Projekts bearbeitet werden.

Wenn die Benutzer an mehreren Projekten wie *entwicklung* arbeiten, brauchen sie beim Wechsel zwischen den Projekten ihre umask oder Gruppe nicht zu ändern. Das setgid-Bit im Hauptverzeichnis des jeweiligen Projekts "wählt" die richtige Gruppe.

Da ein Benutzer und seine eigene Gruppe stets Eigentümer des Home-Verzeichnisses dieses Benutzers sind, kann das SGID-Bit ohne Bedenken für das Home-Verzeichnis gesetzt werden. Da aber Dateien bei Ihrer Erstellung standardmäßig der Hauptgruppe des Benutzers zugeordnet werden, ist das SGID-Bit in diesem Fall redundant.

Das Grundprinzip der benutzereigenen Gruppen

Obwohl UPGs nicht ganz neu in Red Hat Linux 7.0 sind, haben viele Benutzer immer noch Fragen zu diesem Thema, z.B. warum UPG überhaupt notwendig ist. Im Folgenden wird das Grundprinzip dargestellt.

- Eine Arbeitsgruppe soll Dateien bearbeiten, z.B. im Verzeichnis `/usr/lib/emacs/site-lisp`. Sie möchten vermeiden, dass bestimmte Mitarbeiter dabei aus Unkenntnis Schaden anrichten.
- Also geben Sie Folgendes ein:

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

  und Sie fügen die richtigen Benutzer der Gruppe hinzu.
- Damit die Benutzer Dateien im Verzeichnis erstellen können, geben Sie Folgendes ein:

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

- Wenn ein Benutzer jedoch eine neue Datei anlegt, wird sie der Standardgruppe des Benutzers zugeordnet (meistens `users`). Um das zu verhindern, geben Sie Folgendes ein:

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

  Daraufhin werden alle in diesem Verzeichnis erstellten Dateien der Gruppe "emacs" zugeordnet.
- Damit andere Benutzer in der Gruppe "emacs" die neue Datei bearbeiten können, muss der Modus 664 eingestellt werden. Setzen Sie dazu die Standard-umask auf 002.
- Das funktioniert so weit ganz gut. Wenn Ihre Standardgruppe "users" ist, kann allerdings jede von Ihnen im Home-Verzeichnis erstellte Datei von jedem Mitglied der Gruppe "users" überschrieben werden (in der Regel also von allen Benutzern).

- Um das zu ändern, ordnen Sie jedem Benutzer eine "benutzereigene Gruppe" als Standardgruppe zu.

An dieser Stelle können Sie durch das Setzen der Standard-umask auf 002 und das Zuordnen von benutzereigenen Standardgruppen zu allen Benutzern auf einfache Art und Weise Gruppen erstellen, die den Benutzern sehr nützlich sein können. Erstellen Sie einfach die Gruppe, fügen Sie die Benutzer hinzu, und wenden Sie die oben genannten Befehle `chown` und `chmod` auf die Gruppenverzeichnisse an.

2.4 Konfigurieren des Zugriffs auf die Konsole

Wenn sich normale Benutzer (nicht Root) an einem Computer lokal anmelden, werden ihnen zwei spezielle Berechtigungen zugeteilt. Zum einen dürfen Sie bestimmte Programme ausführen, die sie normalerweise nicht ausführen können, zum anderen haben sie Zugriff auf bestimmte Dateien (in der Regel spezielle Gerätedateien für den Zugriff auf Disketten und CD-ROMs usw.), auf die sie im Normalfall keinen Zugriff haben.

Da ein einzelner Computer über mehrere Konsolen verfügt und zur selben Zeit mehrere Benutzer lokal am gleichen Computer angemeldet sein können, muss es einen Benutzer geben, der beim Streit um den Dateizugriff "gewinnt". Der erste Benutzer, der sich an der Konsole anmeldet, wird zum Eigentümer dieser Dateien. Wenn sich der erste Benutzer abgemeldet hat, wird der Benutzer, der sich als Nächstes angemeldet hat, zum Eigentümer der Dateien.

Dagegen darf *jeder* Benutzer, der sich an der Konsole anmeldet, Programme ausführen, die normalerweise nur Root vorbehalten sind. Standardmäßig fragen diese Programme nach dem Passwort des Benutzers, und zwar in grafischer Darstellung, wenn X ausgeführt wird. Dadurch ist es möglich, diese Aktionen als Menüeinträge in einer grafischen Benutzeroberfläche zu realisieren. Red Hat Linux wird mit den über die Konsole ausführbaren Programmen `shutdown`, `halt` and `reboot` ausgeliefert.

2.4.1 Deaktivieren des Zugriffs auf Programme über die Konsole

In Umgebungen, in denen die Konsole anderweitig gesichert ist (BIOS- und LILO-Passwörter gesetzt, [Strg]-[Alt]-[Entf] deaktiviert, Netz- und Reset-Schalter deaktiviert usw.), sollte es beliebigen anderen Benutzern der Konsole nicht erlaubt sein, `shutdown`, `halt` und `reboot` auszuführen.

Zum Deaktivieren jeglicher Zugriffe von Konsolenbenutzern auf Konsolenprogramme müssen Sie den folgenden Befehl ausführen:

```
rm -f /etc/security/console.apps/*
```

2.4.2 Deaktivieren aller Zugriffe über die Konsole

Um alle Konsolenzugriffe einschließlich Programm- und Dateizugriffe zu deaktivieren, kommentieren Sie im Verzeichnis `/etc/pam.d/` alle Zeilen aus, die sich auf `pam console.so` beziehen. Das folgende Skript kann Ihnen diese Arbeit abnehmen:

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

2.4.3 Definieren der Konsole

Die Datei `/etc/security/console.perms` definiert die Konsolengruppe. Die Syntax dieser Datei ist sehr flexibel. Die Datei kann bearbeitet werden, um die in ihr enthaltenen Befehle zu verändern. Die Standarddatei enthält jedoch die folgende Zeile:

```
<Konsole>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

Wenn sich die Benutzer anmelden, sind sie mit irgendeinem benannten Terminal verbunden. Das kann entweder ein X-Server mit einem Namen wie `:0` oder `mymachine.example.com:1.0` sein, oder es kann sich um ein Gerät wie `/dev/ttyS0` oder `/dev/pts/2` handeln. In der Standardeinstellung wird definiert, dass nur lokale virtuelle Konsolen und lokale X-Server als lokal angesehen werden. Wenn Sie aber das serielle Terminal an Port `/dev/ttyS1` gleich nebenan ebenfalls als lokales Terminal definieren möchten, können Sie diese Zeile wie folgt ändern:

```
<Konsole>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

2.4.4 Gewähren des Zugriffs auf Dateien über die Konsole

Die Datei `/etc/security/console.perms` enthält einen Abschnitt mit Zeilen wie die Folgende:

```
<Floppy>=/dev/fd[0-1]*
<CD-ROM>=/dev/cdrom
<jaz>=/dev/zip
```

Sie können auch eigene Zeilen hinzufügen:

```
<Scanner>=/dev/sga
```

(Natürlich muss `/dev/sga` tatsächlich Ihr Scanner sein und nicht z.B. Ihr Festplattenlaufwerk.)

So viel zum ersten Teil. Im zweiten Teil müssen Sie definieren, was mit diesen Dateien zu geschehen hat. Suchen Sie im letzten Abschnitt von `/etc/security/console.perms` nach Zeilen wie:

```
<Konsole> 0660 <Floppy> 0660 root.floppy
<Konsole> 0600 <CD-ROM>  0600 root.disk
<Konsole> 0600 <jaz>    0660 root.disk
```

Fügen Sie eine Zeile hinzu:

```
<Konsole> 0600 <Scanner>  0600 root
```

Wenn Sie sich danach an der Konsole anmelden, werden Sie Eigentümer des Geräts `/dev/sga` mit der Zugriffsberechtigung 0600 (Lesen und Schreiben nur durch Sie selbst möglich). Wenn Sie sich abmelden, wird Root zum Eigentümer, und die

Zugriffsberechtigung bleibt weiterhin 0600 (jetzt ist Lesen und Schreiben nur durch Root möglich).

2.4.5 Aktivieren des Zugriffs auf andere Anwendungen über die Konsole

Um Konsolenbenutzern neben `shutdown`, `reboot` und `halt` Zugriff auf weitere Anwendungen zu geben, müssen Sie etwas mehr Aufwand treiben.

Über die Konsole kann *nur* auf Anwendungen zugegriffen werden, die in `/sbin` oder `/usr/sbin` abgelegt sind. Die Anwendung, die Sie ausführen möchten, muss also dort abgelegt sein.

Erstellen Sie einen Link vom Namen Ihrer Anwendung mit der Anwendung `/usr/bin/consolehelper`:

```
cd /usr/bin
ln -s consolehelper foo
```

Erstellen Sie die Datei `/etc/security/console.apps/foo`:

```
touch /etc/security/console.apps/foo
```

Erstellen Sie eine PAM-Konfigurationsdatei für den Dienst *foo* in `/etc/pam.d/`. Es empfiehlt sich, mit einer Kopie des shutdown-Dienstes zu beginnen und diesen dann zu ändern, falls Sie dessen Verhalten ändern möchten:

```
cp /etc/pam.d/shutdown /etc/pam.d/foo
```

Wenn Sie jetzt `/usr/bin/foo` ausführen, wird das Programm `consolehelper` aufgerufen, das wiederum mit Hilfe von `/usr/sbin/userhelper` den Benutzer authentifiziert. (Wenn `/etc/pam.d/foo` eine Kopie von `/etc/pam.d/shutdown` ist, werden Sie nach dem Passwort gefragt. Anderenfalls läuft genau das ab, was in `/etc/pam.d/foo` angegeben ist.) Dann wird `/usr/sbin/foo` mit Root-Zugriffsberechtigung ausgeführt.

2.5 Die Gruppe floppy

Wenn Sie aus irgendeinem Grund keinen Konsolenzugriff haben und Benutzern, die nicht Root sind, Zugriff auf das Diskettenlaufwerk Ihres Systems geben müssen, können Sie die Gruppe `floppy` verwenden. Fügen Sie die Benutzer einfach der Gruppe `floppy` hinzu. Dazu können Sie verschiedene Tools verwenden. Hier ein Beispiel, wie Sie mit `gpasswd` den Benutzer stephan zur Gruppe `floppy` hinzufügen können.

```
[root@bigdog root]# gpasswd -a stephan floppy
Adding user stephan to group floppy
[root@bigdog root]#
```

Jetzt kann der Benutzer stephan auf das Diskettenlaufwerk des Systems zugreifen.

2.6 Benutzerauthentifizierung mit PAM

Programme, die Benutzern Zugriffsrechte jeglicher Art einräumen, müssen die Benutzer authentifizieren können. Wenn Sie sich bei einem System anmelden, geben Sie Ihren Namen und Ihr Passwort an. Der Anmeldeprozess verwendet diese nun, um die Anmeldung zu authentifizieren — d.h., um zu überprüfen, ob Sie auch tatsächlich derjenige sind, für den Sie sich ausgeben. Neben der Verwendung von Passwörtern gibt es auch andere Formen der Authentifizierung. Für die Speicherung von Passwörtern gibt es verschiedene Varianten.

PAM steht für **Pluggable Authentication Modules** (einfügbare Authentifizierungsmodule). Damit kann der Systemadministrator die Authentifizierungsregelungen festlegen, ohne dass die Authentifizierungsprogramme neu kompiliert werden müssen. Bei PAM bearbeiten Sie eine Konfigurationsdatei und bestimmen so, wie die Module in die Programme eingefügt werden.

Die wenigsten Benutzer von Red Hat Linux werden diese Konfigurationsdatei jemals verändern müssen. Wenn Sie mit RPM Programme installieren, die eine Authentifizierung vornehmen müssen, so nehmen diese die für die normale Passwortauthentifizierung notwendigen Änderungen automatisch vor. Wenn Sie jedoch eine benutzerdefinierte Konfiguration vornehmen möchten, müssen Sie den Inhalt der Konfigurationsdatei verstehen.

2.6.1 PAM-Module

Der PAM-Standard definiert vier verschiedene Modultypen.

- auth-Module nehmen die eigentliche Authentifizierung vor (z.B. durch Erfragen und Überprüfen des Passworts) und erstellen "credentials" (Berechtigungsmerkmale), z.B. die Mitgliedschaft in einer Gruppe oder Kerberos-"tickets".
- account-Module prüfen, ob die Authentifizierung erlaubt ist (der Account darf nicht abgelaufen sein, der Benutzer muss für die Anmeldung um diese Uhrzeit zugelassen sein usw.).
- password-Module dienen zum Setzen von Passwörtern.
- session-Module sorgen dafür, dass ein Benutzer nach seiner Authentifizierung seinen Account benutzen kann, z.B. durch das Mounten des Home-Verzeichnisses des Benutzers oder durch Aktivierung der Mailbox.

Diese Module können *gestapelt* werden, so dass mehrere Module verwendet werden können. Zum Beispiel verwendet rlogin in der Regel mindestens zwei Authentifizierungsmethoden: Wenn die rhosts-Authentifizierung erfolgreich ist, kann die Verbindung sofort zugelassen werden. Wenn die Authentifizierung nicht erfolgreich ist, wird zur Standardauthentifizierung mit Passwort übergegangen.

Es können jederzeit neue Module hinzugefügt werden. PAM-kompatible Anwendungen können dann so angepasst werden, dass auf diese Module zugegriffen werden kann. Falls Sie z.B. über ein Rechensystem für Einmal-Passwörter verfügen und festlegen können, dass es von einem bestimmten Modul unterstützt werden soll (weitere Informationen zum Schreiben von Modulen finden Sie im System unter /usr/share/doc/pam*), sind PAM-kompatible Programme in der Lage, das neue Modul zu verwenden und mit dem neuen Rechensystem für Einmal-Passwörter zu arbeiten, ohne dass es neu kompiliert oder anderweitig modifiziert werden müsste.

2.6.2 Dienste

Jedes Programm, das PAM verwendet, definiert seinen eigenen "Dienste"-Namen. Das Programm login definiert den Dienstetyp login, ftpd definiert den Dienstetyp ftp usw. Generell ist der Dienstetyp der Name des Programms, das zum *Zugriff* auf den Dienst verwendet wird, und nicht das Programm, das den Dienst *bereitstellt* (falls es diese Unterscheidung gibt).

2.6.3 Die Konfigurationsdateien

Alle PAM-Anwendungen werden im Verzeichnis `/etc/pam.d` konfiguriert. (In früheren PAM-Versionen wurde dafür die Datei `/etc/pam.conf` verwendet. Wenn das Programm keinen Eintrag in `/etc/pam.d/` findet, wird die Datei `pam.conf` eingelesen. Sie sollte aber nicht mehr verwendet werden.) Jede Anwendung (genau genommen jeder *Dienst*) hat eine eigene Datei, die wie folgt aussieht:

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

Die erste Zeile ist ein Kommentar. (Kommentarzeilen beginnen immer mit dem Zeichen `#`.) Die Zeilen zwei bis vier stapeln drei Module für die Anmeldeautorisierung. *Wenn* der Benutzer sich als Root anzumelden versucht, stellt Zeile zwei sicher, dass das Terminal, an dem er sich anmeldet, in der Datei `/etc/securetty` aufgeführt ist, *falls* solch eine Datei existiert. Zeile drei sorgt dafür, dass der Benutzer nach dem Passwort gefragt wird und dass dieses überprüft wird. Zeile vier prüft, ob die Datei `/etc/nologin` existiert. Falls ja, wird der Inhalt der Datei auf dem Bildschirm angezeigt und eine Anmeldung des Benutzers verhindert, es sei denn, er ist Root.

Beachten Sie, dass alle drei Module überprüft werden, *auch wenn schon beim ersten Modul Fehler auftreten*. Hierbei handelt es sich um eine Sicherheitsfunktion — sie wurde entwickelt, um zu verhindern, dass Benutzer erfahren, weshalb ihre Authentifizierung nicht zugelassen wurde. Der Grund dafür ist: Wenn ein Benutzer weiß, weshalb seine Authentifizierung abgelehnt wurde, ist es für ihn einfacher, die Authentifizierung zu knacken. Sie können diese Einstellung ändern, indem Sie statt required requisite eintragen. Wenn ein requisite-Modul eine Fehlermeldung liefert, bricht PAM sofort ab, ohne weitere Module aufzurufen.

Die fünfte Zeile veranlasst die Prüfung des Benutzeraccounts. Wenn z.B. Shadow-Passwörter aktiviert worden sind, überprüft das Modul `pam_unix.so`, ob der Account abgelaufen ist oder ob der Benutzer keine Passwortänderung vorgenommen hat und die Nachfrist für eine Änderung abgelaufen ist.

Die sechste Zeile unterzieht das gerade geänderte Passwort einer Reihe von Prüfungen, um sicherzustellen, dass es z.B. nicht auf einfache Weise durch ein wörterbuchbasiertes Tool zum Knacken von Passwörtern herausgefunden werden kann.

Die siebte Zeile (evtl. umgebrochen) gibt an, dass das Programm login bei einer Änderung des Passworts hierfür das Modul `pam_unix.so` verwenden soll. (Zu einer Änderung des Passwortes kommt es nur dann, wenn ein `auth`-Modul festgelegt hat, dass das Passwort geändert werden muss — wenn z.B. ein Shadow-Passwort abgelaufen ist.)

Die achte und letzte Zeile gibt an, dass das Modul `pam_unix.so` für die Verwaltung der Sitzung verwendet werden soll. Gegenwärtig hat dieses Modul keine Funktion. Es kann durch ein beliebiges notwendiges Modul ersetzt (oder durch Stapeln ergänzt) werden.

Beachten Sie, dass die Reihenfolge der Zeilen in diesen Dateien wichtig ist. Während die Reihenfolge beim Aufrufen von required-Modulen keine große Rolle spielt, ist dies bei den anderen verfügbaren *Steuer-Flags* sehr wohl der Fall. Das Flag optional wird nur selten verwendet (bei Red Hat Linux Systemen niemals standardmäßig). Bei sufficient und requisite ist die Reihenfolge wichtig.

Hier ein Blick auf die `auth`-Konfigurationsdatei für `rlogin`:

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

Erstens meldet PAM (sobald `pam_rhosts_auth.so` den Benutzer authentifiziert) unverzüglich die erfolgreiche Ausführung an `rlogin`, ohne das Passwort zu überprüfen. Eine gescheiterte Authentifizierung des Benutzers durch `pam_rhosts_auth.so` wird ignoriert.

Zweitens verhindert `pam_securetty.so`, dass Root-Anmeldungen auf unsicheren Terminals vorgenommen werden können. Damit werden praktisch alle Root-Anmeldungen über `rlogin` verhindert. Entfernen Sie diese Zeile, falls Sie entsprechende Anmeldungen zulassen möchten (nur empfehlenswert, wenn entweder keine Verbindung zum Internet besteht oder eine gute Firewall vorhanden ist).

Drittens (falls `pam_rhosts_auth.so` den Benutzer nicht authentifizieren konnte) führt das Modul `pam_stack.so` eine normale Passwortauthentifizierung durch.

Schließlich prüft `pam_nologin.so` `/etc/nologin` wie oben beschrieben.

Beachten Sie: Wenn nach einem negativen Ausgang der securetty-Überprüfung nicht nach dem Passwort gefragt werden soll, ändern Sie das Modul `pam_securetty.so` von required in requisite.

2.6.4 Shadow-Passwörter

Das Modul `pam_unix.so` erkennt automatisch, dass Sie Shadow-Passwörter verwenden und nimmt alle notwendigen Anpassungen vor. Weitere Informationen finden Sie in Abschnitt 2.7, *Shadow-Dienstprogramme*.

2.6.5 Rexec und PAM

Aus Sicherheitsgründen ist in Red Hat Linux 7.0 rexec nicht aktiviert. Wenn Sie rexec aktivieren möchten, müssen Sie die Kommentarzeichen am Beginn einer Zeile in der Datei `/etc/pam.d/rexec` entfernen. Hier eine Beispieldatei (beachten Sie, dass Ihre Datei etwas anders aussehen kann):

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

Um rexec zu aktivieren, müssen Sie die Kommentarzeichen in der Zeile entfernen, die auf das Modul `pam_nologin.so` verweist.

```
#%PAM-1.0
auth       required     /lib/security/pam_securetty.so
```

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

Wenn Sie die Datei wie beschrieben bearbeitet haben, ist rexec aktiviert.

Bitte beachten

Wenn die Datei `/etc/pam.d/rexec` eine Zeile enthält, die auf das Modul `pam_securetty.so` verweist, können Sie `rexec` als Root nicht ausführen. Wenn das jedoch möglich sein soll, müssen Sie die Kommentarzeichen in der Zeile entfernen, die auf das Modul `pam_securetty.so` verweist.

Bitte beachten

Die meisten Konfigurationsdateien wurden neu geschrieben, um das Vornehmen von systemweiten Änderungen zu vereinfachen. Auf diese Weise müssen erforderliche Konfigurationsänderungen nur noch an einer Stelle im System vorgenommen werden. Zu dieser Änderung kommt es, weil die Datei `pam_stack` es ermöglicht, einen bestimmten Dienst aus dem Stapel heraus aufzurufen, während der Stapel für einen anderen Dienst definiert ist. Weitere Informationen finden Sie in der man-Seite `pam_stack`.

Weitere Informationen

Bei diesem Abschnitt handelt es sich lediglich um eine Einführung in PAM. Weiterführende Informationen finden Sie im Verzeichnis `/usr/share/doc/pam*`, das den *System Administrators' Guide* (Leitfaden für den Systemadministrator), das

Module Writers' Manual (Handbuch für Modulentwickler), das *Application Developers' Manual* (Handbuch für den Anwendungsentwickler) und den PAM-Standard DCE-RFC 86.0 enthält.

2.7 Shadow-Dienstprogramme

Shadow-Passwörter erhöhen die Systemsicherheit dadurch, dass die verschlüsselten Passwörter (normalerweise im Verzeichnis `/etc/passwd` abgelegt) im Verzeichnis `/etc/shadow` abgelegt werden, das nur von Root gelesen werden kann. Während der Installation von Red Hat Linux konnten Sie wählen, ob der Shadow-Passwortschutz aktiviert werden soll.

Das Paket `shadow-utils` enthält eine Reihe von Dienstprogrammen, die Folgendes unterstützen:

- Konvertierung von normalen Passwörtern in Shadow-Passwörter und umgekehrt (`pwconv`, `pwunconv`)
- Überprüfung von Passwort, Gruppe und zugehörigen Shadow-Dateien (`pwck`, `grpck`)
- Methoden gemäß Industriestandard zum Hinzufügen, Löschen und Bearbeiten von Benutzerkonten (`useradd`, `usermod` und `userdel`)
- Methoden gemäß Industriestandard zum Hinzufügen, Löschen und Bearbeiten von Benutzergruppen (`groupadd`, `groupmod` und `groupdel`)
- Methoden gemäß Industriestandard zum Verwalten der Datei `/etc/group` (`gpasswd`).

Bitte beachten

Hier noch weitere wichtige Hinweise zu diesen Dienstprogrammen:

- Die Dienstprogramme funktionieren unabhängig davon, ob Shadowing aktiviert oder deaktiviert ist.
- Die Dienstprogramme wurden geringfügig modifiziert, um die Unterstützung der individuellen Benutzergruppen von Red Hat zu ermöglichen. Eine Beschreibung der Änderungen finden Sie in der man-Seite `useradd`. Weitere Informationen zu benutzereigenen Gruppen finden Sie in Abschnitt 2.3.3, *Benutzereigene Gruppen*.
- Das Skript `adduser` ist durch einen symbolischen Verweis auf `/usr/sbin/useradd` ersetzt worden.
- Die Tools im Paket `shadow-utils` sind weder für Kerberos noch für LDAP aktiviert. Neue Benutzer sind daher nur lokale Benutzer.

2.8 Erstellen eines benutzerdefinierten Kernels

Linux-Neulinge stellen häufig die Frage: "Warum soll ich einen eigenen Kernel generieren?" Angesichts der Fortschritte, die beim Einsatz von Kernel-Modulen gemacht worden sind, kann die Antwort auf diese Frage nur sein: "Wenn Sie nicht genau wissen, warum Sie einen eigenen Kernel generieren sollen, brauchen Sie wahrscheinlich auch keinen eigenen Kernel." Wenn Sie also keinen speziellen Grund haben, einen benutzerdefinierten Kernel zu generieren (es sei denn, Sie gehören zu den neugierigen Menschen), können Sie getrost zu Abschnitt 2.9, *Sendmail* weiterblättern.

Früher war es notwendig, den Kernel neu zu kompilieren, wenn Sie Ihrem System neue Hardware hinzufügen wollten. Anders ausgedrückt: der Kernel war **statisch**. Durch Verbesserungen an den Kerneln von Linux 2.0.*x* war es möglich, viele der Hardware-Treiber zu Komponenten zu **modularisieren**, die nur bei Bedarf eingefügt werden konnten. Es traten jedoch erhebliche Probleme auf, wenn mehrere Kernel im System vorhanden waren, die für unterschiedliche Versionen kompiliert worden waren (beispielsweise SMP- im Gegensatz zu UP-Kerneln). Weitere Fortschritte bei der Modularisierung des Linux 2.2.x-Kernel ermöglichen jetzt eine bessere Verträglichkeit bei der Verwendung mehrerer Kernel (das gilt jedoch *nicht* für den gemeinsamen Zugriff auf Module).

Informationen zur Handhabung von Kernel-Modulen finden Sie in Abschnitt 3.2.2, *Laden von Kernelmodulen*. Die meisten Änderungen sind nur beim Neukompilieren eines angepassten Kernels sichtbar.

2.8.1 Erstellen eines modularen Kernels

Diese Anweisungen vermitteln Ihnen die nötigen Kenntnisse für die Nutzung der Leistungsfähigkeit und Flexibilität, die aus der Kernel-Modularisierung resultieren. Falls Sie keine Kernel-Modularisierung verwenden möchten, finden Sie in Abschnitt 2.8.3, *Erstellen eines monolithischen Kernels* Erläuterungen zu den verschiedenen Gesichtspunkten der Erstellung und Installation eines monolithischen Kernels. Wir gehen davon aus, dass Sie die Pakete `kernel-headers` und `kernel-source` bereits installiert haben und dass das Verzeichnis `/usr/src/linux` das aktuelle Verzeichnis ist.

Stellen Sie unbedingt sicher, dass Sie über eine funktionierende Notfall-Bootdiskette verfügen, falls etwas schief geht. Wenn Sie während der Installation keine Bootdiskette erstellt haben, holen Sie dies jetzt mit dem Befehl `mkbootdisk` nach. Der Standardbefehl lautet ähnlich wie `mkbootdisk --device /dev/fd0 2.2.x`, wobei 2.2.x für die vollständige Version Ihres Kernels steht (z.B. 2.2.14-5.0). Wenn Sie fertig sind, überprüfen Sie die Bootdiskette, um sicherzugehen, dass Sie damit das System booten können.

Zu Beginn der Erstellung eines Kernels ist es wichtig, dass sich der Quellcodebaum in einem bekannten Zustand befindet. Es wird deshalb empfohlen, zuerst den Befehl `make mrproper` anzuwenden. Dieser Befehl entfernt alle Konfigurationsdateien einschließlich der Reste früherer Builds, deren Dateien möglicherweise im Quellcodebaum verstreut sind. Als Nächstes müssen Sie eine Konfigurationsdatei erstellen, die festlegt, welche Komponenten Ihr neuer Kernel enthalten soll. Folgende Methoden zur Kernelkonfiguration stehen zur Verfügung:

- `make config` — Ein interaktives Textprogramm. Es werden Ihnen Komponenten angeboten, und Sie wählen **Y** (Ja), **N** (Nein) oder **M** (Modul).
- `make menuconfig` — Ein grafisches, menügesteuertes Programm. In einem Menü mit verschiedenen Kategorien werden Ihnen Komponenten angeboten. Sie wählen die gewünschten Komponenten auf die gleiche Weise wie im Red Hat Linux Installationsprogramm aus. Markieren Sie die einzubindenden Komponenten mit **Y** (Ja), **N** (Nein) oder **M** (Modul).
- `make xconfig` — ein X Window System-Programm. Die Komponenten sind in verschiedenen Menüebenen angeordnet und können mit der Maus ausgewählt werden. Wählen Sie auch hier zwischen **Y** (Ja), **N** (Nein) oder **M** (Modul).
- `make oldconfig` — Hierbei handelt es sich um ein nicht-interaktives Skript, das die Einstellungen in der Datei Makefile als Standardeinstellungen einrichtet. Wenn Sie den von Red Hat gepatchten Kernel verwenden, wird Ihr System für den Kernel konfiguriert, der in Ihrem Software-Paket mitgeliefert wird. Dies ist sinnvoll, da auf diese Weise der Kernel mit bekannten, funktionierenden Standardeinstellungen konfiguriert werden kann. Anschließend können Sie Funktionsmerkmale deaktivieren, die Sie nicht benötigen.

Bitte beachten

Um `kmod` (Einzelheiten siehe Abschnitt 3.2.2, *Laden von Kernelmodulen*) und Kernel-Module verwenden zu können, müssen Sie bei der Konfiguration bei `kmod support` und `module version (CONFIG_MODVERSIONS) support` mit **Ja** antworten.

Wenn Sie einen Kernel mit einer Konfigurationsdatei erstellen möchten, (`/usr/src/linux/.config` — diese Datei wird erstellt, sobald eine der oben genannten Methoden ausgeführt wurde), die Sie bereits mit einer der erwähnten Methoden erzeugt haben, können Sie die Befehle `make mrproper` und `make config` auslassen und stattdessen den Befehl `make dep`, gefolgt von `make clean` verwenden, um den Quellcodebaum für den Build vorzubereiten.

Der nächste Schritt zur Erstellung eines modularisierten Kernels ist das Bearbeiten der Datei `/usr/src/linux/Makefile` und das Kompilieren die Quellcodekomponenten zu einem lauffähigen Programm, mit dem Ihr Computer gebootet werden kann. Mit der hier beschriebenen Methode können Sie am problemlosesten wieder in den Ausgangszustand zurückkehren, falls etwas schief gehen sollte. Falls Sie sich für weitere Möglichkeiten interessieren, finden Sie nähere Informationen hierzu im Kernel-HOWTO oder in Ihrem Linux-System in der Datei `Makefile` unter `/usr/src/linux`.

- Bearbeiten Sie die Datei `Makefile`, und ändern Sie die Zeile: `EXTRAVERSION =` in eine "eindeutige" Bezeichnung (zum Beispiel durch Anfügen Ihrer Initialen an das Ende der Zeichenkette, wie in `EXTRAVERSION = -2.5.0sjs`). Dadurch können der alte und der neue Kernel gleichzeitig auf Ihrem System verwendet werden.
- Erstellen Sie den Kernel mit `make bzImage`.
- Erstellen Sie die von Ihnen konfigurierten Module mit `make modules`.
- Installieren Sie die neuen Module (auch, wenn Sie selbst keine Module erstellt haben) mit `make modules_install`. Dadurch werden die Kernel-Module im Verzeichnis `/lib/modules/` unter Verwendung des in `Makefile` angegebenen Pfadnamens gespeichert. In unserem Beispiel wäre das `/lib/modules/2.2.15-2.5.0sjs/`.

Falls Sie einen SCSI-Adapter verwenden und den SCSI-Treiber modularisiert haben, erstellen Sie ein neues `initrd`-Image (siehe Abschnitt 2.8.2, *Erstellen eines initrd-Images*. Beachten Sie aber, dass es kaum praktische Gründe gibt, in einem benutzerdefinierten Kernel den SCSI-Treiber zu modularisieren). Erzeugen Sie kein `initrd`-Image, es sei denn, Sie haben einen spezifischen Grund dafür. Verzichten Sie ansonsten darauf, und fügen Sie ein solches Image auch niemals zu `lilo.conf` hinzu.

Es empfiehlt sich, den ursprünglichen Kernel aufzubewahren. So können Sie zum Booten jederzeit auf einen zusätzlichen, funktionierenden Kernel zurückgreifen, falls der neu erstellte Kernel Fehler enthalten sollte. Zum Hinzufügen des Kernels zu LILO benennen Sie den ursprünglichen Kernel in `/boot` um, kopieren den neuen Kernel nach `/boot`, fügen einige Zeilen in `/etc/lilo.conf` ein und führen

`/sbin/lilo` aus. Hier ein Beispiel für eine mögliche standardmäßige Datei `/etc/lilo.conf`, wie sie im Lieferumfang von Red Hat Linux enthalten ist:

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

image=/boot/vmlinuz-2.2.16-12
        label=linux
        initrd=/boot/initrd-2.2.16-12.img
        read-only
        root=/dev/hda8

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

Als Nächstes müssen Sie `/etc/lilo.conf` aktualisieren. Wenn Sie ein neues `initrd` -Image erstellt haben, müssen Sie LILO zuvor die Anweisung geben, das neue Image zu verwenden. Im folgenden Beispiel zu `/etc/lilo.conf` wurden in der Mitte der Datei vier Zeilen eingefügt, die bewirken, dass ein anderer Kernel beim Booten verwendet wird. Dazu wurde `/boot/vmlinuz` in `/boot/vmlinuz.old` umbenannt und das Label auf `old` gesetzt. Außerdem wurde eine `initrd`-Zeile für den neuen Kernel eingefügt:

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

image=/boot/vmlinuz-2.2.16-12
        label=linux
        initrd=/boot/initrd-2.2.16-12.img
        read-only
        root=/dev/hda8
```

```
image=/boot/vmlinuz-2.2.16-12.sjs
        label=test
        initrd=/boot/initrd-2.2.16-12sjs.img
        read-only
        root=/dev/hda8

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

Wenn das System jetzt gestartet wird und Sie am Prompt LILO `boot:` die [Tabulatortaste] drücken, werden Ihnen die verfügbaren Auswahlmöglichkeiten angezeigt:

```
LILO boot:
linux  test  dos
```

Drücken Sie die [Eingabetaste], um mit dem alten Kernel (**`linux`**) zu booten. Wenn Sie keine Taste drücken, lädt LILO den alten Kernel nach einer Zeitverzögerung automatisch. Wenn Sie mit dem neuen Kernel (**`test`**) booten wollen, geben Sie **`test`** ein und drücken die [Eingabetaste].

Es folgt eine Zusammenfassung der Schritte:

- Kopieren Sie den kompilierten Kernel in Ihr Verzeichnis `/boot`. Verwenden Sie dabei den Namen, der sich aus früheren Änderungen der Datei `Makefile` ergab. Dazu ein Beispiel:

  ```
  cp -p
  /usr/src/linux/arch/i386/boot/bzImage
  /boot/vmlinuz-2.2.15-2.5.0sjs
  /usr/src/linux/System.map  /boot/System.map-2.2.15-2.5.0sjs
  ```

- Bearbeiten Sie die Datei `/etc/lilo.conf`.
- Erstellen Sie bei Bedarf eine neue initiale Ramdisk, `initrd`-Image (siehe Abschnitt 2.8.2, *Erstellen eines initrd-Images*).
- Führen Sie `/sbin/lilo` aus (es empfiehlt sich, `/sbin/lilo -t` zuerst zu verwenden — dieser Befehl testet Ihre `lilo.conf`-Datei, ohne einen neuen Boot-Sektor oder eine Map-Datei zu schreiben). Sie können die Option `-v` zu

`lilo` hinzufügen, um ausführlichere Meldungen anzeigen zu lassen, wenn Sie glauben, es könnte Probleme geben.

Sie können den neuen Kernel testen, indem Sie Ihren Computer neu starten und die Meldungen am Bildschirm verfolgen. Dabei wird angezeigt, ob die Hardware richtig erkannt wird.

2.8.2 Erstellen eines initrd-Images

Beim Booten wird ein `initrd`-Image für das Laden der SCSI-Module benötigt. Wenn Sie kein `initrd` -Image benötigen, erstellen Sie keines, und bearbeiten Sie auch nicht die Datei `lilo.conf`, um dieses Image einzufügen.

Das Shell-Skript `/sbin/mkinitrd` kann das richtige `initrd`-Image für Ihren Computer erstellen, wenn die folgenden Bedingungen erfüllt sind:

- Das Loopback-Blockgerät ist verfügbar.
- Die Datei `/etc/conf.modules` enthält eine Zeile für Ihren SCSI-Adapter, zum Beispiel:

```
alias scsi_hostadapter BusLogic
```

Um das neue `initrd`-Image zu erstellen, führen Sie `/sbin/mkinitrd` mit den folgenden Parametern aus:

```
/sbin/mkinitrd /boot/newinitrd-image 2.2.15-2.5.0sjs
```

Dabei ist `/boot/newinitrd-image` die Datei für Ihr neues Image, und `2.2.15` ist der Kernel, dessen Module (aus `/lib/modules`) im `initrd`-Image verwendet werden sollen. (Die Versionsnummer dieses Kernels stimmt nicht notwendigerweise mit der Versionsnummer des aktuell verwendeten Kernels überein.)

2.8.3 Erstellen eines monolithischen Kernels

Um einen monolithischen Kernel zu erstellen, führen Sie - von ein paar Ausnahmen abgesehen - dieselben Schritte aus wie beim Erstellen eines modularen Kernels.

- Antworten Sie auf die Fragen bei der Konfiguration des Kernels ausschließlich mit **`Ja`** oder **`Nein`** (keine Modularisierung). Außerdem müssen Sie bei der Konfiguration bei `kmod support` und `module version (CONFIG_MODVERSIONS) support` mit **`Nein`** antworten.
- Lassen Sie die folgenden Schritte aus:

```
make modules
make modules_install
```

- Bearbeiten Sie die Datei `lilo.conf`, und fügen Sie die Zeile `append=nomodules` hinzu.

2.9 Sendmail

Im Verzeichnis `/etc` wird die Standarddatei `sendmail.cf` installiert. Die Standardkonfiguration ist für die meisten Systeme geeignet, die ausschließlich SMTP (Simple Mail Transfer Protocol) verwenden. Sie arbeitet *nicht* mit UUCP-Sites (UNIX/UNIX Copy). Wenn für Ihre E-Mail-Übertragungen UUCP erforderlich ist, müssen Sie eine neue Datei `sendmail.cf` erstellen.

Bitte beachten

Obwohl SMTP-Server automatisch unterstützt werden, gilt dies nicht für **IMAP** (Internet Message Access Protocol)-Server. Wenn Ihr ISP statt eines SMTP-Servers einen IMAP-Server verwendet, müssen Sie das Paket IMAP installieren. Ohne dieses Paket kann Ihr System keine Informationen an den IMAP-Server weitergeben bzw. Ihre E-Mail nicht abrufen.

Um eine neue Datei `sendmail.cf` zu erstellen, müssen Sie `m4` und das Quellcodepaket `sendmail` installieren. Nähere Einzelheiten zum Erstellen von sendmail-Konfigurationsdateien finden Sie in der Datei `README` in den sendmail-Quellen. Daneben gibt es eine gute sendmail -Referenz unter dem Titel *sendmail* von Bryan Costales, herausgegeben von O'Reilly & Associates. Und zuletzt finden Sie außerdem unter www.sendmail.net ein breites Angebot an sendmail-Funktionen und Konfigurationsbeispielen.

Häufig ist sendmail so konfiguriert, dass ein Computer als E-Mail-Gateway für alle Computer eines Netzwerks dient. Red Hat verwendet beispielsweise einen einzelnen Computer mit der Adresse `mail.redhat.com`, der die gesamten E-Mails verarbeitet. Die Namen der Computer, für die mail.redhat.com die E-Mail verwaltet, brauchen auf diesem Computer nur in die Datei `/etc/sendmail.cw` eingetragen zu werden. Dazu ein Beispiel:

```
# sendmail.cw - Tragen Sie hier alle Aliase für Ihren Rechner
# ein.
torgo.redhat.com
poodle.redhat.com
devel.redhat.com
```

Auf den anderen Computern `torgo`, `poodle` und `devel` muss die Datei `/etc/sendmail.cf` bearbeitet werden. Beim Senden von E-Mails geben sich diese Computer als `mail.redhat.com` aus. Die lokale E-Mail-Verarbeitung wird an `redhat.com` weitergeleitet. Suchen Sie die Zeilen `DH` und `DM` in `/etc/sendmail.cf`, und bearbeiten Sie diese wie folgt:

```
# An wen erfolgt die Sendung bei Rechnernamen ohne Angabe der Domäne?
# (kein Eintrag = lokal)
DRmail.redhat.com

# An welchen Computer gehen lokale E-Mails?
DHmail.redhat.com

# Wer gebe ich vor zu sein? (Masquerading) (kein Eintrag = kein Masquerading)
DMredhat.com
```

Bei dieser Konfiguration tragen alle E-Mails den Absender `redhat.com`, und alle E-Mails, die an `torgo.redhat.com` oder die anderen Rechner gesendet werden, kommen bei `mail.redhat.com` an.

Wenn Sie Ihr System für Masquerading konfigurieren, beachten Sie bitte, dass die von Ihrem System an Ihr eigenes System gesendeten E-Mails auf dem Computer eingehen, für den sich Ihr System ausgibt. So werden im Bild oben beispielsweise die in regelmäßigen Abständen vom `cron`-Dämon an root@poodle.redhat.com gesendeten Protokolldateien an root@mail.redhat.com gesendet.

2.10 Zugriffskontrolle auf Dienste

Es ist von größter Wichtigkeit, Ihr Red Hat Linux-System gegen unberechtigte Eingriffe zu sichern. Eine Möglichkeit, die Sicherheit in Ihrem System zu gewährleisten, besteht darin, den Zugriff auf die verschiedenen Systemdienste sorgfältig zu verwalten. Möglicherweise ist es erforderlich, dass Ihr System den freien Zugriff auf bestimmte Dienste (z.B. `httpd`, falls Sie mit einem Webserver arbeiten) zulässt. Dienste, die Sie nicht zur Verfügung stellen müssen, sollten Sie dagegen ausschalten — auf diese Weise minimiert sich das Risiko, dass Bugs für Angriffe auf Ihr System genutzt werden.

Es gibt verschiedene Methoden, um den Zugriff auf Systemdienste zu verwalten. Für welche Methode Sie sich entscheiden, hängt von dem jeweiligen Dienst, Ihrer Systemkonfiguration und Ihrer Erfahrung mit Linux ab.

Am einfachsten verweigern Sie den Zugriff auf einen Dienst, indem Sie den Dienst ausschalten. Die von `xinetd` verwalteten Dienste (an späterer Stelle in diesem Abschnitt beschrieben) als auch die Dienste in der `/etc/rc.d`-Hierarchie können dafür konfiguriert werden, entweder mit Hilfe des Dienstprogramms ntsysv oder unter Verwendung von `chkconfig` zu starten und zu stoppen. Wahrscheinlich wird Ihnen die Verwendung dieser Tools im Vergleich zu den zur Verfügung stehenden folgenden Alternativen leichter fallen — manuelles Bearbeiten der zahlreichen symbolischen Links, die sich in den Verzeichnissen unter `/etc/rc.d` befinden, oder Bearbeiten der `xinetd`-Konfigurationsdateien in `/etc/xinetd.d`.

ntsysv stellt eine einfache Schnittstelle zum Aktivieren und Deaktivieren von Diensten zur Verfügung. Sie können ntsysv dazu verwenden, um einen von `xinetd` verwalteten Dienst ein- oder auszuschalten. Außerdem können Sie mit ntsysv einen Dienst in der `/etc/rc.d`-Hierarchie starten oder stoppen. In diesem Fall wird das aktuelle Runlevel durch den (optionslosen) Befehl `ntsysv` konfiguriert. Falls Sie ein anderes Runlevel konfigurieren möchten, müssen Sie den entsprechenden Befehl dazu eingeben, z.B.: `ntsysv --levels 016`. (In diesem Beispiel stellen Sie die Dienste für die Runlevel 0, 1 und 6 ein.)

Die ntsysv-Schnittstelle funktioniert wie das Installationsprogramm im Textmodus. Verwenden Sie die Nach-oben- und die Nach-unten-Tasten, um in der Liste nach oben und nach unten zu blättern. Mit der Leertaste können Sie die einzelnen Dienste auswählen/abwählen und die Buttons **Ok** und **Abbrechen** "betätigen". Um zwischen der Liste mit den Diensten und den Buttons **Ok** und **Abbrechen** zu wechseln, drücken Sie die [Tabulatortaste]. Ein ***** zeigt an, dass ein Dienst eingeschaltet ist. Durch Drücken der Taste [F1] wird eine kurze Beschreibung zu jedem Dienst eingeblendet.

`chkconfig` kann ebenfalls zum Aktivieren und Deaktivieren von Diensten verwendet werden. Wenn Sie den Befehl `chkconfig --list` verwenden, wird Ihnen eine Liste mit Systemdiensten angezeigt und die Information, ob sie in den Runlevels 0-6 gestartet (`eingeschaltet`) oder gestoppt (`ausgeschaltet`) wurden (am Ende der Liste erscheint ein Abschnitt für die von `xinetd` verwalteten Dienste, die an einer späteren Stelle in diesem Abschnitt beschrieben werden).

Außerdem können Sie mit `chkconfig` feststellen, ob ein bestimmter Dienst ausgeführt wird. Der folgende Befehl überprüft z.B. den Dämon `finger`:

```
$ chkconfig --list finger
finger          on
```

Wie oben gezeigt, ist `finger` im aktuellen Runlevel eingeschaltet.

Wenn Sie `chkconfig --list` verwenden, um einen Dienst in `/etc/rc.d` abzufragen, werden Ihnen die Einstellungen des Dienstes für jedes Runlevel angezeigt. Zum Beispiel:

```
$ /sbin/chkconfig --list anacron
anacron         0:off   1:off   2:on    3:on
4:on    5:on    6:off
```

Doch was noch wichtiger ist: Mit `chkconfig` können Sie einstellen, ob ein Dienst in einem bestimmten Runlevel gestartet werden soll oder nicht. Wenn z.B. `nscd` in den Runlevels 3, 4 und 5 ausgeschaltet werden soll, verwenden Sie den Befehl:

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

Weitere Informationen darüber, wie Sie `chkconfig` verwenden können, finden Sie in der entsprechenden man-Seite.

`xinetd` ist eine weitere Möglichkeit, um den Zugriff auf Internet-Dienste zu kontrollieren, und stellt eine sichere Alternative zu `inetd` dar. `xinetd` erhält die Systemressourcen, bietet Zugriffskontrolle und Anmeldefunktionen und kann dazu verwendet werden, Server zu starten, die einem speziellen Zweck dienen. `xinetd` kann dazu verwendet werden, den Zugriff nur auf bestimmte Hosts zu gewähren, den Zugriff auf bestimmte Hosts zu verweigern, den Zugriff auf nur einen Dienst und nur zu einer bestimmten Zeit zuzulassen, die Zahl der eingehenden Verbindungen und/oder die durch die Verbindungen erzeugte Auslastung zu begrenzen etc.

`xinetd` wird konstant ausgeführt und fragt alle Ports der von ihm verwalteten Dienste ab. Sobald für einen der von ihm verwalteten Dienste eine Verbindungsanforderung eingeht, startet `xinetd` den für diesen Dienst geeigneten Server.

Die Konfigurationsdatei für `xinetd` ist `/etc/xinetd.conf`; doch wenn Sie die Datei überprüfen, werden Sie feststellen, dass sie nur einige wenige Standardeinstellungen und eine Anweisung zum Einfügen des Verzeichnisses `/etc/xinetd.d` enthält. Die Dateien innerhalb des Verzeichnisses `/etc/xinetd.d` enthalten die Konfigurationsoptionen für jeden der von `xinetd` verwalteten Dienste, so dass Sie diese Dateien bearbeiten müssen, um `xinetd` zu konfigurieren.

Die man-Seite `xinetd` (8) und die man-Seite `xinetd.conf` (8) enthalten genaue Anweisungen darüber, wie Sie die Dateien in `/etc/xinetd.d` einrichten. Eine andere gute Informationsquelle ist die `xinetd`-Web-Seite, die Sie unter http://www.xinetd.org/ finden.

Viele UNIX-Systemadministratoren verwenden TCP-Wrapper, um den Zugriff auf bestimmte Netzwerkdienste zu verwalten. Alle von `xinetd` verwalteten Netzwerkdienste (sowie jedes Programm mit integrierter Unterstützung für libwrap) kann TCP-Wrapper verwenden, um den Zugriff zu verwalten. `xinetd` kann die Dateien `/etc/hosts.allow` und `/etc/hosts.deny` verwenden, um den Zugriff auf die Systemdienste zu konfigurieren. Falls Sie TCP-Wrapper verwenden möchten, finden Sie weitere Informationen hierzu in den man-Seiten hosts_access (5).

Außerdem können Sie den Zugriff auf Systemdienste verwalten, indem Sie mit `ipchains` eine IP-Firewall konfigurieren. Bedenken Sie bitte: Falls Sie zum ersten Mal mit Linux arbeiten und noch nicht mit dem Programm vertraut sind, ist `ipchains` möglicherweise nicht die beste Lösung für Sie. Das Einrichten von `ipchains` kann kompliziert sein und sollte daher am besten nur von erfahrenen UNIX/Linux-Systemadministratoren ausgeführt werden.

Andererseits bietet `ipchains` den Vorteil der Flexibilität. Wenn Sie beispielsweise eine benutzerdefiniert gestaltete Lösung benötigen, bei der nur bestimmten Rechnern der Zugriff auf bestimmte Dienste gewährt wird, dann kann `ipchains` Ihnen diese Lösung bieten. In der Publikation *Linux IPCHAINS-HOWTO*, die unter http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html zur Verfügung steht, finden Sie weitere Informationen zu `ipchains`. Außerdem ist *Linux IPCHAINS-HOWTO* auch auf der Dokumentations-CD enthalten.

Wenn Sie auf der Suche nach einem Dienstprogramm sind, das die allgemeinen Zugriffsregeln für Ihren Computer zu Hause festlegt, und/oder wenn Sie noch nicht so sehr mit Linux vertraut sind, sollten Sie als Alternative das Dienstprogramm gnome-lokkit ausprobieren. Bei gnome-lokkit handelt es sich um ein Dienstprogramm mit grafischer Benutzeroberfläche, das Ihnen verschiedene Fragen darüber stellt, wie Sie Ihren Computer verwenden möchten. Anhand Ihrer Antworten konfiguriert gnome-lokkit dann eine einfache Firewall für Sie.

2.11 Anonymer Zugriff mit FTP

Das Einrichten des anonymen FTP-Zugriffs ist nicht schwer. Sie müssen lediglich das anonftp RPM -Paket installieren (was Sie möglicherweise schon bei der Installation getan haben). Nach der Installation ist der anonyme Zugriff auf FTP fertig eingerichtet.

Zum Konfigurieren des FTP-Servers können Sie die entsprechenden Dateien bearbeiten.

`/etc/ftpaccess`

Diese Datei definiert den größten Teil der Zugriffskontrolle auf Ihren FTP-Server. Sie können unter anderem logische "Gruppen" zur Zugriffskontrolle von verschiedenen Sites aus einrichten, die Zahl der gleichzeitigen FTP-Verbindungen begrenzen, die Protokollierung der Übertragungen konfigurieren u.v.m. Einzelheiten dazu finden Sie in der man-Seite ftpaccess.

/etc/ftphosts

Die Datei `ftphosts` wird verwendet, um den Zugriff auf bestimmte Accounts von verschiedenen Rechnern zuzulassen oder zu verwehren. Einzelheiten finden Sie in der man-Seite ftphosts.

/etc/ftpusers

In dieser Datei sind alle Benutzer aufgeführt, die *nicht* per FTP auf Ihren Computer zugreifen dürfen. Zum Beispiel ist `root` standardmäßig in `/etc/ftpusers` enthalten, d.h. Sie können nicht per FTP auf Ihren Computer zugreifen und sich als Root anmelden. Das gewährleistet höhere Sicherheit. Manche Administratoren entfernen jedoch den Eintrag `root` aus dieser Datei.

2.12 NFS-Konfiguration

NFS steht für *N*etwork *F*ile *S*ystem (Netzwerkdateisystem). Es ermöglicht die Freigabe von Dateien zwischen verschiedenen Computern, so dass der Eindruck entsteht, sie befänden sich auf Ihrer lokalen Festplatte. Linux kann sowohl als NFS-Server als auch als NFS-Client fungieren, d.h. es kann Dateisysteme **exportieren** (anderen Systemen anbieten) und von anderen Computern exportierte Dateisysteme **mounten**.

2.12.1 Mounten von NFS-Dateisystemen

Mit dem Befehl `mount` können Sie das NFS-Dateisystem eines anderen Computers mounten:

```
mkdir /mnt/local
# Nur erforderlich, wenn /mnt/local noch nicht vorhanden ist
mount bigdog:/mnt/export /mnt/local
```

Bei diesem Befehl ist bigdog der Name des NFS-Dateiservers. `/mnt/export` ist das Dateisystem, das von bigdog exportiert wird. `/mnt/local` ist ein Verzeichnis auf dem lokalen Computer, in dem das lokale Dateisystem gemountet werden soll.

Nachdem der Befehl `mount` ausgeführt wurde, können Sie, wenn Sie über die entsprechenden Berechtigungen von `bigdog` verfügen, `ls /mnt/local` eingeben. Die Dateien in `/mnt/export` auf dem Computer bigdog werden dann aufgelistet.

2.12.2 Exportieren von NFS-Dateisystemen

In der Datei `/etc/exports` ist angegeben, welche Dateisysteme Sie exportieren möchten. Das Format lautet:

```
Verzeichnis        Hostname(Optionen)
```

die `(Optionen)` sind benutzerbestimmbar. Dazu ein Beispiel:

```
/mnt/export     speedy.redhat.com
```

Damit erlauben Sie speedy.redhat.com, `/mnt/export` zu mounten

```
/mnt/export     speedy.redhat.com(ro)
```

Hiermit würden Sie speedy jedoch nur erlauben, `/mnt/export` schreibgeschützt zu mounten.

Nach jeder Änderung von `/etc/exports` müssen Sie die NFS-Dämonen anweisen, diese Datei auf neue Informationen zu überprüfen. Dazu können Sie die Dämonen einfach stoppen und wieder starten.

```
/etc/rc.d/init.d/nfs stop
/etc/rc.d/init.d/nfs start
```

Sie können die Dämonen auch mit diesem Befehl neu starten:

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

Es geht aber auch so:

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

Genauere Einzelheiten finden Sie in den man-Seiten nfsd(8), mountd(8) und exports(5). Eine weitere gute Informationsquelle ist *Managing NFS and NIS Services* von Hal Stern, herausgegeben von O'Reilly & Associates.

2.13 Der Bootprozess, Init und Shutdown

In diesem Abschnitt werden die Vorgänge beim Starten und Herunterfahren eines Red Hat Linux Systems dargestellt.

2.13.1 Interne Abläufe beim i386-Bootprozess

Wenn ein Computer gestartet wird, sucht der Prozessor am Ende des Systemspeichers nach dem **BIOS** (Basic Input/Output System) und führt es aus. Das BIOS-Programm ist im schreibgeschützten Speicher abgelegt und ständig einsatzbereit. Das BIOS stellt die Schnittstelle der untersten Ebene zu den Peripheriegeräten dar und steuert den ersten Schritt des Bootprozesses.

Das BIOS prüft das System, sucht und prüft Peripheriegeräte und sucht dann nach einem Bootlaufwerk. Normalerweise prüft es das Diskettenlaufwerk (oder auf vielen neueren Systemen das CD-ROM-Laufwerk, falls ein solches vorhanden ist) und sucht anschließend auf der Festplatte. Auf der Festplatte sucht das BIOS einen **Master Boot Record** (MBR), der im ersten Sektor der ersten Festplatte beginnt, und startet den MBR.

Der MBR sucht nach der ersten aktiven Partition und liest den Boot Record der Partition. Der Boot Record enthält Anweisungen zum Laden des Bootloaders LILO (*LI*nux *LO*ader). Anschließend lädt der MBR dann LILO, und LILO übernimmt den Prozess.

LILO liest die Datei `/etc/lilo.conf`, in der festgelegt ist, welche(s) Betriebssystem(e) zu konfigurieren ist/sind bzw. welcher Kernel zu starten ist und wo sich LILO installieren soll (zum Beispiel `/dev/hda` für Ihre Festplatte). LILO zeigt den `LILO:` -Prompt auf dem Bildschirm an und wartet eine festgelegte Zeitspanne (ebenfalls in der Datei `lilo.conf` festgelegt) auf Benutzereingaben. Wenn in Ihrer `lilo.conf` festgelegt ist, dass mit LILO ein bestimmtes Betriebssystem gewählt werden kann, können Sie am LILO-Prompt die Kennung des Betriebssystems eingeben, das Sie starten möchten.

Nach einer festgelegten Zeitspanne (üblicherweise fünf Sekunden), startet LILO dasjenige Betriebssystem, das zuerst in der Datei `lilo.conf` aufgeführt ist.

Beim Booten von Linux bootet LILO zuerst den Kernel, bei dem es sich um eine `vmlinuz`-Datei (plus Versionsnummer, z.B. `vmlinuz-2.2.15-xx`) handelt, die sich im Verzeichnis `/boot` befindet. Dann übernimmt der Kernel den weiteren Bootprozess.

Der Kernel sucht in mehreren verschiedenen Verzeichnissen nach init (üblicherweise in `/sbin` abgelegt) und führt das erste gefundene Programm init aus. Init übernimmt den weiteren Bootprozess.

Init startet alle Prozesse Ihres Linux-System (und wird gleichzeitig zum Elternteil bzw. Großelternteil dieser Prozesse). Zuerst wird `/etc/rc.d/rc.sysinit` ausgeführt, wodurch Ihr Pfad eingestellt und Swapping gestartet wird, die Dateisysteme überprüft werden usw. `rc.sysinit` schafft alle Voraussetzungen, die für Ihr System zum Zeitpunkt der Systeminitialisierung erfüllt sein müssen. In einem vernetzten System verwendet `rc.sysinit` beispielsweise die Informationen in den Dateien `/etc/sysconfig/network` und `/etc/sysconfig/clock`, um den Netzwerkprozess und die Uhr zu initialisieren. Außerdem wird `rc.serial` ausgeführt, falls Sie über serielle Port-Prozesse verfügen, die initialisiert werden müssen.

Init wertet die Datei `/etc/inittab` aus und implementiert die dort vorhandenen Angaben. Die Datei `/etc/inittab` beschreibt, wie das System auf jedem Runlevel einzurichten ist und legt das Standard-Runlevel fest. Diese Datei legt fest, dass `/etc/rc.d/rc` und `/sbin/update` beim Start eines Runlevels ausgeführt werden müssen.

Die Datei `/sbin/update` gibt fehlerhafte Puffer auf der Festplatte wieder frei.

Sobald sich das Runlevel ändert, startet und stoppt `/etc/rc.d/rc` die Dienste. Zuerst legt rc die Quellfunktionsbibliothek für das System fest (normalerweise `/etc/rc.d/init.d/functions`), in der beschrieben ist, wie Programme zu starten/beenden sind und wie die PID eines Programms bestimmt werden kann. Die Datei rc stellt dann fest, in welchem Runlevel sich das System aktuell befindet und in welchem es sich vorher befand, und übergibt diese Informationen an linuxconf.

Die Datei rc startet alle Hintergrundprozesse, die für die Ausführung des Systems erforderlich sind, und sucht nach einem rc-Verzeichnis für dieses Runlevel (`/etc/rc.d/rc<x>.d`, wobei das <*x*> eine Zahl zwischen 0 und 6 sein kann). rc beendet alle kill-Skripten (ihr Dateiname beginnt mit einem K). Dann initialisiert es alle start-Skripten (ihr Dateiname beginnt mit einem S) in dem geeigneten Runlevel-Verzeichnis (so dass alle Dienste und Anwendungen korrekt gestartet werden).

Beispiel für Runlevel 5: rc sucht im Verzeichnis `/etc/rc.d/rc5.d` und stellt fest, dass rusersd, rwalld, rwhod, mcserv, mars-nwe, apmd und pcmcia beendet werden müssen. Danach sucht rc im selben Verzeichnis nach Startskripten und findet Startskripten für kmod, network, nfsfs, randomc, syslog, atd, crond, portmap, snmpd, inet, xntpd, lpd, dhcpd, ypbind, autofs, keytable, sendmail, gpm und sound. Und so beginnt der ganze Vorgang erneut.

Die Datei `/etc/inittab` erzeugt mit fork einen Terminalprozess für jede virtuelle Konsole (Anmelde-Prompts) für jedes Runlevel (die Runlevels 2-5 verfügen über sechs solcher Konsolen, Runlevel 1 (Einzelbenutzermodus) nur über eine Konsole, Runlevels 0 und 6 erhalten keine virtuellen Konsolen).

In Runlevel 5 führt `/etc/inittab` außerdem ein Skript mit dem Namen `/etc/X11/prefdm` aus. Das Skript `prefdm` führt den bevorzugten X-Displaymanager aus (`gdm`, falls Sie GNOME ausführen, `kdm`, falls Sie KDE ausführen oder `xdm`, falls Sie AnotherLevel ausführen), basierend auf dem Inhalt des Verzeichnisses `/etc/sysconfig/desktop`.

Außerdem beschreibt /etc/inittab, wie das System [Strg]-[Alt]-[Entf] in einen Befehl wie `/sbin/shutdown -t3 -r now` übersetzen soll. Schließlich gibt `/etc/inittab` an, wie das System bei einem Stromausfall zu reagieren hat.

Wenn das System an dieser Stelle angelangt ist, sollten Sie einen Anmelde-Prompt auf dem Bildschirm sehen. Diese Aufgaben werden innerhalb weniger Sekunden ausgeführt.

Im nächsten Abschnitt werden die Dateien im Verzeichnis `/etc/sysconfig` beschrieben.

2.13.2 Sysconfig

Im Folgenden werden die verschiedenen Dateien in `/etc/sysconfig`, ihre Funktion und ihr Inhalt beschrieben.

Dateien in `/etc/sysconfig`

In der Regel enthält `/etc/sysconfig` die folgenden Dateien:

- `/etc/sysconfig/apmd`
- `/etc/sysconfig/clock`
- `/etc/sysconfig/harddisks`
- `/etc/sysconfig/hwconf` (sollte beim Bearbeiten ignoriert werden)
- `/etc/sysconfig/init`
- `/etc/sysconfig/keyboard`
- `/etc/sysconfig/mouse`
- `/etc/sysconfig/network`
- `/etc/sysconfig/pcmcia`
- `/etc/sysconfig/sendmail`
- `/etc/sysconfig/soundcard` (wird von sndconfig erstellt)

Es folgt eine Beschreibung der einzelnen Dateien.

`/etc/sysconfig/apmd`

Die Datei `/etc/sysconfig/apmd` wird von apmd zur Konfiguration verwendet, welche Prozesse nach den Befehlen suspend bzw. resume gestartet/gestoppt/geändert werden sollen. In ihr ist festgelegt, ob apmd beim Startvorgang aktiviert oder deaktiviert wird, je nachdem, ob Ihre Hardware Advanced Power Management (apm) unterstützt bzw. ob Sie diese Funktionalität verwenden wollen.

/etc/sysconfig/clock

In der Datei `/etc/sysconfig/clock` wird festgelegt, wie die Systemuhr zu interpretieren ist. In früheren Red Hat Linux Versionen wurden die folgenden Werte verwendet (in dieser Version bitte nicht mehr verwenden):

- `CLOCKMODE=`*`Modus`*, wobei *Modus* die folgenden Werte annehmen kann:
  - `GMT` — zeigt an, dass die Uhr auf UTC eingestellt wurde.
  - `ARC` — (bei Alpha-basierten Systemen) zeigt nur an, dass der 42-Jahre-Zeitoffset der ARC-Konsole wirksam ist.

In neueren Versionen werden nur noch die folgenden Einstellungen verwendet:

- `UTC=`*`boolean`*, wobei *boolean* einen der folgenden Werte annehmen kann:
  - `true` (wahr) — zeigt an, dass die Uhr auf UTC eingestellt ist. Jeder andere Wert stellt die Uhr auf lokale Zeit.
- `ARC=`*`boolean`*, wobei *boolean* einen der folgenden Werte annehmen kann:
  - `true` (wahr) — (nur bei Alpha-basierten Systemen) zeigt an, dass der 42-Jahre-Zeitoffset der ARC-Konsole wirksam ist. Jeder andere Wert stellt die Uhr auf normale Unix-Epoche (nur bei Alpha-Systemen).

- `ZONE=`*`"Dateiname"`* — zeigt der Zone-Datei unter `/usr/share/zoneinfo` an, dass `/etc/localtime` eine Kopie von beispielsweise folgender Datei ist:

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

/etc/sysconfig/desktop

Die Datei `/etc/sysconfig/desktop` legt fest, welcher Desktop-Manager ausgeführt werden soll.

/etc/sysconfig/harddisks

Die Datei `/etc/sysconfig/harddisks` ermöglicht es Ihnen, Ihre Festplatte(n) abzustimmen.

Folgende Werte können verwendet werden:

- `USE_DMA=1`, der Wert 1 aktiviert DMA. Bei einigen Chipsätzen und Festplattenkombinationen kann dies jedoch zu Datenverlusten führen.
- `Multiple_IO=16`, die Einstellung 16 lässt mehrere Sektoren pro E/A-Interrupt zu. Ist diese Funktion aktiviert, wird der Verwaltungsaufwand des Betriebssystems um 30-50 % reduziert. *Bei der Verwendung nur äußerst vorsichtig vorgehen.*
- `EIDE_32BIT=3`, aktiviert (E)IDE 32-Bit-E/A-Unterstützung für eine Schnittstellenkarte.
- `LOOKAHEAD=1`, aktiviert Lookahead-Lesezugriffe auf das Laufwerk.
- `EXTRA_PARAMS=`, ermöglicht das Hinzufügen von zusätzlichen Parametern.

/etc/sysconfig/hwconf

In der Datei `/etc/sysconfig/hwconf` sind alle Hardware-Komponenten aufgeführt, die kudzu in Ihrem System erkannt hat, außerdem Informationen zu den verwendeten Treibern, Anbieter-ID und Geräte-ID. Diese Datei darf nicht verändert werden. Wenn Sie diese Datei bearbeiten, kann es passieren, dass manche Geräte plötzlich als *hinzugefügt* oder *entfernt* angezeigt werden.

/etc/sysconfig/init

In der Datei `/etc/sysconfig/init` ist die Art der Bildschirmdarstellung beim Systemstart festgelegt.

Folgende Werte können verwendet werden:

- `BOOTUP=<Startmodus>`, wobei <*Startmodus*> einen der folgenden Werte annehmen kann:
  - `BOOTUP=color` erzeugt eine neue Bildschirmdarstellung beim Systemstart (verglichen mit Red Hat Linux 6.0).

- BOOTUP=verbose erzeugt eine Bildschirmdarstellung im herkömmlichen Stil.
- Alle übrigen Werte erzeugen eine neue Bildschirmdarstellung ohne ANSI-Formatierung.

- LOGLEVEL=<*Zahl*>, wobei <*Zahl*> den anfänglichen Konsolenanmeldelevel für den Kernel bestimmt. Die Standardeinstellung ist 7. Der Wert 8 aktiviert alles (einschließlich Debugging). 1 deaktiviert alles außer Kernel-Panik. syslogd hebt diese Einstellungen auf, nachdem es gestartet ist.
- RES_COL=<*Zahl*>, wobei <*Zahl*> eine Spalte des Bildschirms ist, wo Statuskennungen beginnen. Die Standardeinstellung ist 60.
- MOVE_TO_COL=<*Befehl*>, wobei <*Befehl*> den Cursor auf $RES_COL bewegt. Die Standardeinstellung ist die Ausgabe von ANSI-Sequenzen durch echo -e.
- SETCOLOR_SUCCESS=<*Befehl*>, wobei <*Befehl*> die Farbe für die Anzeige von erfolgreichen Vorgängen bestimmt. Die Standardeinstellung ist die Ausgabe von ANSI-Sequenzen mit echo -e, wobei die Farbe grün eingestellt wird.
- SETCOLOR_FAILURE=<*Befehl*>, wobei <*Befehl*> die Farbe für die Anzeige von nicht erfolgreichen Vorgängen bestimmt. Die Standardeinstellung ist die Ausgabe von ANSI-Sequenzen mit echo -e, wobei die Farbe rot eingestellt wird.
- SETCOLOR_WARNING=<*Befehl*>, wobei <*Befehl*> die Farbe für die Anzeige von Warnungen bestimmt. Die Standardeinstellung ist die Ausgabe von ANSI-Sequenzen mit echo -e, wobei die Farbe gelb eingestellt wird.
- SETCOLOR_NORMAL=<*Befehl*>, wobei <*Befehl*> die Farbe auf ’normal’ einstellt. Die Standardeinstellung ist die Ausgabe von ANSI-Sequenzen durch echo -e.
- PROMPT=*Antwort*, wobei *Antwort* folgende Werte annehmen kann:
  - yes — Aktiviert die Key-Überprüfung für den interaktiven Modus.

– `no` — Deaktiviert die Key-Überprüfung für den interaktiven Modus.

/etc/sysconfig/i18n

Die Datei `/etc/sysconfig/i18n` stellt die Standardsprache ein etc.

/etc/sysconfig/keyboard

Die Datei `/etc/sysconfig/keyboard` bestimmt das Verhalten der Tastatur. Folgende Werte können verwendet werden:

- `KEYTABLE=`*`Datei`*, wobei *Datei* der Name der keytable-Datei ist, zum Beispiel: `KEYTABLE="/usr/lib/kbd/keytables/us.map"`
- `KEYBOARDTYPE=sun|pc`, wird nur auf SPARC-Systemen verwendet. `sun` bedeutet, eine Sun-Tastatur ist an `/dev/kbd` angeschlossen, `pc` bedeutet, eine PS/2-Tastatur ist am PS/2-Port angeschlossen.

/etc/sysconfig/mouse

Die Datei `/etc/sysconfig/mouse` enthält Informationen über die angeschlossene Maus. Folgende Werte können verwendet werden:

- `MOUSETYPE=`*`Typ`*, wobei `Typ` einen der folgenden Werte annehmen kann:
  - `microsoft` — Eine Microsoft-Maus.
  - `mouseman` — Eine MouseMan-Maus.
  - `mousesystems` — Eine Mouse Systems-Maus.
  - `ps/2` — Eine PS/2-Maus.
  - `msbm` — Eine Microsoft-Bus-Maus.
  - `logibm` — Eine Logitech-Bus-Maus.
  - `atibm` — Eine ATI-Bus-Maus.
  - `logitech` — Eine Logitech-Maus.
  - `mmseries` — Eine ältere MouseMan-Maus.

  – `mmhittab` — Eine mmhittab-Maus.

- `XEMU3=`*`Emulation`*, wobei *Emulation* einen der folgenden Werte annehmen kann:
  – `yes` — Es sollen drei Maustasten emuliert werden.
  – `no` — Die Maus verfügt bereits über drei Maustasten.

Außerdem ist `/dev/mouse` ein symbolischer Link, der auf das eigentliche Mausgerät zeigt.

`/etc/sysconfig/network`

Die Datei `/etc/sysconfig/network` enthält Informationen über die gewünschte Netzwerkkonfiguration. Folgende Werte können verwendet werden:

- `NETWORKING=`*`Antwort`*, wobei *Antwort* einen der folgenden Werte annehmen kann:
  – `yes` — Das Netzwerk soll konfiguriert werden.
  – `no` — Das Netzwerk soll nicht konfiguriert werden.

- `HOSTNAME=`*`Rechnername`*, wobei als *Rechnername* der vollständige Domänenname (FQDN, Fully Qualified Domain Name) angegeben werden muss. Sie können aber jeden gewünschten Rechnernamen eintragen.

Bitte beachten

Um die Kompatibilität mit älteren Programmen (z.B. `trn`) sicherzustellen, muss die Datei `/etc/HOSTNAME` denselben Wert enthalten, der hier verwendet wird.

- `GATEWAY=`*`Gateway-IP`*, wobei *Gateway-IP* die IP-Adresse des Netzwerk-Gateways ist.
- `GATEWAYDEV=`*`Gateway-Gerät`*, wobei *Gateway-Gerät* der Gerätename für die Netzwerkkarte ist (z.B. eth0).
- `NISDOMAIN=`*`Domänenname`*, wobei *Domänenname* der Name der NIS-Domäne ist.

/etc/sysconfig/pcmcia

Die Datei `/etc/sysconfig/pcmcia` enthält Informationen über die PCMCIA-Konfiguration. Folgende Werte können verwendet werden:

- `PCMCIA=`*`Antwort`*, wobei *Antwort* einen der folgenden Werte annehmen kann:
  - `yes` — Die PCMCIA-Unterstützung soll aktiviert werden.
  - `no` — Die PCMCIA-Unterstützung soll nicht aktiviert werden.

- `PCIC=`*`PCIC-Typ`*, wobei *PCIC-Typ* einen der folgenden Werte annehmen kann:
  - `i82365` — Der Computer verfügt über einen Chipsatz mit i82365-PCMCIA-Steckplatz.
  - `tcic` — Der Computer verfügt über einen Chipsatz mit tcic-PCMCIA-Steckplatz.

- `PCIC_OPTS=`*`Option`*, wobei *Option* die Timing-Parameter für den Steckplatztreiber angibt (i82365 oder tcic).
- `CORE_OPTS=`*`Option`*, wobei *Option* die Liste der `pcmcia_core`-Optionen ist.
- `CARDMGR_OPTS=`*`Option`*, wobei *Option* die Liste der Optionen für den PCMCIA-Kartenmanager cardmgr ist (z.B. `-q` keine Meldungsausgabe (quiet mode), `-m` sucht ladbare Kernelmodule im angegebenen Verzeichnis usw. Weitere Informationen finden Sie in der man-Seite zu cardmgr).

/etc/sysconfig/sendmail

Die Datei `/etc/sysconfig/sendmail` ermöglicht das Versenden von Nachrichten an einen oder mehrere Empfänger, wobei die Nachrichten je nach den Erfordernissen über beliebige Netzwerke geroutet werden können. In der Datei sind die Standardwerte für die Ausführung des Programms sendmail festgelegt. Standardmäßig läuft das Programm als Dämon im Hintergrund und prüft seine Warteschlange pro Stunde einmal für den Fall, dass Nachrichten zurückgekommen sind.

Folgende Werte können verwendet werden:

- `DAEMON=`*`Antwort`*, wobei *Antwort* einen der folgenden Werte annehmen kann:
  - `yes` — Sendmail soll konfiguriert werden, um Port 25 auf eingehende Mails abzufragen. `yes` bedeutet `-bd`.
  - `no` — Sendmail soll nicht dafür konfiguriert werden, Port 25 auf eingehende Mails abzufragen.

- `QUEUE=1h`, wird an sendmail als `-q$QUEUE` übergeben. Die Option `-q` wird nicht an sendmail übergeben, wenn `/etc/sysconfig/sendmail` vorhanden ist und QUEUE leer oder nicht definiert ist.

/etc/sysconfig/soundcard

Die Datei `/etc/sysconfig/soundcard` wird von sndconfig erstellt und darf nicht verändert werden. Dies hat nur den Zweck, dass festgelegt wird, welcher Karteneintrag im Menü standardmäßig geöffnet werden soll, wenn sndconfig das nächste Mal ausgeführt wird.

Folgende Werte können verwendet werden:

- `CARDTYPE=<`*`Karte`*`>`, wobei <*Karte*> zum Beispiel als `CARDTYPE=SB16` angegeben wird.

Dateien in `/etc/sysconfig/network-scripts/`

In der Regel enthält `/etc/sysconfig/network-scripts` die folgenden Dateien:

- `/etc/sysconfig/network-scripts/ifup`
- `/etc/sysconfig/network-scripts/ifdown`
- `/etc/sysconfig/network-scripts/network-functions`
- `/etc/sysconfig/network-scripts/ifcfg-`<*Schnittstellenname*>
- `/etc/sysconfig/network-scripts/ifcfg-`<*Schnittstellenname*>-<*Klonname*>
- `/etc/sysconfig/network-scripts/chat-`<*Schnittstellenname*>
- `/etc/sysconfig/network-scripts/dip-`<*Schnittstellenname*>
- `/etc/sysconfig/network-scripts/ifup-post`

Es folgt eine Beschreibung der einzelnen Dateien.

`/etc/sysconfig/network-scripts/ifup`, `/etc/sysconfig/network-scripts/ifdown`

Es handelt sich um symbolische Links auf `/sbin/ifup` bzw. `/sbin/ifdown`. In diesem Verzeichnis dürfen nur diese beiden Skripten direkt aufgerufen werden. Die anderen Skripten werden von diesen beiden Skripten nach Bedarf aufgerufen. Diese symbolischen Links sind nur für ältere Systeme gedacht — in zukünftigen Versionen werden sie vermutlich wegfallen, daher sollten derzeit nur `/sbin/ifup` und `/sbin/ifdown` verwendet werden.

Diesen Skripten wird in der Regel nur ein Argument übergeben: der Name des Geräts (z.B. " `eth0`"). Beim Booten werden sie mit einem zweiten Argument "`boot`" aufgerufen, damit Geräte, die nicht schon beim Booten eingerichtet werden sollen (`ONBOOT=no`, [siehe unten]), in dieser Phase ignoriert werden können.

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

Dies ist eigentlich keine öffentliche Datei. Sie enthält Funktionen, die von den Skripten für das Einrichten und Entfernen von Schnittstellen verwendet werden. Sie enthält insbesondere den größten Teil des Codes für die Verwaltung alternativer Schnittstellenkonfigurationen und Schnittstellenänderungsmeldungen durch netreport.

/etc/sysconfig/network-scripts/ifcfg-<*Schnittstellenname*>, /etc/sysconfig/network-scripts/ifcfg-<*Schnittstellenname*>:<*Klonname*>

Die erste Datei definiert eine Schnittstelle, während die zweite Datei nur die Teile der Definition enthält, die in einer "Alias"- (oder einer alternativen) Schnittstelle anders sind. Zum Beispiel können sich die Netzwerknummern unterscheiden, während alle anderen Definitionen gleich sind. In diesem Fall enthält die Klondatei nur die Netzwerknummern, während alle Geräteinformationen in der zugrundeliegenden `ifcfg`-Datei stehen.

Die in der Datei `ifcfg` definierbaren Einträge hängen vom Schnittstellentyp ab.

Folgende Werte sind gemeinsame Werte:

- `DEVICE=`*`Name`*, wobei *Name* der Name des physikalischen Geräts ist (mit Ausnahme von dynamisch eingerichteten PPP-Geräten, bei denen hier der "logische Name" eingetragen wird).
- `IPADDR=`*`Adresse`*, wobei *Adresse* die IP-Adresse ist.
- `NETMASK=`*`Maske`*, wobei *Maske* der Wert für die Netzmaske ist.
- `NETWORK=`*`Adresse`*, wobei *Adresse* die Netzwerkadresse ist.
- `BROADCAST=`*`Adresse`*, wobei *Adresse* die Broadcast-Adresse ist.
- `GATEWAY=`*`Adresse`*, wobei *Adresse* die Gateway-Adresse ist.
- `ONBOOT=`*`Antwort`*, wobei *Antwort* einen der folgenden Werte annehmen kann:
  - `yes` — Dieses Gerät soll beim Systemstart aktiviert werden.
  - `no` — Dieses Gerät soll beim Systemstart nicht aktiviert werden.
- `USERCTL=`*`Antwort`*, wobei *Antwort* einen der folgenden Werte annehmen kann:

- `yes` — Benutzer, die keine Root-Benutzer sind, dürfen dieses Gerät steuern.
- `no` — Benutzer, die keine Root-Benutzer sind, dürfen dieses Gerät nicht steuern.

• `BOOTPROTO=`*`Protokoll`*, wobei *Protokoll* einen der folgenden Werte annehmen kann:

- `none` — Es soll kein Protokoll beim Systemstart verwendet werden.
- `bootp` — Das BOOTP-Protokoll soll verwendet werden.
- `dhcp` — Das DHCP-Protokoll soll verwendet werden.

Folgende Werte sind in allen SLIP-Dateien enthalten:

• `PERSIST=`*`Antwort`*, wobei *Antwort* einen der folgenden Werte annehmen kann:

- `yes` — Dieses Gerät soll jederzeit aktiv bleiben, selbst wenn es nach einem Auflegen des Modems deaktiviert wurde.
- `no` — Dieses Gerät soll nicht jederzeit aktiv sein.

• `MODEMPORT=`*`Port`*, wobei *Port* der Gerätename des Modemports ist (z.B. `"/dev/modem"`).

• `LINESPEED=`*`Baud`*, wobei *Baud* die Leitungsgeschwindigkeit des Modems ist (z.B. `"115200"`).

• `DEFABORT=`*`Antwort`*, wobei *Antwort* einen der folgenden Werte annehmen kann:

- `yes` — Beim Erstellen/Bearbeiten des Skripts für diese Schnittstelle sollen standardmäßige Abbruch-Strings eingefügt werden.
- `no` — Beim Erstellen/Bearbeiten des Skripts für diese Schnittstelle sollen keine standardmäßigen Abbruch-Strings eingefügt werden.

/etc/sysconfig/network-scripts/chat-<*Schnittstellenname*>

Diese Datei ist ein Chat-Skript für SLIP-Verbindungen und dient dazu, die Verbindung herzustellen. Bei SLIP-Geräten erzeugt das Chat-Skript ein DIP-Skript.

/etc/sysconfig/network-scripts/dip-<*Schnittstellenname*>

Dieses Write-only-Skript wird von `netcfg` aus dem Chat-Skript erzeugt. Es darf nicht bearbeitet werden. Möglicherweise wird diese Datei später nicht mehr verwendet und vom Chat-Skript zum Zeitpunkt der Verwendung neu erzeugt.

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

Diese Datei wird aufgerufen, wenn ein Netzwerkgerät (mit Ausnahme eines SLIP-Geräts) eingerichtet wird. Sie ruft `/etc/sysconfig/network-scripts/ifup-routes` auf, um statische, von diesem Gerät abhängende Routes und Alias-Namen für dieses Gerät hervorzurufen und richtet den Hostnamen ein, falls er noch nicht eingerichtet wurde — außerdem kann für das IP-Protokoll dieses Gerätes ein Hostname gefunden werden. `ifup-post` sendet SIGIO an alle Programme, die die Meldung von Netzwerkereignissen angefordert haben.

Diese Datei kann bei Bedarf erweitert werden, um die Konfiguration des Namensdienstes vorzunehmen, freie Skripten aufzurufen u.v.m.

2.13.3 Systemstart mit SysV-Init

In diesem Abschnitt werden die internen Vorgänge beim Bootvorgang kurz beschrieben. Es wird im Einzelnen dargestellt, wie der Computer mit SysV init bootet. Darüber hinaus werden die Unterschiede zwischen init in älteren Linux-Versionen und SysV init beschrieben.

Init wird beim Booten vom Kernel ausgeführt. Es ist für das Starten aller normalen Prozesse verantwortlich, die beim Booten ausgeführt werden müssen: die getty-Prozesse zum Anmelden am System, NFS-Dämonen, FTP-Dämonen und alle weiteren Prozesse, die Sie beim Booten Ihres Computers ausführen möchten.

SysV init setzt sich in der Linux-Welt immer mehr als Standard für die Steuerung des Startvorgangs durch. Der Grund: Es ist leichter bedienbar sowie leistungsfähiger und flexibler als das herkömmliche BSD-init.

SysV init unterscheidet sich von BSD init auch darin, dass die Konfigurationsdateien in einem Unterverzeichnis von `/etc` liegen und nicht direkt in `/etc`. Dieses Verzeichnis heißt `/etc/rc.d`. Es enthält `rc.sysinit` und die folgenden Verzeichnisse:

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

`init.d` enthält eine ganze Reihe von Skripten. Grundsätzlich brauchen Sie ein Skript für jeden Dienst, den Sie beim Booten oder beim Wechsel in ein anderes Runlevel starten müssen. Zu den Diensten gehören Netzwerkdienste wie `nfs`, `sendmail`, `httpd` usw. Programme wie `setserial`, die nur einmal ausgeführt werden müssen und dann beendet werden, zählen nicht zu diesen Diensten. Solche Programme sollten in `rc.local` oder `rc.serial` abgelegt werden.

Wenn Sie `rc.local` verwenden möchten, muss diese Datei in `/etc/rc.d` abgelegt werden. Obwohl die Datei rc.local kaum Aktionen auslöst, ist sie in den meisten Systemen enthalten. Wenn beim Booten des Systems der serielle Port bestimmte Aufgaben wahrnehmen muss, können Sie in `/etc/rc.d` auch die Konfigurationsdatei `rc.serial` ablegen.

Folgende Ereignisse laufen nacheinander ab:

- Der Kernel sucht an verschiedenen Stellen nach init und führt das init-Programm aus, das er zuerst findet.
- init führt `/etc/rc.d/rc.sysinit aus.`
- `rc.sysinit` kümmert sich um die meisten Bootloader-Prozesse und führt dann `rc.serial` aus (falls vorhanden).
- init führt alle Skripten für das Standard-Runlevel aus.
- init führt `rc.local aus.`

Der Standard-Runlevel wird in `/etc/inittab` festgelegt. Dort sollte in einer der ersten Zeilen etwa Folgendes stehen:

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

Wie Sie sehen, ist in der zweiten Spalte der Standard-Runlevel auf 3 eingestellt. Sie können `/etc/inittab` von Hand bearbeiten und einen anderen Wert als 3 eintragen. Vorsicht bei Änderungen an `inittab`. Falls die Datei nicht mehr funktionsfähig ist, können Sie sie reparieren, indem Sie einen Neustart einleiten und Folgendes eingeben:

```
LILO boot:  linux single
```

Damit *sollte* es möglich sein, im Einzelbenutzermodus zu booten, so dass Sie `inittab` noch einmal bearbeiten und wieder auf den früheren Wert einstellen können.

Wie führt init nun die richtigen Skripten aus? Wenn Sie im Verzeichnis `rc3.d` `ls -l` eingeben, wird Folgendes angezeigt:

```
lrwxrwxrwx 1 root root 17 3:11 S10network -> ../init.d/network
lrwxrwxrwx 1 root root 16 3:11 S30syslog -> ../init.d/syslog
lrwxrwxrwx 1 root root 14 3:32 S40cron -> ../init.d/cron
lrwxrwxrwx 1 root root 14 3:11 S50inet -> ../init.d/inet
lrwxrwxrwx 1 root root 13 3:11 S60nfs -> ../init.d/nfs
lrwxrwxrwx 1 root root 15 3:11 S70nfsfs -> ../init.d/nfsfs
lrwxrwxrwx 1 root root 18 3:11 S90lpd -> ../init.d/lpd.init
lrwxrwxrwx 1 root root 11 3:11 S99local -> ../rc.local
```

Es fällt Ihnen sicher auf, dass es in diesem Verzeichnis keine "echten" Dateien gibt. Alle Einträge sind Verweise auf eines der Skripten im Verzeichnis `init.d`. Außerdem steht am Beginn der Verweisnamen ein "S" und danach eine Zahl. Das "S" bedeutet, dass dieses Skript gestartet werden soll. Ein "K" würde bedeuten, dass es gestoppt werden soll. Die Zahl im Dateinamen dient nur der Festlegung einer Reihenfolge. Init startet die Dienste entsprechend ihrer Reihenfolge. Sie können Zahlen mehrfach verwenden, was allerdings zu Verwechslungen führen kann. Eine aus zwei Ziffern bestehende Zahl in Verbindung mit einem großen "S" oder "K" reicht aus, um die von Ihnen benötigten Dienste zu starten oder zu stoppen.

Wie startet und stoppt init Dienste? Ganz einfach: Die Skripten sind so geschrieben, dass ihnen ein Argument" `start`" bzw. "`stop`" übergeben werden kann. Sie können diese Skripten sogar mit einem Befehl wie dem folgenden manuell ausführen:

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

Dadurch wird der `httpd`-Server gestoppt. init liest den Namen ein. Beginnt er mit einem "K", ruft init das Skript mit dem Argument " `stop`" auf. Bei einem "S" ruft init das Skript mit dem Argument "`start`" auf.

Warum gibt es verschiedene Runlevels? Manche Systemadministratoren möchten Computer ohne großen Aufwand für verschiedene Zwecke nutzen. Ein "Server"-Runlevel könnte z.B. nur `httpd`, `sendmail`, Netzwerkunterstützung usw. ausführen. Weiterhin könnte ein "User"-Runlevel `gdm`, Netzwerkunterstützung usw. ausführen.

2.13.4 Init-Runlevels

Im Allgemeinen arbeitet Red Hat Linux in Runlevel 3 — d.h. im vollständigen Mehrbenutzermodus. Folgende Runlevels sind in Red Hat Linux definiert:

- `0` — Halt
- `1` — Einzelbenutzermodus
- `2` — Mehrbenutzermodus, ohne Netzwerk
- `3` — Vollständiger Mehrbenutzermodus
- `4` — Nicht verwendet
- `5` — Vollständiger Mehrbenutzermodus (mit einem X-basierten Anmeldebildschirm)
- `6` — Reboot

Wenn sich Ihr Computer aufgrund einer fehlerhaften Datei `/etc/inittab` nicht mehr booten lässt, oder wenn Sie sich nicht mehr anmelden können, weil `/etc/passwd` beschädigt ist oder weil Sie Ihr Passwort vergessen haben, dann booten Sie Ihren Computer im Einzelbenutzermodus, indem Sie am LILO-Boot-Prompt `linux single` eingeben. Es wird ein sehr einfaches System gestartet, bei dem Ihnen eine Shell angeboten wird, mit der Sie Reparaturen durchführen können.

2.13.5 Initscript-Dienstprogramme

Das Dienstprogramm `chkconfig` ist ein einfaches Befehlszeilentool für die Pflege der `/etc/rc.d`-Verzeichnishierarchie. Es erspart den Systemadministratoren, die zahlreichen symbolischen Links in `/etc/rc.d` direkt bearbeiten zu müssen.

Außerdem gibt es das Dienstprogramm `ntsysv`. Im Gegensatz zur befehlszeilenorientierten Oberfläche von `chkconfig` wird hier eine bildschirmorientierte Oberfläche verwendet.

Weitere Informationen hierzu finden Sie in Abschnitt 2.10, *Zugriffskontrolle auf Dienste* oder den man-Seiten `chkconfig` und `ntsysv`.

2.13.6 Ausführen von Programmen beim Systemstart

Die Datei `/etc/rc.d/rc.local` wird beim Systemstart ausgeführt, nachdem alle anderen Initialisierungen abgeschlossen sind, sowie bei jedem Wechsel des Runlevels. Dieser Datei können Sie zusätzliche Initialisierungsbefehle hinzufügen. Zum Beispiel könnten Sie zusätzliche Dämonen starten oder einen Drucker initialisieren. Wenn Sie zusätzlich einen seriellen Port einrichten müssen, können Sie die Datei `/etc/rc.d/rc.serial` bearbeiten. Beim Systemstart wird der Port dann automatisch eingerichtet.

Die Standarddatei `/etc/rc.d/rc.local` erstellt nur eine einfache Meldung beim Booten, die Ihre Kernel-Version und den Computertyp ausgibt.

2.13.7 Herunterfahren

Um Red Hat Linux herunterzufahren, geben Sie den Befehl `shutdown` ein. In der man-Seite zu `shutdown` finden Sie alle Einzelheiten. Die zwei am häufigsten verwendeten Befehlsvarianten sind:

```
shutdown -h now
shutdown -r now
```

Beide Varianten fahren das System ordnungsgemäß herunter. Bei Verwendung der Option `-h` wird das System nach dem Herunterfahren angehalten, bei Verwendung der Option `-r` wird das System nach dem Herunterfahren neu gestartet.

Obwohl die Befehle `reboot` und `halt` mittlerweile so "intelligent" sind, dass diese `shutdown` aufrufen, wenn sie in den Runlevels 1-5 ausgeführt werden, sollten Sie sich diese beiden Befehle nicht angewöhnen, da nicht alle Linux-ähnlichen Betriebssysteme über dieses Leistungsmerkmal verfügen.

2.14 Rettungsmodus

Wenn etwas schief geht, gibt es verschiedene Möglichkeiten, die Sache wieder in Ordnung zu bringen. Voraussetzung ist jedoch, dass Sie das System gut kennen. Wir zeigen Ihnen, wie Sie in den Rettungsmodus gelangen. Sie können dann Ihr eigenes Wissen anwenden, um das System zu retten.

2.14.1 Was ist der Rettungsmodus?

Unter Rettungsmodus wird das vollständige Booten einer kompakten Linux-Umgebung von Diskette oder CD verstanden.

Die Angaben in diesem Abschnitt helfen Ihnen beim Beheben zahlreicher Probleme mit Ihrem System.

Wie der Name andeutet, dient der Rettungsmodus zum Beseitigen von schwerwiegenden Problemen - gewissermaßen zur "Rettung" Ihres Systems. Während des normalen Betriebs verwendet Ihr Red Hat Linux-System für sämtliche Vorgänge Dateien, die sich auf der Festplatte des Systems befinden — das heißt, zum Ausführen von Programmen, Abspeichern von Dateien etc.

Möglicherweise treten jedoch manchmal Fehler auf, die Ihnen das vollständige Booten von Linux unmöglich machen, so dass Sie nicht auf die Dateien auf Ihrer Festplatte zugreifen können. Mit dem Rettungsmodus können Sie auf die Dateien, die auf der Festplatte Ihres Systems gespeichert sind, zugreifen, und zwar selbst dann, wenn Sie Linux nicht auf dieser Festplatte ausführen können.

Normalerweise benötigen Sie den Rettungsmodus in zwei Fällen:

- Sie können Linux nicht booten und möchten Ihr System reparieren.
- Sie haben Probleme mit Ihrer Hardware oder Software, und Sie möchten einige wichtige Dateien auf Ihrer Festplatte sichern.

Im Folgenden sollen nun diese beiden Szenarien näher betrachtet werden.

Linux kann nicht gebootet werden

Häufig ist dies auf die Installation eines weiteren Betriebssystems auf der Festplatte zurückzuführen, auf der Sie auch Red Hat Linux installiert haben. Einige Betriebssysteme sind nicht für die Koexistenz mit anderen Betriebssystemen ausgelegt und überschreiben den Master Boot Record (MBR), in dem sich ursprünglich Ihr LILO Bootloader befand. Wenn LILO auf diese Weise überschrieben wurde, haben Sie Pech gehabt — es sei denn, Sie können in den Rettungsmodus wechseln.

Hardware-/Software-Probleme

Unter diese Kategorie fallen genauso viele Probleme, wie es Systeme gibt, auf denen Linux ausgeführt wird. So können unter anderem defekte Festplatten oder ein nicht korrekt eingerichteter Bootloader nach dem Kompilieren eines neuen Kernels verhindern, dass Ihr System Red Hat Linux bootet. Wenn Sie in den Rettungsmodus wechseln können, besteht die Möglichkeit, das Problem zu lösen — oder Sie können zumindest Kopien der wichtigsten Dateien anlegen.

Um Ihr System im Rettungsmodus zu booten, geben Sie die folgenden Parameter am Installations-Boot-Prompt ein:

```
boot: linux rescue
```

Sie können auf zwei verschiedenen Wegen zum Boot-Prompt gelangen:

- Durch das Booten Ihres Systems von der mit Red Hat Linux gelieferten Diskette oder CD-ROM.
- Durch Booten über eine Netzwerk- oder PCMCIA-Bootdiskette. Dabei wird davon ausgegangen, dass Sie über eine funktionierende Netzwerkverbindung verfügen. Sie müssen außerdem den Netzwerkrechner und Übertragungstyp kennen. Informationen darüber, wie diese Informationen eingegeben werden können, finden Sie in "Installieren über das Netzwerk" in Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm*.

Sobald sich Ihr System im Rettungsmodus befindet, erscheint ein Prompt auf der virtuellen Konsole (VC, Virtual Console) 2 (verwenden Sie die Tastenkombination [Strg]-[Alt]-[F2], um auf VC 2 zuzugreifen):

```
bash#
```

An diesem Prompt können Sie die folgenden Befehle eingeben:

```
anaconda         gzip        mkfs.ext2   ps
badblocks        head        mknod       python
bash             hwclock     mkraid      python1.5
cat              ifconfig    mkswap      raidstart
chatter          init        mlabel      raidstop
chmod            insmod      mmd         rcp
chroot           less        mmount      rlogin
clock            ln          mmove       rm
collage          loader      modprobe    rmmod
cp    ls         mount       route
cpio             lsattr      mpartition  rpm
dd               lsmod       mrd         rsh
ddcprobe         mattrib     mread       sed
depmode          mbadblocks  mren        sh
df               mcd         mshowfat    sync
e2fsck           mcopy       mt          tac
fdisk            mdel        mtools      tail
fsck             mdeltree    mtype       tar
fsck.ext2        mdir        mv          touch
ftp              mdu         mzip        traceroute
genhdlist        mformat     open        umount
gnome-pty-helper minfo       pico        uncpio
grep             mkdir       ping        uniq
gunzip           mke2fs      probe       zcat
```

Wenn Ihr Root-Dateisystem jedoch nicht beschädigt ist, können Sie es mounten und anschließend jedes beliebige Linux-Dienstprogramm ausführen. Angenommen, Ihr Root-Dateisystem befindet sich in `/dev/hda5`. Dann wird diese Partition wie folgt gemountet:

```
mount -t ext2 /dev/hda5 /foo
```

Dabei ist */foo* ein von Ihnen erstelltes Verzeichnis.

Jetzt können Sie `chroot`, `fsck`, `man` und andere Dienstprogramme ausführen. In dieser Phase wird Linux im Einzelbenutzermodus ausgeführt.

Wenn Sie die Namen der Linux-Partitionen nicht kennen, können Sie versuchen, sie zu erraten. Das Mounten nicht vorhandener Partitionen verursacht keinen Schaden.

Einzelbenutzermodus direkt booten

Unter Umständen können Sie direkt in den Einzelbenutzermodus booten. Wenn Ihr System bootet, Sie sich nach dem Start aber nicht anmelden können, können Sie versuchen, nach einem Neustart am LILO-Boot-Prompt eine der folgenden Optionen anzugeben:

```
LILO boot: linux single
LILO boot: linux emergency
```

Im Einzelbenutzermodus bootet Ihr Computer in Runlevel 1. Ihr lokales Dateisystem wird gemountet, das Netzwerk ist jedoch nicht aktiviert. Es wird Ihnen eine Systemwartungsshell mit nützlichen Funktionen zur Verfügung gestellt.

Im Notfallmodus wird in die minimal mögliche Umgebung gebootet. Das Root-Dateisystem wird schreibgeschützt gemountet, und ansonsten ist fast nichts eingerichtet. Der Hauptvorteil dieses Modus im Vergleich zu `linux single` ist, dass Ihre init-Dateien nicht geladen werden. Wenn init fehlerhaft ist oder nicht funktioniert, können Sie trotzdem Dateisysteme mounten, um Daten wiederherzustellen, die bei einer Neuinstallation verloren gehen könnten.

Ein Trick für die Praxis

Ist es Ihnen schon einmal passiert, dass Sie einen Kernel neu konfiguriert haben und - erpicht darauf, Ihr neues Werk auszuprobieren - den Rechner neu gestartet haben, ohne vorher LILO auszuführen? Und Sie verfügen über keinen Eintrag für einen älteren Kernel in `lilo.conf`? Dann lesen Sie weiter…

In vielen Fällen ist es möglich, Ihr Red Hat Linux/Intel System von der Red Hat Linux Bootdiskette mit gemountetem und fertig vorbereitetem Root-Dateisystem zu starten. Das geht folgendermaßen:

Geben Sie den folgenden Befehl am `boot:` -Prompt der Bootdiskette ein:

```
linux single root=/dev/hdXX initrd=
```

(Ersetzen Sie *XX* in `/dev/hd`*XX* durch den Buchstaben und die Zahl, die Ihrer Root-Partition entsprechen.)

Was wird damit bewirkt? Zuerst startet der Bootprozess im Einzelbenutzermodus, wobei die Root-Partition Ihre Root-Partition ist. Die leere Angabe `initrd` umgeht das installationsbezogene Image auf der Bootdiskette, so dass Sie sich sofort im Einzelbenutzermodus befinden.

Hat dieser Trick auch einen Nachteil? Leider ja. Da der Kernel auf der Red Hat Linux Bootdiskette nur IDE unterstützt, funktioniert dieser Trick nicht auf Systemen mit SCSI-Controllern. In diesem Fall müssen Sie die oben erwähnte Kombination aus Bootdiskette und Rettungsdiskette verwenden.

3 Systemkonfiguration

Eine der Hauptstärken von Red Hat Linux ist, dass man bei entsprechender Konfiguration mit diesem Betriebssystem fast alles machen kann. In der Vergangenheit mussten dazu manchmal kryptische Konfigurationsdateien von Hand bearbeitet und Systemdienste neu gestartet werden. Dann mussten Sie darauf hoffen, dass die Veränderungen richtig vorgenommen wurden. Außerdem kann die Vielfalt der Konfigurationsoptionen für neue Benutzer verwirrend sein, die vielleicht nicht wissen, wo sie eine spezielle Konfigurationsdatei finden können.

Red Hat Linux bietet zwei Dienstprogramme zur Systemkonfiguration: linuxconf und das Control Panel. Das Control Panel verfügt über ein Startprogramm für verschiedene Red Hat Systemkonfigurationstools einschließlich linuxconf. Eine Bedienungsanleitung für das Control Panel und seine Tools finden Sie in Abschnitt 3.2, *Konfigurieren des Systems mit Control Panel*.

Das Konfigurationstool linuxconf erleichtert die Systemkonfiguration. linuxconf ist sowohl:

- Eine Konfigurationsschnittstelle — Sie geben die Werte zur Konfiguration Ihres Systems unter einer Benutzeroberfläche ein.
- Ein Tool zum Aktivieren der Konfiguration — Sobald Sie Ihre Änderungen vorgenommen haben, kann linuxconf die Änderungen übernehmen.

Obwohl linuxconf gegenwärtig fast alles leisten kann, was die Control Panel Tools können, ist das Control Panel in zwei Bereichen weiterhin unschlagbar:

- Druckerkonfiguration
- Laden von Kernelmodulen zur Unterstützung neuer Hardware

Aber nun zu linuxconf.

3.1 Konfigurieren des Systems mit Linuxconf

linuxconf ist ein Dienstprogramm, das Ihnen die Konfiguration und Steuerung verschiedener Aspekte Ihres Systems ermöglicht und eine Vielzahl von Programmen und Tasks handhaben kann. Die vollständige Dokumentation von linuxconf würde ein eigenes Buch ergeben und daher den Rahmen dieses Kapitels sprengen. Wir konzentrieren uns deshalb auf häufige Aufgaben wie das Hinzufügen eines neuen Benutzers oder die Anbindung an ein Netzwerk.

Weitere Informationen zu linuxconf einschließlich der neuesten Version finden Sie auf der linuxconf-Website:

http://www.solucorp.qc.ca/linuxconf/

Die linuxconf-Website bietet neben der Software recht umfangreiche Informationen wie Beschreibung, Grundgedanke, Geschichte, Liste mit Kontaktpersonen und vieles mehr. Die Website wird von Jacques Gelinas, dem Schöpfer von linuxconf, gepflegt und enthält daher die neuesten Informationen zu linuxconf.

Dieses Kapitel beschreibt nur einige wenige Funktionen von linuxconf detailliert. Eine Kurzreferenz, die zeigt, wo Sie in linuxconf die in diesem Kapitel beschriebenen Aufgaben durchführen können, finden Sie in Abschnitt 3.1.15, *So finden Sie sich zurecht mit* linuxconf.

Wenn Sie mehr Hilfe zu linuxconf benötigen, können Sie folgende Quellen konsultieren:

- Die linuxconf-FAQ, verfügbar unter http://www.xc.org/jonathan/linuxconf-faq.html.
- Die Archive der linuxconf-Mailingliste, verfügbar unter http://hub.xc.org/scripts/lyris.pl?visit=linuxconf.
- Wenn Sie nicht in den linuxconf-FAQ und den Archiven der linuxconf-Liste fündig werden, können Sie versuchen, Ihre Frage in der linuxconf-Liste zu stellen. Informationen zur Anmeldung für die linuxconf-Liste finden Sie auf der linuxconf-Website (http://www.solucorp.qc.ca/linuxconf/). Klicken Sie dazu auf den Link "Mailing lists".

  Beachten Sie bitte, dass diese Liste für Fragen zu linuxconf gedacht ist, nicht für allgemeine Linux-Fragen.

3.1.1 Ausführen von linuxconf

Um linuxconf ausführen zu können, müssen Sie Root-Zugriffsrechte haben. Melden Sie sich also mit `su` als Root an, wenn Sie sich in Ihrem Benutzeraccount befinden.

Geben Sie nun am Shell Prompt `linuxconf` ein, um das Programm zu starten.

3.1.2 linuxconf Benutzeroberflächen

linuxconf verfügt über vier Benutzeroberflächen:

- Textbasiert — Diese Oberfläche entspricht der des textbasierten Installationsprogramms von Red Hat Linux. Das Navigieren durch linuxconf ist einfach, wenn Sie X nicht ausführen. Wenn Sie X ausführen, schalten Sie auf eine virtuelle Konsole um, melden sich als Root an, und geben `linuxconf` ein, um linuxconf im Textmodus aufzurufen.

  Verwenden Sie die [Tabulator]- und [Cursor]-Tasten zum Navigieren in Textmodus-Bildschirmen. Ein **nach unten gerichteter Pfeil** auf einer Zeile zeigt an, dass in dieser Zeile ein Pulldown-Menü vorhanden ist. Mit der Tastenkombination [Strg]-[X] können Pull-Down-Menüs geöffnet werden.

- Grafische Benutzeroberfläche (GUI) — linuxconf kann vom X Window System profitieren. Red Hat Linux enthält gnome-linuxconf, eine GUI für linuxconf.

  Die in dieser Dokumentation dargestellten Bildschirme von linuxconf gehören zur Oberfläche gnome-linuxconf. Sie sollten jedoch anhand der hier aufgeführten Anweisungen auch mit den anderen Oberflächen problemlos arbeiten können.

- Web-basiert— Die Oberfläche auf Web-Basis macht die Verwaltung von Remote-Systemen zum Kinderspiel. Sie kann auch mit dem textbasierten Browser Lynx dargestellt werden.

  Sie können die Web-Oberfläche von linuxconf verwenden, indem Sie Ihren Web-Browser mit dem Port 98 des Rechners verbinden, auf dem linuxconf ausgeführt wird (also http://Ihr_Rechner:98).

  Bevor Sie die Web-basierte Oberfläche verwenden können, müssen Sie linuxconf so konfigurieren, dass Verbindungen von dem Rechner, auf dem der Browser ausgeführt wird, zugelassen sind. Eine Anleitung für das Aktivieren des Web-

Zugriffs auf linuxconf finden Sie in Abschnitt 3.1.4, *Aktivieren des web-basierten Zugriffs auf* linuxconf.

- Befehlszeile — Der Befehlszeilenmodus von linuxconf eignet sich zur Änderung Ihrer Systemkonfiguration mit Skripten.

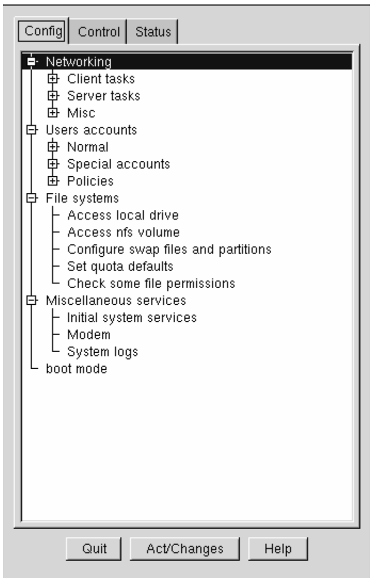
linuxconf startet normalerweise entweder im Textmodus oder im X-Modus, je nachdem, wie die Umgebungsvariable **DISPLAY** gesetzt ist. Wenn Sie linuxconf zum ersten Mal aufrufen, wird eine einleitende Meldung angezeigt. Später können Sie diese grundlegenden Informationen durch Aufrufen der Hilfe vom Hauptbildschirm aus finden.

linuxconf bietet kontextspezifische Hilfe. Weitere Informationen zu speziellen Aspekten von linuxconf erhalten Sie, wenn Sie in dem Bildschirm, zu dem Sie Hilfe benötigen, auf **Hilfe** klicken. Beachten Sie, dass momentan noch nicht alle Hilfebildschirme vollständig sind. Die Bildschirme werden nach und nach aktualisiert und in die nachfolgenden Versionen von linuxconf eingefügt.

3.1.3 gnome-linuxconf, Schnittstelle

gnome-linuxconf ermöglicht das schnelle und mühelose Navigieren durch die hierarchische Struktur von linuxconf.

Abbildung 3–1 Linuxconf **Menüansicht**



Bitte beachten

Wenn die oben dargestellte Baumstruktur nicht angezeigt wird, befolgen Sie die folgenden Anweisungen:

---

1. Öffnen Sie **System** => **Systemsteuerung** => **linuxconf Module**.
2. Aktivieren Sie das Kontrollkästchen treemenu.
3. Klicken Sie auf **Bestätigen**.
4. Klicken Sie auf **Beenden**.
5. Starten Sie linuxconf neu.

Wenn Sie mit der Baumenü-Ansicht arbeiten, können Sie die entsprechenden Teilfenster schnell und mühelos aufrufen. Klicken Sie auf + bzw. - neben den Menüeinträgen, um Abschnitte anzuzeigen oder zu verbergen.

Ausgewählte Einträge erscheinen als Register im rechten Teilfenster und verbleiben dort, bis sie geschlossen werden. Wenn zu viele Register geöffnet sind, klicken Sie im unteren Bereich des jeweiligen Registers auf **Abbrechen**, um es zu schließen, oder klicken Sie auf **Bestätigen**, um die Einstellungen zu übernehmen.

3.1.4 Aktivieren des web-basierten Zugriffs auf linuxconf

Aus Sicherheitsgründen ist der web-basierte Zugriff auf linuxconf standardmäßig deaktiviert. Um mit einem Web-Browser auf linuxconf zugreifen zu können, müssen Sie zuerst den Zugriff aktivieren. Führen Sie hierzu die folgenden Schritte aus:

1. Öffnen Sie **Verwaltung** => **Netzwerk** => **Verschiedenes** => **linuxconf Netzwerkzugriff.**
2. Geben Sie im Dialogfeld **Linuxconf html access control** den Host-Namen aller Computer ein, die Zugriff auf Linuxconf erhalten sollen. Dazu gehört auch Ihr eigenes System, falls Sie die web-basierte Oberfläche lokal verwenden möchten. Aktivieren Sie das Kontrollkästchen, wenn Webzugriffe auf linuxconf in der Datei `htmlaccess.log` protokolliert werden sollen.
3. Klicken Sie auf den Button **Bestätigen.**

Jetzt ist der web-basierte Zugriff aktiviert. Führen Sie an einem der Systeme, die Sie zur Zugriffskontrollliste hinzugefügt haben, einen Test durch. Starten Sie den Web-Browser, und geben Sie die folgende URL ein:

```
http://<host>:98/
```

(`<host>` wird natürlich durch den Rechnernamen Ihres Systems ersetzt. Entfernen Sie außerdem die Zeile "disable=yes" aus der Datei `/etc/xinetd.d/linuxconf`, und führen Sie anschließend den Befehl `/sbin/service xinetd reload` von einem Shell Prompt aus.) Daraufhin sollte die Hauptseite von linuxconf angezeigt werden. Beachten Sie, dass Sie das Root-Passwort Ihres Systems eingeben müssen, um die folgenden Seiten aufrufen zu können.

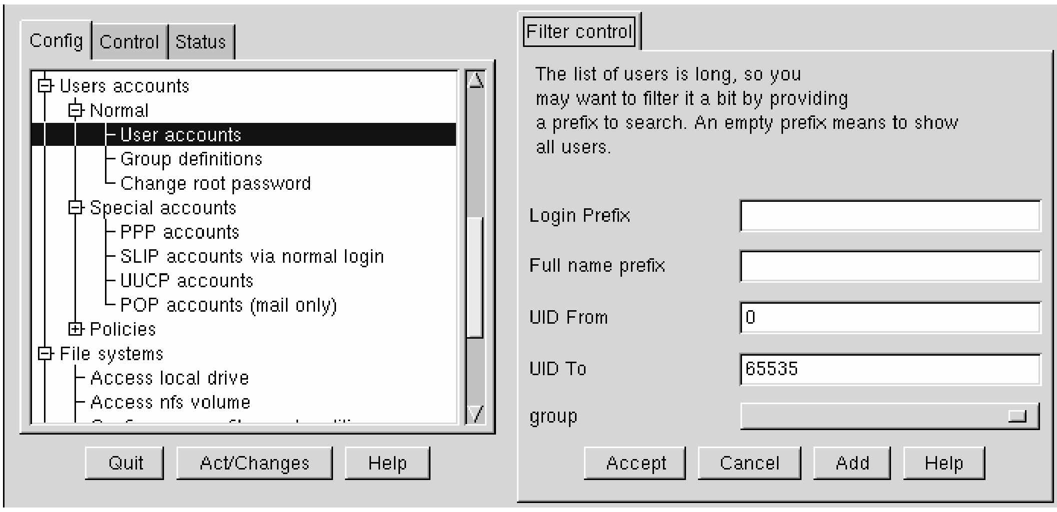
Sie können auch den Zugriff auf linuxconf im gesamten Netzwerk aktivieren, indem Sie genauso vorgehen und statt des Rechnernamens einen Netzwerknamen eingeben.

3.1.5 Hinzufügen eines Benutzeraccounts

Das Hinzufügen eines Benutzers ist eine der grundlegendsten Aufgaben der Systemadministration. So fügen Sie einen Benutzer hinzu:

- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts.** linuxconf zeigt möglicherweise einen Filterbildschirm an (siehe Abbildung 3–2, *Bildschirm Filtereinstellungen*).

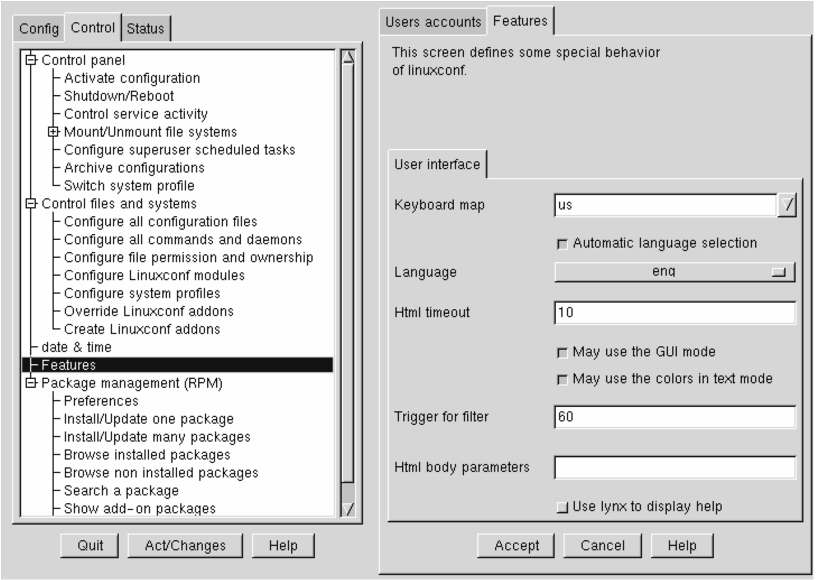
Abbildung 3–2 Bildschirm Filtereinstellungen



Mit dem Filterbildschirm können Sie aus der gesamten Liste einen kleineren Accountbereich auswählen. Um die vollständige Liste anzuzeigen, klicken Sie einfach auf **Bestätigen**, und ändern Sie keinen der Parameter. Genauere Informationen über die verschiedenen Filter erhalten Sie, wenn Sie im Bildschirm **Filtereinstellungen** auf den Button **Hilfe** klicken. Wenn Sie den Filter angewandt oder dessen Verwendung abgebrochen haben, wird das Register **Benutzeraccounts** angezeigt (siehe Abbildung 3–4, *Bildschirm Benutzeraccounts*).

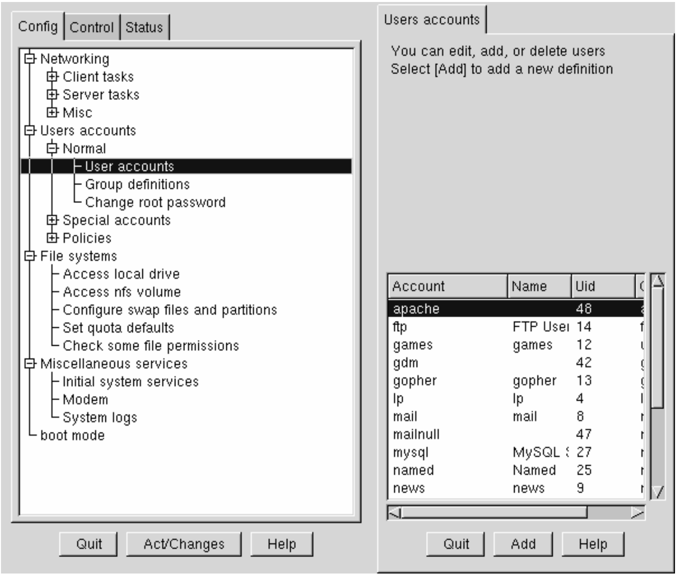
Sie können den Filter über **Control** => **Features** steuern. Im Register **Features** können Sie den Parameter **Trigger for filter** einstellen wie in Abbildung 3–3, *Einstellen des Auslösers der Filterfunktion* gezeigt.

Abbildung 3–3 Einstellen des Auslösers der Filterfunktion



Im Feld **Trigger for filter** legen Sie fest, bei wie vielen Einträgen ein Filterbildschirm aufgerufen werden soll.

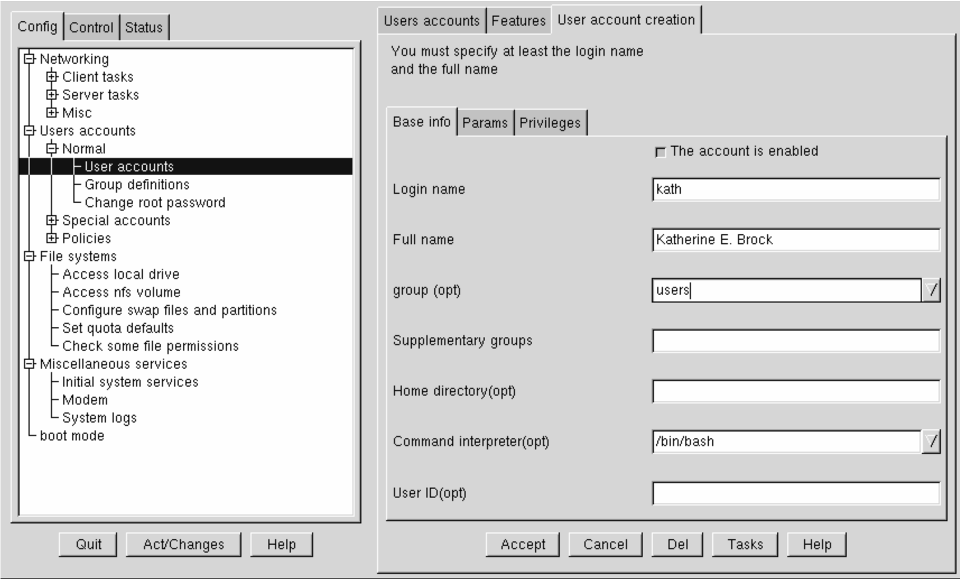
Abbildung 3–4 Bildschirm Benutzeraccounts



- Klicken Sie auf **Neu**. Das Register **Benutzeraccounterzeugung** wird geöffnet (siehe Abbildung 3–5, *Erstellen von Benutzeraccounts*).

Der Bildschirm **Benutzeraccounterzeugung** enthält die Abschnitte **Basisinformationen**, **Params** und **Privileges**. Es muss hier nur der **Anmeldename** angegeben werden, doch sollten Sie auch die anderen Felder beachten, in denen es Ihnen freigestellt ist, ob Sie etwas eintragen.

Abbildung 3–5 Erstellen von Benutzeraccounts



Basisinformationen für Benutzeraccounts

Der **Login-Name** ist der Name des Accounts und wird meist vollständig in Kleinbuchstaben geschrieben. Übliche Anmeldenamen bestehen aus Vornamen, Familiennamen, Initialen oder einer beliebigen Kombination aus diesen. Für einen Benutzer mit dem Namen Thomas Mustermann wären **`mustermann`**, **`thomas`**, **`tmst`** oder **`tmustermann`** übliche Benutzernamen. Selbstverständlich ist **`liesel`** oder Ähnliches ebenfalls möglich. Zahlen können ebenfalls verwendet werden: **`tm2`** wäre für einen zweiten Benutzer mit denselben Initialen denkbar. Einen Standardwert gibt es für dieses Feld nicht.

Der **vollständige Name** ist der Name des Benutzers bzw. des Accounts. Bei einer Person wäre das der Name der Person, z.B. **`Thomas Mustermann`**. Wenn der Account keine Person, sondern eine Position repräsentiert, könnte der vollständige Name aus dem Titel bestehen. Ein Account mit dem Namen **`webmaster`** könnte den vollständigen Namen **`Red Hat Webmaster`** oder auch nur **`Webmaster`** haben. Einen Standardwert gibt es für dieses Feld nicht.

Da Red Hat Linux das Prinzip der benutzereigenen Gruppen verwendet, wird jeder Benutzer einer **Standardgruppe** zugeordnet, die nur aus diesem Benutzer besteht. Weitere Informationen zu benutzereigenen Gruppen finden Sie in Abschnitt 2.3.3, *Benutzereigene Gruppen*.

Im Feld **Zusätzliche Gruppen** können Sie zusätzliche Gruppen angeben. Gruppennamen müssen durch Leerzeichen voneinander getrennt sein. Standardwert für dieses Feld ist ein leeres Feld, also keine zusätzliche Gruppe.

Das **Benutzerverzeichnis** gibt das Heimat- oder Anmeldeverzeichnis für den Account an. Der Standardwert ist `/home/login`, wobei *`login`* durch den Anmeldenamen ersetzt wird. Bei der Anmeldung ist das Home-Verzeichnis Ihr Startpunkt in der Verzeichnisstruktur. Falls Sie sich in X befinden, ist das Home-Verzeichnis der Startpunkt für jedes geöffnete XTerm-Fenster. Dieses Verzeichnis enthält auch accountspezifische Dateien mit persönlichen Einstellungen.

Der **Befehlsinterpreter** ist die Standardshell für den Account. Die `bash`-Shell ist die Standardshell für Red Hat Linux.

Die **Benutzer-ID** (UID) ist die Nummer, die jedem Benutzeraccount zugeordnet ist. Diese wird bei der Erstellung des Accounts automatisch vom System erzeugt. Lassen Sie das Feld also leer. Das System verwendet die UID, um einen Account zu identifizieren.

Params für Benutzeraccounts

Die **Params** werden für die Passwort- und Accountverwaltung verwendet. Gemäß der Voreinstellung werden alle Einstellungen **Ignored**, d.h. nicht verwendet. **Must keep # days** legt fest, wie viele Tage das Benutzerpasswort mindestens beibehalten werden soll.

Im Feld **Must change after # days** können Sie festlegen, nach wie vielen Tagen ein Benutzerpasswort ablaufen soll. Wenn Sie die Benutzer darauf hinweisen möchten, dass ihr Passwort abläuft (empfehlenswert) sollten Sie das Feld **Warn # days before expiration** ausfüllen.

Sollen ihre Accounts nach einer bestimmten Anzahl an Tagen ablaufen, verwenden Sie das Feld **Account expire after # days** , oder stellen Sie einen festen Zeitpunkt für das **Expiration date** ein.

Berechtigungen für Benutzeraccounts

Im Bereich **Berechtigungen** können Sie den Zugriff auf und/oder die Kontrolle über verschiedene Aspekte des Systems gewähren. Standardmäßig sind normalen Benutzern alle Berechtigungen in diesem Fenster entzogen. Sie können ihnen aber spezifische Berechtigungen gewähren oder stillschweigend gewähren. Der Unterschied zwischen **Gewährt** und **Gewährt/stillschweigend** besteht darin, dass linuxconf bei einer gewährten Berechtigung das Passwort des Benutzers abfragt, bevor die Berechtigung vergeben wird, bei der stillschweigenden Berechtigung jedoch nicht.

Im Allgemeinen wird ein gewissenhafter Systemadministrator Benutzern keine Berechtigungen zur Systemadministration gewähren, es sei denn, es ist absolut notwendig. Daher sollten Sie beim Gewähren von stillschweigenden Berechtigungen Vorsicht walten lassen. Wenn sich ein Benutzer mit stillschweigend gewährten Berechtigungen an seinem/ihrem Rechner anmeldet und den Rechner unbeaufsichtigt lässt, kann im Prinzip jeder beliebige andere Benutzer Änderungen am System vornehmen. Stillschweigend gewährte Berechtigungen sind weniger riskant, wenn sie auf Rechnern in einem räumlich getrennten Bereich verwendet werden.

Kann linuxconf verwenden: der Benutzer kann auf alle Funktionen und Fähigkeiten von linuxconf zugreifen und die entsprechenden Parameter einstellen oder verändern. Beachten Sie, dass die Berechtigung zur Verwendung von **linuxconf** etwas anderes ist als die Berechtigung zum Aktivieren von Konfigurationsänderungen. Möglicherweise will der Systemadministrator das Recht zur Verwendung von linuxconf einräumen, jedoch die Aktivierungsberechtigung nicht gewähren, damit er selbst die endgültige Entscheidung treffen kann, ob Konfigurationsänderungen aktiviert werden sollen.

Kann Konfigurationsänderungen aktivieren: Nach dem Ändern eines Parameters in linuxconf müssen Sie linuxconf anweisen, die Änderungen zu übernehmen. Sie haben hierzu je nach verwendeter Benutzerschnittstelle die folgenden Möglichkeiten: Klicken Sie in der GUI von linuxconf auf den Button **Activate the changes**, klicken Sie im web-basierten linuxconf auf den Button **Bestätigen**, klicken Sie im textbasierten linuxconf auf den Button **Bestätigen** usw.

Sie können einem Benutzer die Berechtigung zum Aktivieren von Änderungen gewähren. In diesem Fall kann der Benutzer alle in linuxconf geänderten Parameter der Systemkonfiguration aktivieren.

Kann System herunterfahren: Einem Benutzer kann die Berechtigung zum Herunterfahren des Systems gewährt werden. Beachten Sie, dass Red Hat Linux in `/etc/inittab` so konfiguriert ist, dass das System nach Eingabe der Tastenkombination [Strg]-[Alt]-[Entf] sauber heruntergefahren wird.

Sie können Benutzern die Berechtigung gewähren, zwischen verschiedenen Netzwerkmodi umzuschalten oder Systemprotokolle anzuzeigen, und Sie können sogar Superuser-Berechtigungen vergeben.

Wenn Sie den Anmeldenamen und alle erforderlichen Informationen eingegeben haben, klicken Sie im unteren Bereich des Bildschirms auf den Button **Bestätigen**. Wenn Sie keinen neuen Benutzer erstellen wollen, klicken Sie stattdessen auf **Abbrechen**.

Wenn Sie auf **Bestätigen** klicken, werden Sie von linuxconf nach dem Passwort gefragt, siehe Abbildung 3–6, *Bildschirm Ändere Passwort*. Das Passwort muss nochmals eingegeben werden, um eine Falscheingabe des Passworts zu verhindern. Passwörter müssen mindestens sechs Zeichen umfassen. Sie können die erforderliche Länge jedoch auch erhöhen und andere Parameter für Benutzerpasswörter definieren. Rufen Sie hierfür den Bildschirm **Benutzeraccounts** => **Policies** => **Password & Account Policies** auf.

Gute Passwörter bestehen aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen und sollten sowohl Groß- als auch Kleinbuchstaben enthalten. Ungeeignet sind leicht zu erratende Namen wie Ihr Benutzername, Ihr Geburtstag, Ihre Versicherungsnummer, den Namen Ihres Hundes, Ihr zweiter Vorname oder das Wort root. Verwenden Sie auch keine Variation eines Wortes, das mit Ihrem Account oder mit Ihnen selbst zusammenhängt. Verwenden Sie keine Wörter, die in einem Wörterbuch vorkommen. Solche Wörter können leicht geknackt werden.

Eine einfache Methode zum Finden von Passwörtern ist die Verwendung des ersten Buchstabens jedes Wortes eines Satzes, den Sie kennen (z.B. eine Zeile aus einem Ihrer Lieblingslieder). Verwenden Sie einige Großbuchstaben und Zahlen und/oder Sonderzeichen anstelle von Buchstaben, und Sie haben ein geeignetes Passwort.

Klicken Sie abschließend wieder auf **Bestätigen**. Das System teilt Ihnen mit, ob das Passwort leicht zu knacken ist. Wenn eine entsprechende Warnmeldung ausgegeben wird, sollten Sie das Passwort nicht verwenden.

3.1.6 Ändern eines Benutzeraccounts

- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts**, verwenden Sie erforderlichenfalls den Filter, und wählen Sie den Account, den Sie ändern wollen.
- Hilfe zum Ausfüllen der Felder finden Sie in Abschnitt 3.1.5, *Hinzufügen eines Benutzeraccounts*.

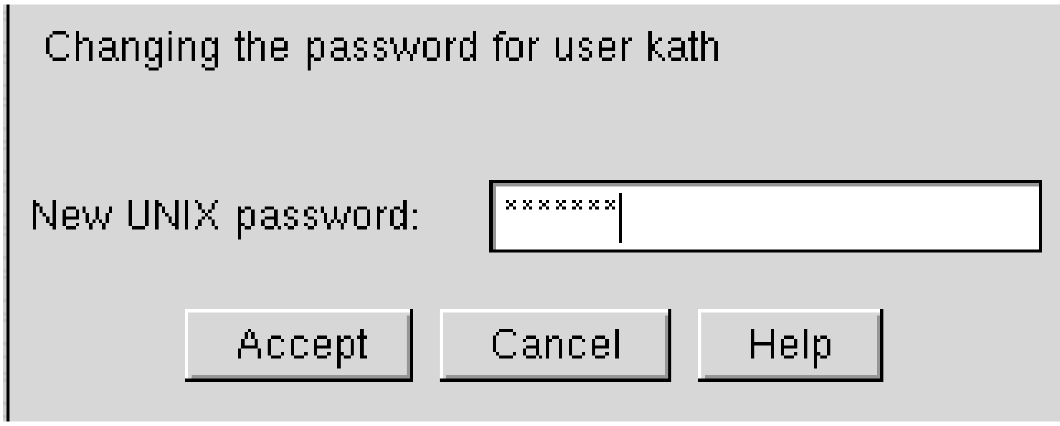
Klicken Sie auf **Bestätigen**, um die Änderungen zu übernehmen. Wenn keine Änderungen vorgenommen werden sollen, klicken Sie auf **Abbrechen**. Damit wird sichergestellt, dass keine Änderungen übernommen werden.

3.1.7 Ändern eines Benutzerpassworts

- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts**. Das Register **Benutzeraccounts** erscheint (siehe Abbildung 3–4, *Bildschirm Benutzeraccounts*).
- Je nach den ausgewählten Einstellungen im Bildschirm **Control** => **Features**, wird ein Filterbildschirm eingeblendet. Klicken Sie auf `Bestätigen` , ohne irgendwelche Parameter zu ändern, wenn Sie die vollständige Liste anzeigen lassen wollen. Um genauere Informationen über die verschiedenen Filter zu erhalten, klicken Sie im Bildschirm **Filtereinstellungen** auf den Button `Hilfe`.
- Klicken Sie auf den Account, dessen Passwort Sie ändern möchten. Der Bildschirm **Benutzerinformationen** wird geöffnet.
- Klicken Sie im unteren Bereich des Bildschirms auf **Passwort**.

linuxconf fordert Sie auf, ein neues Passwort einzugeben. Im Feld `Retype new UNIX password` muss das Passwort nochmals eingegeben werden. Hierdurch soll eine Falscheingabe des Passworts verhindert werden. Hinweise zur Wahl eines Passworts finden Sie in Abschnitt 3.1.5, *Hinzufügen eines Benutzeraccounts*. Wenn keine Passwortänderung vorgenommen werden soll, klicken Sie auf `Abbrechen`. Wenn Sie das Passwort eingegeben haben, klicken Sie auf `Bestätigen`.

Abbildung 3–6 Bildschirm Ändere Passwort



3.1.8 Ändern des Root-Passworts

Zur Gewährleistung der Sicherheit beim Root-Zugriff verlangt linuxconf von Ihnen die Bestätigung, dass Sie gegenwärtig Zugriff auf den Root-Account haben.

- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Root-Passwort wechseln**.

Sie müssen zuerst das aktuelle Root-Passwort eingeben, damit das System überprüfen kann, ob Sie Zugriff auf den Root-Account haben.

Nachdem Sie das aktuelle Root-Passwort eingegeben haben, werden Sie nach einem neuen Passwort gefragt. Geben Sie das Passwort im Feld **Bestätigung** erneut ein. Hierdurch soll eine Falscheingabe des Passworts verhindert werden. Anleitungen zur Wahl eines Passworts finden Sie in Abschnitt 3.1.5, *Hinzufügen eines Benutzeraccounts*. Wählen Sie ein sicheres Passwort! Wenn Sie das Root-Passwort beibehalten möchten, wählen Sie **Abbrechen** aus. Wenn Sie das Passwort eingegeben haben, klicken Sie auf **Bestätigen**.

3.1.9 Deaktivieren eines Benutzeraccounts

Das Deaktivieren eines Benutzeraccounts ist dem Löschen vorzuziehen, es sei denn, Sie benötigen den Speicherplatz, oder Sie sind sicher, dass die Benutzerdaten in Zukunft nicht mehr benötigt werden. Wenn ein Benutzeraccount deaktiviert ist, kann sich der betreffende Benutzer nicht am System anmelden.

- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts.**
- Wählen Sie einen Account aus.
- Deaktivieren Sie das Kontrollkästchen `Der Account wurde aktiviert`. Klicken Sie im unteren Bereich des Bildschirms auf den Button `Bestätigen`.

Damit ist der Account deaktiviert und kann später in ähnlicher Weise wieder aktiviert werden.

3.1.10 Aktivieren eines Benutzeraccounts

Standardmäßig sind alle neu erstellten Benutzeraccounts aktiviert. Falls erforderlich, können Accounts mit linuxconf aktiviert werden.

Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts**. Wählen Sie einen Account aus. Aktivieren Sie das Kontrollkästchen **Der Account wurde aktiviert.**

3.1.11 Löschen eines Benutzeraccounts

Bitte beachten

Es gibt verschiedene Optionen, bei denen die mit Accounts verbundenen Dateien erhalten bleiben. Einmal gelöschte Dateien sind jedoch verloren und praktisch nicht wiederherstellbar. Daher Vorsicht beim Umgang mit dieser Option!

Um einen Account zu löschen, sind die folgenden Schritte auszuführen:

- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts.**

- Klicken Sie im Bildschirm **Benutzeraccounts** (siehe Abbildung 3–4, *Bildschirm Benutzeraccounts*) auf den Account, der gelöscht werden soll.
- Klicken Sie im unteren Bereich des Bildschirms **Benutzerinformation** auf **Löschen**, um den Account zu löschen.

linuxconf präsentiert Ihnen nun eine Liste mit Optionen.

Abbildung 3–7 Bildschirm Lösche Account

Die Standardoption ist die Archivierung der Accountdaten. Die Archivierungsoption bewirkt Folgendes:

1. Entfernung des Benutzers aus der Liste der Benutzeraccounts.
2. Archivierung aller Dateien im Home-Verzeichnis des Benutzers (mit Komprimierung durch tar und gzip) und Speichern der Archivdatei im Verzeichnis `/default_home_directory/oldaccounts`. Für einen Account mit dem Namen *`benutzeraccount`* würde sich etwa folgender Dateiname ergeben:

```
benutzeraccount-2000-01-10-497.tar.gz
```

Das Datum gibt an, wann der Account gelöscht wurde. Die nachfolgende Zahl ist die ID des Prozesses, der die Löschung vorgenommen hat. Wenn Sie zum ersten Mal mit dieser Option einen Benutzeraccount löschen, wird das Verzeichnis `oldaccounts` automatisch in dem Verzeichnis erstellt, in dem alle Ihre Benutzerverzeichnisse liegen.

3. Dateien, die nicht im Home-Verzeichnis des Benutzers abgelegt sind, deren Eigentümer er aber ist, werden nicht gelöscht. Zum Eigentümer der Dateien wird dann die Benutzer-ID (UID) des gelöschten Accounts. Wenn Sie einen neuen Account erstellen und ihm ausdrücklich die UID eines gelöschten Accounts zuweisen, wird er zum Eigentümer aller nicht gelöschten Dateien des gelöschten Accounts.

Wenn Sie im Bildschirm **Deleting account <*Accountname*>** die Option **Delete the account's data** auswählen (siehe Abbildung 3–7, *Bildschirm Lösche Account*), werden die folgenden Schritte ausgeführt:

1. Der Benutzer wird aus der Liste der Benutzeraccounts gelöscht.
2. Das Home-Verzeichnis und dessen gesamter Inhalt werden gelöscht.

Bitte beachten

Dateien, die nicht im Home-Verzeichnis des Benutzers abgelegt sind, deren Eigentümer er aber ist, werden nicht gelöscht. Eigentümer ist weiterhin die Benutzer-ID (UID) des Accounts. Wenn Sie einen neuen Account erstellen und ihm ausdrücklich die UID eines gelöschten Accounts zuweisen, wird er zum Eigentümer aller "verwaisten" Dateien des gelöschten Accounts.

Wenn Sie im Bildschirm **Deleting account <*Accountname*>** die Option **Leave the account's data in place** auswählen (siehe Abbildung 3–7, *Bildschirm Lösche Account*) werden die folgenden Schritte ausgeführt:

1. Der Benutzer wird aus der Liste der Benutzeraccounts gelöscht.

2. Das Home-Verzeichnis des Benutzers (und alle enthaltenen Dateien) bleiben erhalten.

Bitte beachten

Dateien und Verzeichnisse, deren Eigentümer die User-ID (UID) des gelöschten Accounts ist, werden nicht gelöscht. Wenn Sie einen neuen Account erstellen und ihm ausdrücklich die UID eines gelöschten Accounts zuweisen, wird es zum Eigentümer aller "verwaisten" Dateien des gelöschten Accounts.

3.1.12 Gruppen

Jeder Benutzer gehört mindestens einer Gruppe an. So wie jede Datei einen bestimmten Eigentümer hat, gehört jede Datei auch zu einer bestimmten Gruppe. Diese Gruppe kann nur dem Eigentümer der Datei zugeordnet sein, kann aber z.B. auch für alle Benutzer freigegeben sein. Einer Gruppe können Lese-, Schreib- oder Ausführrechte für eine Datei zugewiesen werden. Die Rechte des Benutzers werden davon nicht berührt. So kann z.B. der Eigentümer einer Datei auf diese schreibend zugreifen, während andere Gruppenmitglieder diese möglicherweise nur lesen können.

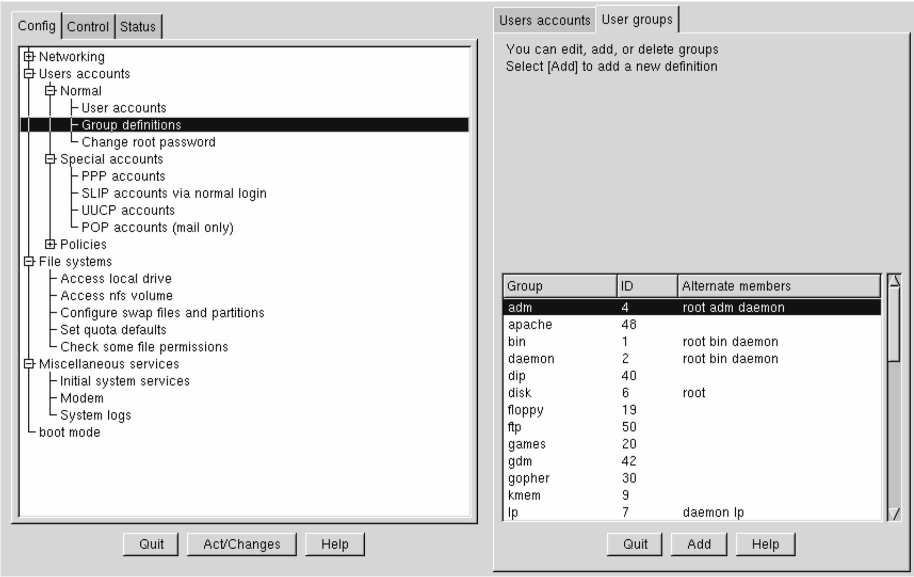
Erstellen einer Gruppe

Zum Erstellen einer neuen Gruppe gehen Sie wie folgt vor:

- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Gruppendefinitionen.**

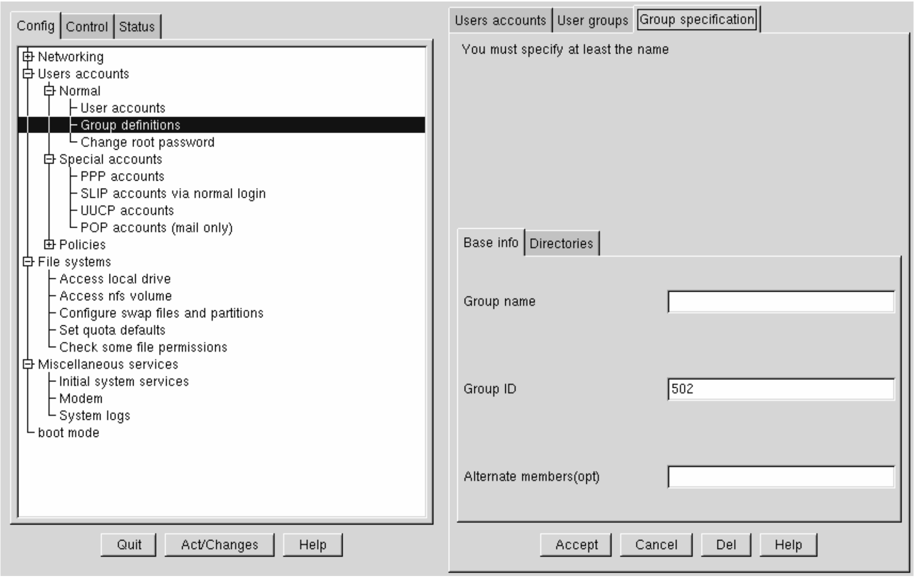
Je nach den Einstellungen in **System** => **Filter** kann es sein, dass ein Filterbildschirm angezeigt wird. Geben Sie entweder einen Filter an, oder klicken Sie auf **Bestätigen**, um den Filter zu umgehen.

Abbildung 3–8 Bildschirm Benutzergruppen



Klicken Sie im unteren Bereich des Bildschirms **Benutzergruppen** auf `Neu`.

Abbildung 3–9 Bildschirm Gruppenspezifikation



Geben Sie einen Gruppennamen ein. Die Mitglieder dieser Gruppe können Sie im Feld **Alternate members** angeben. Innerhalb der Liste müssen die Namen der Benutzer durch Leerzeichen voneinander getrennt sein. Lassen Sie das Feld **Gruppenname** leer, damit das System Ihrer neuen Gruppe eine **Gruppen-ID** (GID) zuweist. Klicken Sie abschließend auf `Bestätigen`. Die Gruppe wird erstellt.

Löschen einer Gruppe

Gehen Sie zum Löschen einer Gruppe wie folgt vor:

- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Gruppendefinitionen.**

  Je nach den Einstellungen in **System** => **Filter** kann es sein, dass ein Filterbildschirm angezeigt wird. Mit dem Filter können Sie die Anzahl der angezeigten Gruppen durch Angabe eines Präfixes einschränken.

- Klicken Sie nach Angabe eines Präfixes (oder auch ohne Angabe eines Präfixes) im unteren Bereich des Bildschirms auf `Bestätigen`.

- Klicken Sie im Bildschirm **Benutzergruppen** (siehe Abbildung 3–8, *Bildschirm Benutzergruppen*) auf die Gruppe, die gelöscht werden soll.
- Der Bildschirm **Gruppenspezifikation** erscheint (siehe Abbildung 3–9, *Bildschirm Gruppenspezifikation*).
- Klicken Sie auf `Löschen`, um die Gruppe zu löschen. linuxconf fordert Sie nun auf, den Löschvorgang zu bestätigen. Klicken Sie auf **Ja**, um die Gruppe zu löschen.

Die Dateien der Gruppe werden nicht gelöscht, und ihre jeweiligen Eigentümer haben weiterhin exklusive Rechte für sie. Der Gruppenname wird durch die ID der gelöschten Gruppe ersetzt. Mit dem Befehl `chgrp` können die Dateien einer neuen Gruppe zugeteilt werden. Weitere Informationen über `chgrp` erhalten Sie durch Eingabe von `info chgrp` oder `man chgrp` am Shell Prompt. Wenn bei der Erstellung einer neuen Gruppe die ID einer gelöschten Gruppe angegeben wird, erhält die neue Gruppe damit Zugriff auf die Dateien der gelöschten Gruppe. Die Nummern gelöschter Gruppen wie auch die IDs gelöschter Benutzer werden von linuxconf nicht wieder neu vergeben - Probleme wegen der Wiedervergabe von Nummern können also nicht entstehen.

Bearbeiten der Gruppenmitglieder

Es gibt zwei verschiedene Möglichkeiten, um die Liste der Benutzer, die zu einer Gruppe gehören, zu bearbeiten. Entweder Sie aktualisieren jeden einzelnen Benutzeraccount, oder Sie aktualisieren die Gruppendefinitionen. Im Allgemeinen ist letzteres der schnellste Weg. Falls mehr als nur die Gruppeninformationen zu ändern sind, macht es eventuell mehr Sinn, die einzelnen Benutzeraccounts zu aktualisieren.

Wir beginnen mit den Gruppendefinitionen.

- Starten Sie linuxconf durch Eingabe von `linuxconf` am Shell Prompt.
- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Gruppendefinitionen.**

  Je nach den Filtereinstellungen in **System** => **Eigenschaften** kann es sein, dass ein Filterbildschirm angezeigt wird. Schränken Sie mit dem Filter die angezeigten Einträge ein, oder klicken Sie auf **Bestätigen**, um den Filter zu umgehen.

- Klicken Sie auf die Gruppe, die bearbeitet werden soll. Der Bildschirm `Gruppenspezifikation` wird geöffnet (siehe Abbildung 3–9, *Bildschirm Gruppenspezifikation*).
- Sie können nun im Feld **Weitere Benutzer (opt.)** neue Benutzer hinzufügen oder löschen. Achten Sie darauf, dass die Benutzernamen durch ein Leerzeichen getrennt sind.
- Klicken Sie im unteren Bereich des Bildschirms auf `Bestätigen`.

Jetzt werden alle Benutzeraccounts automatisch aktualisiert. Dabei wird die Gruppe im Feld **Zusätzliche Gruppen** angezeigt, wenn sie hinzugefügt wurde, bzw. nicht mehr angezeigt, wenn sie entfernt wurde.

Gruppen können auch durch Bearbeitung der einzelnen Benutzeraccounts hinzugefügt oder entfernt werden.

- Starten Sie linuxconf durch Eingabe von `linuxconf` am Shell Prompt.
- Öffnen Sie **Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts**.

  Je nach den Einstellungen in **System** => **Eigenschaften** kann es sein, dass ein Filterbildschirm angezeigt wird. Schränken Sie mit dem Filter die angezeigten Einträge ein, oder klicken Sie auf **Bestätigen**, um den Filter zu umgehen.
- Klicken Sie im Bildschirm **Benutzeraccounts** (siehe Abbildung 3–4, *Bildschirm Benutzeraccounts*) auf einen Benutzer, der aktualisiert werden soll. Der Bildschirm **Benutzerinformation** wird geöffnet.
- Ändern Sie das Feld **Zusätzliche Gruppen** entsprechend. Die Gruppen müssen durch ein Leerzeichen getrennt sein.
- Klicken Sie im unteren Bereich des Bildschirms auf `Bestätigen`, wenn Sie alle Änderungen vorgenommen haben.

Hierdurch werden die Gruppendefinitionen automatisch aktualisiert. Wiederholen Sie diesen Vorgang für jeden Benutzer.

3.1.13 Dateisysteme

Ein Dateisystem besteht aus Dateien und Verzeichnissen, die alle von einem einzigen Verzeichnis ausgehen, dem Root-Verzeichnis. Das Root-Verzeichnis kann eine beliebige Anzahl von Dateien und anderen Verzeichnissen enthalten, wobei Verzeichnisse wiederum Verzeichnisse enthalten können. Meistens sieht das Dateisystem wie ein umgekehrter Baum aus: die Verzeichnisse sind die Äste, die Dateien die Blätter. Dateisysteme gibt es auf Massenspeichergeräten, wie Disketten-, Festplatten- und CD-ROM-Laufwerken.

Zum Beispiel wird ein Diskettenlaufwerk auf einem DOS- oder Windows-Computer üblicherweise mit `A:\` bezeichnet. Damit wird sowohl das Laufwerk (`A:`) als auch das Root-Verzeichnis auf diesem Laufwerk (\) beschrieben. Die primäre Festplatte wird normalerweise als Laufwerk "C" bezeichnet, weil die Laufwerksangabe für die primäre Festplatte `C:` ist. Das Root-Verzeichnis auf Laufwerk C wird mit `C:\` angegeben.

Entsprechend gibt es zwei Dateisysteme — eines auf `A:` und eines auf `C:`. Wenn Sie eine *beliebige* Datei auf einem DOS/Windows-Dateisystem angeben möchten, müssen Sie explizit das Gerät angeben, auf dem die Datei gespeichert ist. Anderenfalls geht das Betriebssystem davon aus, dass sich die Datei auf dem Standardlaufwerk des Systems befindet (daher der Prompt C von DOS — C ist das Standardlaufwerk in einem System mit einer Festplatte).

Unter Linux ist es möglich, Dateisysteme auf mehreren Massenspeichern zu einem einzigen größeren Dateisystem zusammenzufassen. Das wird dadurch erreicht, dass das Dateisystem eines Laufwerks "unter" einem Verzeichnis eines anderen Laufwerks angeordnet wird. Während das Root-Verzeichnis eines Diskettenlaufwerks auf einem DOS-Computer in der Regel als `A:\` bezeichnet wird, kann auf dasselbe Laufwerk auf einem Linux-System z.B. mit `/mnt/floppy` zugegriffen werden.

Dieser Vorgang des Zusammenführens von Dateisystemen wird als **mounten** bezeichnet. Wenn ein Gerät gemountet ist, können die Systembenutzer darauf zugreifen. Das Verzeichnis, "unter" dem auf gemountete Laufwerke zugegriffen werden kann, heißt **Mount-Point**. Im Beispiel des vorangehenden Absatzes war `/mnt/floppy` der Mount-Point des Diskettenlaufwerks. Beachten Sie, dass es keine Beschränkungen (außer den allgemeinen Konventionen) hinsichtlich der Bezeichnung von Mount-Points gibt. Wir hätten das Diskettenlaufwerk ebenso gut auf `/long/path/to/the/floppy/drive` mounten können.

Beachten Sie, dass alle Dateien und Verzeichnisse eines Laufwerks relativ zu dessen Mount-Point angeordnet sind. Dazu das folgende Beispiel:

- Linux-System
  - `/` — System-Root-Verzeichnis
  - `/foo` — Mount-Point für die CD-ROM

- CD-ROM:
  - `/` — Root-Verzeichnis der CD-ROM
  - `/images` — Ein Verzeichnis der Images auf der CD-ROM
  - `/images/old` — Ein Verzeichnis der alten Images

Mit den oben beschriebenen einzelnen Dateisystemen und der auf `/foo` gemounteten CD-ROM ergibt sich die folgende Verzeichnisstruktur:

- Linux-System (mit gemounteter CD-ROM)
  - `/` — System-Root-Verzeichnis
  - `/foo` — Root-Verzeichnis der CD-ROM
  - `/foo/images` — Ein Verzeichnis der Images auf der CD-ROM
  - `/foo/images/old` — Ein Verzeichnis der alten Images

Um ein Dateisystem mounten zu können, müssen Sie als Root angemeldet sein. Wenn das nicht der Fall ist, können Sie das mit dem Befehl `su` nachholen. Geben Sie dazu `su` und anschließend das Root-Passwort am Shell Prompt ein. Wenn Sie als Root angemeldet sind, geben Sie `mount` und dahinter das Laufwerk und den Mount-Point ein. Um z.B. das erste Diskettenlaufwerk auf `/mnt/floppy` zu mounten, müssen Sie `mount /dev/fd0 /mnt/floppy` eingeben.

Während des Installationsvorganges erstellt Red Hat Linux die Datei `/etc/fstab`. Sie enthält Informationen über die Laufwerke und ihre entsprechenden Mount-Points.

Der Vorteil dieser Datei besteht darin, dass mount-Befehle abgekürzt werden können. Außerdem wird in der Datei festgelegt, welche Dateisysteme beim Systemstart automatisch gemountet werden sollen.

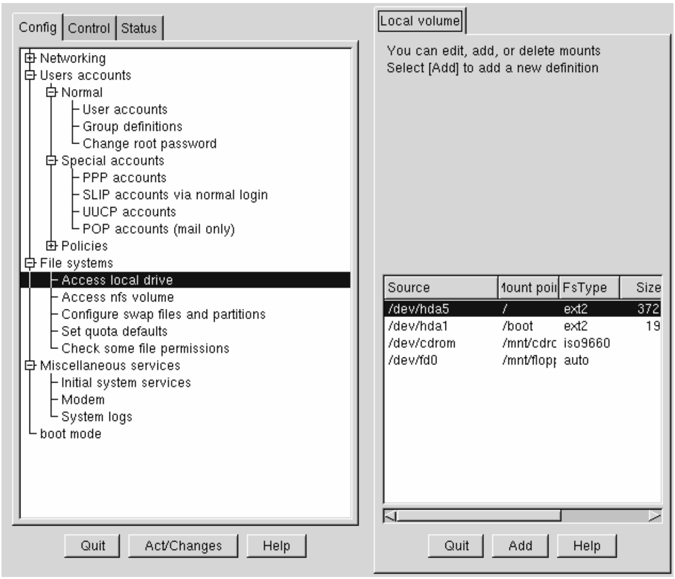
Dank der in `/etc/fstab` abgelegten Informationen reicht es aus, wenn Sie nach `mount` entweder nur den Mount-Point oder nur das Laufwerk angeben. Der Befehl `mount` durchsucht dann `/etc/fstab` nach den ergänzenden Informationen. Die Datei kann sowohl von Hand als auch mit linuxconf bearbeitet werden.

Übersicht über das aktuelle Dateisystem

Zuerst möchten wir uns eine Übersicht über ihre aktuelle Verzeichnisstruktur verschaffen.

- Öffnen Sie **Verwaltung** => **Dateisystem** => **Access local drive** .

Abbildung 3–10 Bildschirm Lokaler Datenträger



Bedeutung der Felder (siehe Abbildung 3–10, *Bildschirm Lokaler Datenträger*):

- **Quelle**: Die physikalische Hardware. `hd` bezeichnet eine IDE-Festplatte, `fd` ein Diskettenlaufwerk und `cdrom` in der Regel ein CD-ROM Laufwerk. Wenn Ihr System mit einem SCSI-Laufwerk ausgestattet ist, wird als Bezeichnung `sd` verwendet. Wenn mehrere Laufwerke eines Typs vorhanden sind, werden zusätzlich Buchstaben zur Bezeichnung verwendet: `hda` ist dann das erste, `hdb` das zweite IDE-Laufwerk. Teilweise erscheinen nach diesen Buchstaben noch Zahlen. Bei Festplattenlaufwerken kennzeichnen diese Zahlen die jeweilige Partition des Laufwerks, bei Diskettenlaufwerken gibt diese Zahl das eigentliche Gerät an.
- **Mount-Point**: Diesem Ort im System wird beim Mounten das Laufwerk zugeordnet.
- **DS-Typ**: Anzeige des Dateisystemtyps. Eine standardmäßige Linux-Partition verwendet den Dateisystemtyp ext2. Der Dateisystemtyp vfat zeigt an, dass es sich um ein DOS-Dateisystem mit Unterstützung für lange Dateinamen handelt, und der Dateisystemtyp fat, dass ein DOS-Dateisystem mit herkömmlichen 8.3-Dateinamen vorliegt. Der Dateisystemtyp iso9660 zeigt an, dass es sich um ein CD-ROM-Laufwerk handelt.

Bitte beachten

Red Hat Linux 7.0 kann auf FAT32-Dateisysteme mit dem Dateisystemtyp `vfat` zugreifen.

- **Größe**: Anzeige der Größe des Dateisystems in Megabyte (M). Diese Angabe kann auch fehlen.
- **Partitionstyp**: Kennzeichnung des Dateisystems dieser Partition (Angabe kann auch fehlen).
- **Status**: Angabe, ob das Gerät gemountet ist.

Möglicherweise sind auch Dateisysteme von anderen Computern im Netzwerk verfügbar. Diese können von einem einzigen kleinen Verzeichnis bis zu einem vollständigen Datenträger reichen. Auch bei diesen Partitionen werden keine Informationen über **Größe** und **Partitionstyp** angezeigt. Weitere Informationen über NFS-Dateisysteme (falls Sie Zugriff auf solche haben sollten) finden Sie unter:

Verwaltung => **Dateisystem** => **access nfs volume**

Der Bildschirm entspricht weitgehend dem Bildschirm **Local Volume** (siehe Abbildung 3–10, *Bildschirm Lokaler Datenträger*), jedoch werden andere Informationen in die Felder eingetragen:

- **Quelle**: Der Name des Computers, der das Dateisystem bereitstellt, gefolgt vom Remote-Verzeichnis. Zum Beispiel: `foo:/var/spool/mail`, wobei `foo` der Computer ist, der das Dateisystem bereitstellt, und `/var/spool/mail` das Verzeichnis, das bereitgestellt wird.
- FsType — Immer "nfs."

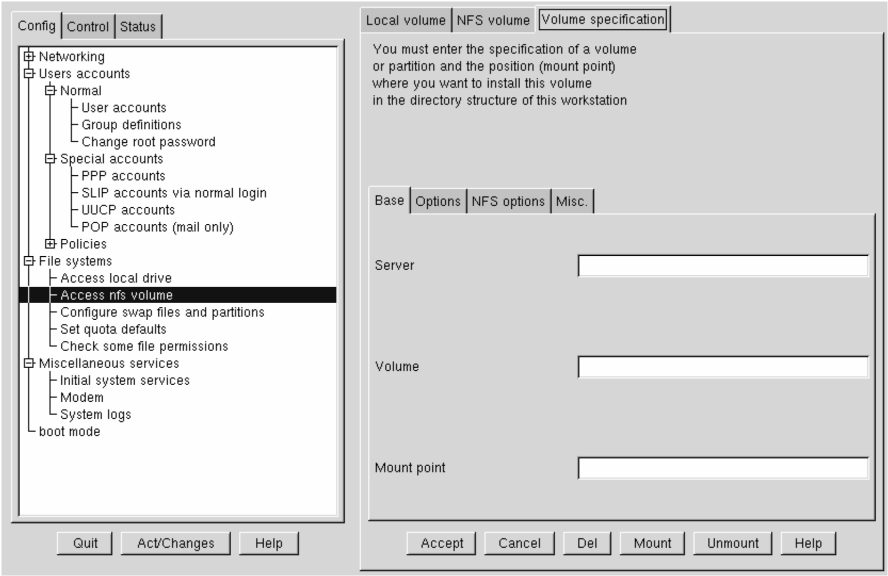
Hinzufügen von NFS-Mounts

Mit NFS (Network File System, Netzwerkdateisystem) können Teile von lokalen Computerdateisystemen für ein Netzwerk freigegeben werden. Diese Teile können von einem einzigen Verzeichnis bis hin zu Tausenden von Dateien in einer umfangreichen Verzeichnishierarchie reichen. Zum Beispiel stellt in vielen Unternehmen ein Mail-Server den lokalen Systemen der Benutzer die Mail-Dateien der einzelnen Mitarbeiter mittels NFS-Mount zur Verfügung.

Zum Hinzufügen eines NFS-Mounts gehen Sie wie folgt vor:

- Öffnen Sie **Verwaltung** => **Dateisystem** => **Access nfs volume**.
- Klicken Sie im Bildschirm **NFS-Datenträger** auf `Neu`.

Abbildung 3–11 Bildschirm Datenträgerspezifikation



Wichtig für Sie sind die drei Felder im Register **Base** (siehe Abbildung 3–11, *Bildschirm Datenträgerspezifikation*).

- **Server**: Der Name des Rechners, der das gewünschte Dateisystem enthält, z. B. foo.bar.com.
- **Volume**: Das Dateisystem, das hinzugefügt werden soll, z. B. `/var/spool/mail`.
- **Mount-Point**: Der Ort im System, von dem aus die Remote-Datei erreichbar sein soll, z.B. `/mnt/mail`.

Weitere Angaben sind nicht erforderlich, um einen Mount zu erstellen. linuxconf aktualisiert dann Ihre Datei `/etc/fstab` entsprechend. Bitte lesen Sie in der Hilfedatei die Informationen über den Bildschirm **Datenträgerspezifikation** sowie die man-Seite zu `mount`, falls zusätzliche Einzelheiten geklärt werden müssen.

Wenn Sie alle Informationen eingegeben haben, klicken Sie auf `Bestätigen`.

3.1.14 Konfigurieren des Netzwerks mit linuxconf

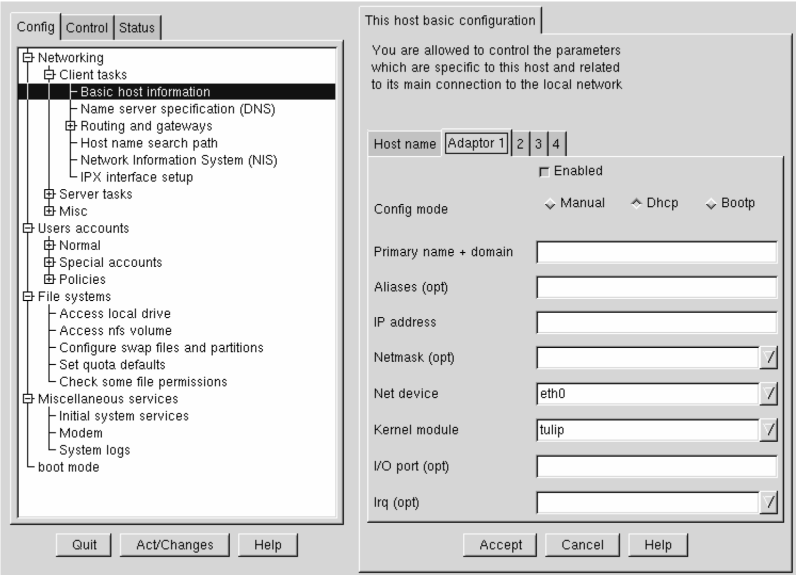
Für den Netzwerkanschluss muss zunächst Klarheit darüber bestehen, ob Ihr Computer an ein LAN (Local Area Network, z.B. mehrere Computer in einem Büro), angeschlossen werden soll oder an ein WAN (Wide Area Network, z.B. das Internet). Bevor Sie fortfahren, muss die verwendete Hardware und die Art der Netzwerkverbindung bekannt sein. Wenn Sie sich in einen anderen Computer per Telefonleitung einwählen möchten, muss zuerst das Modem installiert und die Verkabelung richtig eingerichtet werden. Wenn Sie eine Netzwerkkarte verwenden, muss diese ordnungsgemäß installiert sein, und die Netzwerkkabel müssen richtig verbunden werden. Die Netzwerkkonfiguration allein ist nutzlos, wenn die Telefonleitungen oder Netzwerkkabel nicht richtig verbunden sind.

Netzwerkverbindungen

Die Einrichtung einer Ethernet-Netzwerkverbindung erfordert eine völlig andere Vorgehensweise als die Einrichtung einer Wählverbindung. Netzwerkverbindungen zu Token Ring- und Arcnet-Netzwerken werden in ähnlicher Weise eingerichtet. An dieser Stelle wird nur die Einrichtung einer Ethernet-Netzwerkverbindung beschrieben.

- Voraussetzung ist, dass auf Ihrem Computer eine Ethernet-Netzwerkkarte installiert ist.
- Starten Sie linuxconf durch Eingabe von `linuxconf` am Shell Prompt.
- Öffnen Sie **Verwaltung** => **Netzwerk** => **Grundeinstellungen** => **Allgemeines**. Im Register `Host name` sollte standardmäßig ein Rechnername eingetragen sein, es sei denn, Sie haben Ihr Netzwerk nicht während des Installationsverfahrens eingerichtet. Falls dies nicht der Fall ist, tragen Sie den Rechnernamen ein. Er muss in der Form `localhost.localdomain` angegeben werden. Klicken Sie dann auf das Register `Adapter 1`.

Abbildung 3–12 Adapter 1



Dieser Bildschirm enthält an oberster Stelle ein Kontrollkästchen, das anzeigt, ob dieser Adapter aktiviert oder deaktiviert ist. Aktivieren Sie das Kontrollkästchen, wenn Sie diesen Adapter verwenden möchten. Darunter können Sie den **Konfigurationsmodus** wählen. **Manuell** bedeutet, Sie geben alle Informationen selbst ein. **Dhcp** und **Bootp** rufen die notwendigen Netzwerkkonfigurationsinformationen von einem DHCP- oder BOOTP-Remote-Server ab. Wenden Sie sich an Ihren Systemadministrator, wenn Sie sich nicht sicher sind, welche dieser Optionen die richtige ist.

Obligatorische Felder für DHCP bzw. BOOTP:

- **Net device** — Typ der verwendeten Netzwerkkarte. Tragen Sie zum Beispiel eth0 ein, wenn Sie die erste Ethernet-Karte verwenden möchten.
- **Kernel module** — Das korrekte Modul basierend auf Ihrer Netzwerkkarte. Weitere Informationen finden Sie in der unten aufgeführten Liste.

Für die Konfiguration von DHCP und bootp genügt es, wenn Sie das **Netzwerkgerät** und das **Kernel Modul** angeben. Das **Netzwerkgerät** können Sie aus einer Liste auswählen. Das Präfix **eth** bezeichnet Ethernet-Karten, **arc** bezeichnet Arcnet-Karten, und **tr** bezeichnet Token Ring-Karten. Eine vollständige Liste von Netzwerkkarten und den entsprechenden Modulen finden Sie in Anhang A, *Allgemeine Parameter und Module*. Die aktuelle Liste finden Sie auf unserer Website:

`http://www.redhat.com/support/hardware`

Die Netzmaske wird auf einen Standardwert gesetzt. Hier müssen Sie eventuell Änderungen vornehmen, je nachdem, um welche Art von Netzwerk es sich handelt. Wenn es sich um eine Verbindung mit einem Internet-Diensteanbieter handelt, sollten Sie dort nach den entsprechenden Informationen fragen. Wahrscheinlich wird 255.255.255.0 verwendet.

Obligatorische Felder für manuelle Konfiguration:

- **Primary name + domain** — Der primäre Name ist der Name Ihres Computers, während die Domäne Ihr Netzwerk angibt, z.B. `foo.bar.com`. `foo` ist der Rechnername und `bar.com` die Domäne.
- **IP address** — Die Adresse des Rechners wird im folgenden Format angegeben *x.x.x.x.*, z. B. 192.168.0.13.
- **Net device** — Typ der verwendeten Netzwerkkarte; Tragen Sie eth0 ein, wenn Sie die erste Ethernet-Karte verwenden möchten.
- **Kernel module** — Das korrekte Modul entsprechend Ihrer Netzwerkkarte.

Die Angaben zu Netzwerkgeräten und Kernel-Modulen haben wir bereits weiter oben beschrieben. Rechnername, Domänenname und IP-Adresse hängen davon ab, ob Sie Ihren Computer mit einem bestehenden Netzwerk verbinden oder ob Sie ein neues Netzwerk aufbauen möchten. Wenn Sie Ihren Computer mit einem bestehenden Netzwerk verbinden möchten, fragen Sie Ihren Netzwerkadministrator, welche Angaben zu machen sind. Die Anbindung eines Netzwerks an das Internet geht über den Rahmen dieses Buches hinaus. Als Einstieg in dieses Thema empfehlen wir folgendes Buch:

TCP/IP Network Administration, 2nd Edition, von Craig Hunt (O'Reilly and Associates).

Wenn Sie ein privates Netzwerk einrichten möchten, das *nicht* mit dem Internet verbunden werden soll, können Sie beliebige Rechnernamen und Domänennamen wählen. Die IP-Adressen können Sie innerhalb bestimmter Bereiche wählen (siehe Tabelle 3–1, *Adressen und Beispiele*).

Tabelle 3–1 Adressen und Beispiele

Verfügbare Adressen	Beispiele
10.0.0.0 - 10.255.255.255	10.5.12.14
172.16.0.0 - 172.31.255.255	172.16.9.1, 172.28.2.5
192.168.0.0 - 192.168.255.25	192.168.0.13

Die oben angegebenen Zahlenbereiche entsprechen jeweils Netzwerken der Klassen A, B und C. Die Klassen beschreiben sowohl die Anzahl der verfügbaren IP-Adressen als auch den jeweiligen Zahlenbereich. Die angegebenen Zahlenbereiche sind für private Netzwerke reserviert worden.

Bitte beachten

Für eine Verbindung mit dem Internet sollten Sie diese IP-Adressen nicht verwenden, da 192.168.0.* und 192.168.255.* als private IP-Adressen festgelegt sind. Wenn Sie Ihr Netzwerk jetzt oder später an das Internet anbinden möchten, sollten Sie sich besser nicht-private IP-Adressen zuweisen lassen.

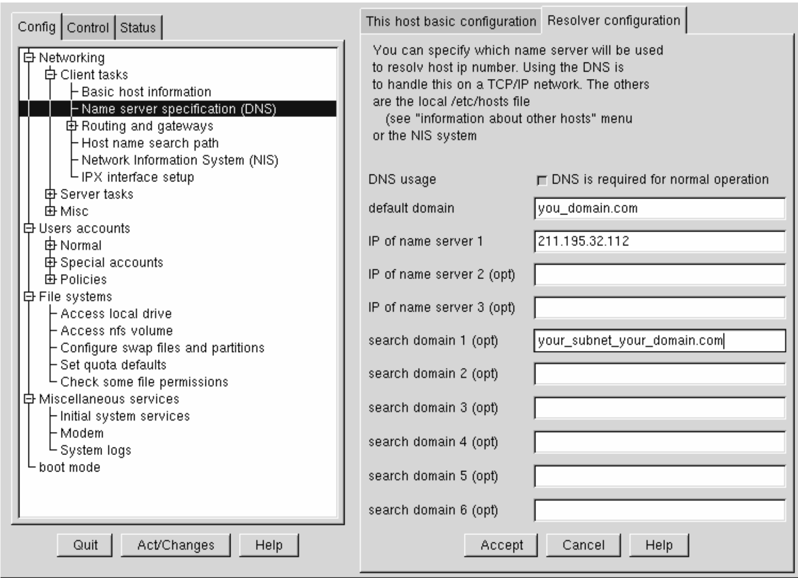
Angeben des Nameservers

Um eine Netzwerkverbindung einzurichten, benötigen Sie auch einen Nameserver und eine Standarddomäne. Der Nameserver setzt Rechnernamen, z.B. `private.network.com`, in die entsprechende IP-Adresse um, z.B. `192.168.7.3`.

Die Standarddomäne gibt an, wo der Computer suchen muss, wenn kein vollständiger Rechnername angegeben wurde. Vollständiger Rechnername bedeutet, dass die komplette Adresse angegeben wird. `foo.redhat.com` ist z.B. der vollständige Rechnername, während `foo` nur der einfache Rechnername ist. Wenn Sie `redhat.com` als Ihre Standarddomäne angegeben haben, reicht der einfache Rechnername aus, um eine Verbindung herzustellen. Zum Beispiel würde `ftp foo` genügen, wenn Ihre Suchdomäne `redhat.com` ist. Dagegen müssten Sie `ftp foo.redhat.com` eingeben, wenn Ihre Suchdömane anders hieße.

Öffnen Sie **Verwaltung** => **Netzwerk** => **Grundeinstellungen** => **Nameserver (DNS)**.

Abbildung 3–13 Bildschirm Konfiguration von Nameserver und Suchdomänen



Wenn mehr als ein Nameserver angegeben ist, wird den Nameservern jeweils ein Rang zugeordnet, der der Reihenfolge entspricht, in der auf sie zugegriffen wird. Oft werden sie dann als erster, zweiter, dritter usw. Nameserver bezeichnet. Für Nameserver müssen Sie eine IP-Adresse (keinen Namen) eintragen, da Ihr Computer erst dann Namen in IP-Adressen umsetzen kann, wenn er eine Verbindung mit einem Nameserver hergestellt hat.

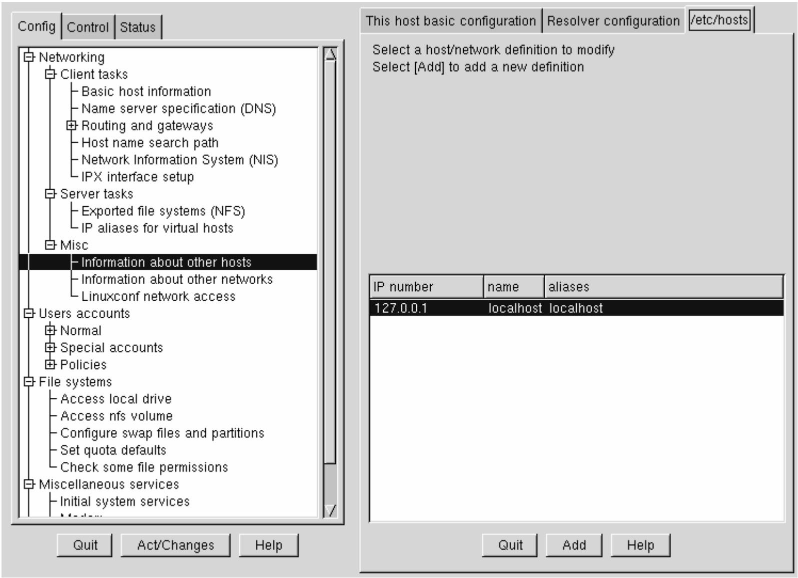
Zusätzlich zur Standarddomäne können Sie auch Suchdomänen angeben. Suchdomänen arbeiten nach einem anderen Prinzip als Nameserver. Sie werden zwar wie die Nameserver entsprechend ihrer Reihenfolge nacheinander angesprochen, haben jedoch Vorrang vor der Standarddomäne. Bedenken Sie dies, wenn Sie Suchdomänen angeben. Suchdomänen werden nur selten verwendet.

Nun noch zum DNS-Kontrollkästchen. In einem kleinen, privaten Netzwerk ohne Internet-Anbindung können Sie zur Namensauflösung die Datei `/etc/hosts` verwenden und diese jeweils zwischen den Computern synchronisieren. Je mehr Computer Sie hinzufügen, desto komplexer wird die Synchronisierung. Schließlich ist es einfacher, DNS auf einem einzelnen Rechner auszuführen als die Dateien `/etc/hosts` zu synchronisieren.

Anstelle von DNS ist auch die Verwendung von NIS in Ihrem Netzwerk möglich. DNS und NIS können übrigens auch nebeneinander eingesetzt werden. Zusammenfassend lässt sich sagen: DNS is wahrscheinlich die beste Lösung für Sie, es sei denn, es gibt einen guten Grund, `/etc/hosts` oder NIS zu verwenden.

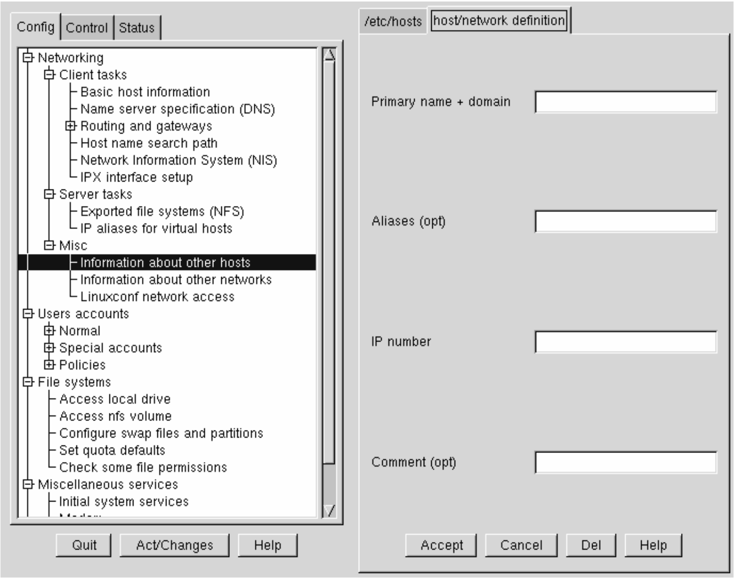
Sie können mit Linuxconf Einträge in `/etc/hosts` hinzufügen, bearbeiten und löschen. Öffnen Sie **Verwaltung** => **Netzwerk** => **Verschiedenes** => **Informationen über andere Rechner**.

Abbildung 3–14 `/etc/hosts`-Bildschirm



Klicken Sie auf einen Eintrag, um ihn zu bearbeiten oder zu löschen. Klicken Sie im unteren Bereich des Bildschirms **Rechner/Netzwerkdefinition** auf **Löschen**, um den Eintrag zu löschen.

Abbildung 3–15 Bildschirm Rechner/Netzwerkdefinition



Sie können die Informationen direkt im Bildschirm ändern. Wenn Sie einen neuen Eintrag hinzufügen möchten, klicken Sie im unteren Bereich des Bildschirms **/etc/hosts** auf `Neu`. Der Bildschirm **Rechner/Netzwerkdefinition** wird geöffnet.

Obligatorische Felder:

- **Primary name + domain** — Der primäre Name gibt den Namen des Computers an, während die Domäne die Bezeichnung des Netzwerks angibt, in das der Computer eingebunden ist. In `foo.bar.com` ist z.B. `foo` der Rechnername und `bar.com` die Domäne.
- **IP number** — Auch als IP-Adresse bezeichnet. Dies ist die Adresse des Computers im Format *x .x. x.x*, z. B. 192.168.0.13.

Optionale Felder:

- **Aliases** — Eine Kurzbezeichnung des vollständigen Domänennamens. Hier wird oft der Rechnername verwendet. Wenn der vollständige Domänenname z.B. foo.bar.com ist, könnten Sie foo als Alias wählen.
- **Comment** — Eine Anmerkung zum Rechner, z.B. "Remote-Nameserver".

Klicken Sie auf `Bestätigen`, wenn Sie alles eingegeben haben.

3.1.15 So finden Sie sich zurecht mit linuxconf

Diese Tabelle gibt Ihnen einen Kurzüberblick über dieses Kapitel. Leider kann es keine umfassende Referenz für linuxconf sein, das über viel mehr Funktionen verfügt, als in dieser Dokumentation beschrieben werden kann.

Tabelle 3–2 Linuxconf Kurzüberblick

Was möchten Sie tun?	So finden Sie den richtigen Bildschirm in linuxconf
Hinzufügen/Ändern/Deaktivieren/Löschen eines Benutzeraccounts	**Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts**
Ändern eines Benutzerpassworts	**Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts**
Ändern des Root-Passworts	**Verwaltung** => **Benutzer** => **Normal** => **Root-Passwort wechseln**
Netzwerk konfigurieren	**Verwaltung** => **Netzwerk** => **Grundeinstellungen** => **Allgemeines**
Erstellen/Löschen einer Gruppe	**Verwaltung** => **Benutzer** => **Normal** => **Gruppendefinitionen**
Passwortparameter ändern	**Benutzeraccounts** => **Passwort und Accountregeln**
Deaktivieren des Menübaums	**System** => **Systemsteuerung** => **linuxconf Module**
Aktivieren des web-basierten Zugriffs auf linuxconf	**Verwaltung** => **Netzwerk** => **Verschiedenes** => **Linuxconf Netzwerkzugriff**

Was möchten Sie tun?	**So finden Sie den richtigen Bildschirm in** linuxconf
Verändern von `/etc/hosts`	**Verwaltung** => **Netzwerk** => **Verschiedenes** => **Informationen über andere Rechner**
Ändern der Gruppenmitgliedschaft	**Verwaltung** => **Benutzer** => **Normal** => **Gruppendefinitionen** oder **Verwaltung** => **Benutzer** => **Normal** => **Benutzeraccounts**
Einstellen von Filterparametern	**System** => **Eigenschaften**
Angeben eines Nameservers (DNS)	**Verwaltung** => **Netzwerk** => **Grundeinstellungen** => **Nameserver (DNS)**
Anzeigen des Dateisystems	**Verwaltung** => **Dateisystem** => **Access local drive** oder **Verwaltung** => **Dateisystem** => **Access nfs volume**

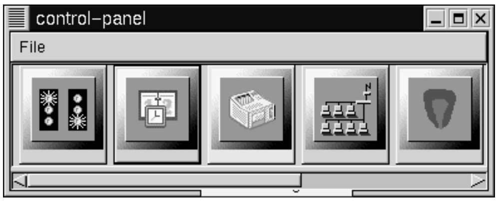
3.2 Konfigurieren des Systems mit Control Panel

Bitte beachten

Der Leistungsumfang des Control Panel wird zum großen Teil durch Linuxconf abgedeckt. Zusätzlich unterstützt linuxconf sowohl die textbasierte *als auch* die grafische Benutzeroberfläche. Eine Einführung zu Linuxconf finden Sie in Abschnitt 3.1, *Konfigurieren des Systems mit* Linuxconf.

Im Control Panel sind eine ganze Reihe von Systemadministrationstools zusammengefasst (siehe Abbildung 3–16, *Das Control Panel*). Diese Tools können Ihnen die Arbeit erleichtern, da Sie sich auf diese Weise weder Formate von Konfigurationsdateien noch Befehlszeilenoptionen merken müssen.

Abbildung 3–16 Das Control Panel



Um das Control Panel auszuführen, starten Sie das X Window System als Root durch Eingabe von `startx`. Geben Sie dann in einem XTerm `control-panel` ein. Um die Control Panel Tools ausführen zu können, müssen Sie als Root angemeldet sein. Wenn Sie als normaler Benutzer angemeldet sind und X ausführen, können Sie `su -c control-panel` eingeben. Geben Sie bei der entsprechenden Aufforderung das Root-Passwort ein. Falls Sie weitere Root-Aufgaben im System erledigen möchten, geben Sie stattdessen `su` ein. Geben Sie das Root-Passwort ein, wenn Sie dazu aufgefordert werden.

Bitte beachten

Wenn Sie X nicht als Root ausführen, müssen Sie Root möglicherweise noch den Zugriff auf den X-Server Ihres Systems einräumen. Geben Sie dazu den folgenden Befehl in einem Terminal-Fenster ein, unter dem *kein* Root-Zugriff möglich ist:

```
xhost +localhost
```

Wenn das Control Panel läuft, können Sie die Tools durch Klicken auf ein Symbol starten. Beachten Sie bitte, dass Sie zwar ohne weiteres dasselbe Programm zweimal starten können, Sie damit aber unter Umständen Schaden anrichten. Es kann sein, dass Sie auf diese Weise dieselbe Datei von zwei Orten aus zu bearbeiten versuchen und Ihre eigenen Änderungen wieder überschreiben.

Bitte beachten

Wenn Sie versehentlich eines der Tools zweimal starten, sollten Sie es sofort wieder schließen. Während die Tools ausgeführt werden, dürfen Sie außerdem keine Dateien manuell bearbeiten, die von den Control Panel Tools verwaltet werden. Dasselbe gilt für andere Programme wie Linuxconf, die eventuell Dateien ändern könnten, während die Tools ausgeführt werden.

3.2.1 Konfigurieren des Druckers

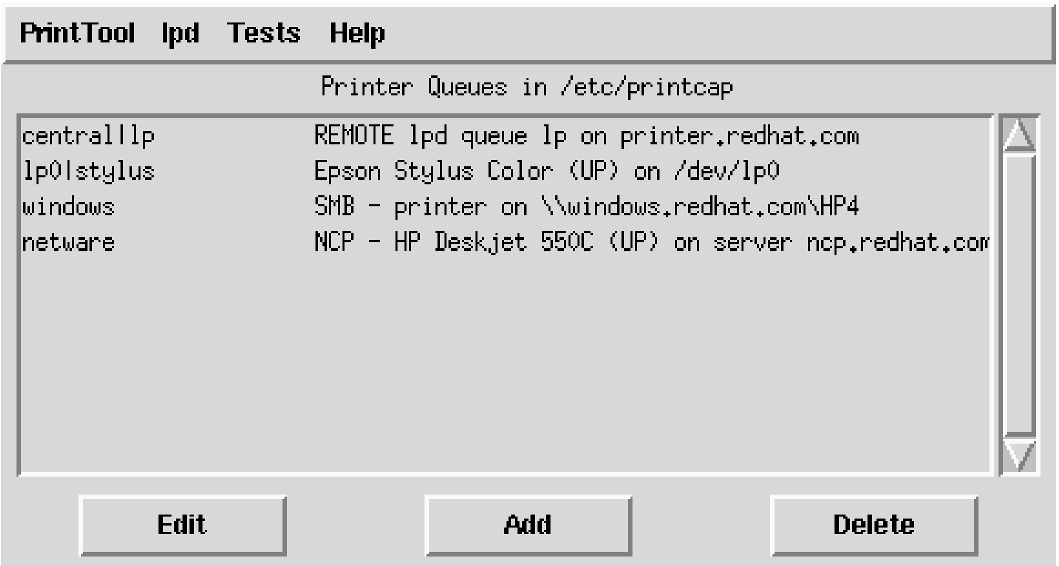
Bitte beachten Sie, dass das *Offizielle Red Hat Linux Handbuch Erste Schritte* weitere aktuelle Dokumentationen zu printtool enthält. Lesen Sie dieses Dokument, bevor Sie printtool verwenden.

Das Tool für die Druckerkonfiguration (printtool) kann verwendet werden, um die Datei `/etc/printcap`, die Druckerspoolverzeichnisse und die Druckerfilter zu bearbeiten. Mit Hilfe der Filter können Sie die verschiedensten Dateitypen ausdrucken. Hierzu gehören:

- Einfache Textdateien (ASCII)
- PostScript-Dateien
- TeX `.dvi`-Dateien
- GIF, JPEG, TIFF und weitere Graphikformate
- RPMs

Mit anderen Worten: Ganz gleich, ob Sie mit dem Befehl `lpr` eine GIF- oder eine RPM-Datei ausdrucken - der Drucker druckt es richtig aus.

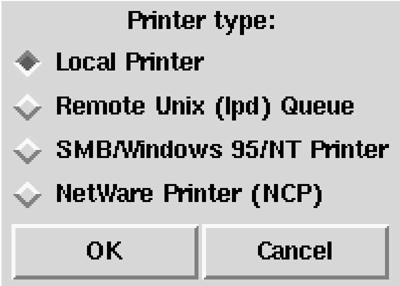
Abbildung 3–17 Das Druckertool



Wenn Sie eine neue **Druckerwarteschlange** erstellen möchten, klicken Sie auf Add. Wählen Sie dann den Typ des Druckers aus, der hinzugefügt werden soll. Mit printtool können vier verschiedene Typen von Druckerwarteschlangen konfiguriert werden:

- Lokale Druckerwarteschlangen für Drucker, die an der Druckerschnittstelle oder der seriellen Schnittstelle Ihres Red Hat Linux Systems angeschlossen sind.
- Remote-Druckerwarteschlangen sind mit einem anderen System verbunden, auf das Sie über ein TCP/IP-Netzwerk zugreifen können.
- SMB-Druckerwarteschlangen sind mit einem anderen System verbunden, das ein Netzwerk vom LAN-Manager-Typ (SMB) verwendet.
- NCP-Druckerwarteschlangen sind mit einem anderen System verbunden, das ein Novell NetWare-Netzwerk verwendet.

Abbildung 3–18 Auswählen des Druckertyps



Nachdem Sie den Druckertyp ausgewählt haben, werden Sie in einem Dialogfeld nach weiteren Angaben über die Druckerwarteschlange gefragt (siehe Abbildung 3–19, *Hinzufügen eines lokalen Druckers*). Die folgenden Angaben sind für alle Typen von Druckerwarteschlangen erforderlich:

- Queue Name — Die Bezeichung der Warteschlange. Mit Hilfe des Zeichens `|` (Pipe) können die Einträge getrennt und somit mehrere Bezeichnungen angegeben werden.
- Spool Directory — Das Verzeichnis auf einem lokalen Rechner, in dem die Dateien vor dem Druck gespeichert werden. Achten Sie darauf, dass jedes Spoolverzeichnis nur von einer Druckerwarteschlange verwendet werden darf.
- File Limit — Die maximal für einen Druckjob unterstützte Dateigröße in Kilobyte (1 KB = 1024 Byte). Tragen Sie 0 ein, wenn die Größe nicht begrenzt sein soll.
- Input Filter — Die Filter konvertieren Druckdateien in ein Format, das der Drucker unterstützt. Klicken Sie auf `Select`, um den Filter auszuwählen, der am besten zu Ihrem Drucker passt (siehe Abbildung 3–20, *Konfigurieren eines Druckerfilters*).

  Neben der Ausgabe im Graphik- oder PostScript-Format können Sie einen reinen **Text**-Drucker konfigurieren, der nur einfachen ASCII-Text ausdruckt. Die meisten Druckertreiber können ASCII-Text drucken, ohne ihn zuvor in PostScript umzuwandeln. Wählen Sie hierzu `Fast text printing`, wenn Sie den Filter konfigurieren.

Bitte beachten

Dies gilt nicht für PostScript-Drucker.

- Suppress Headers — Aktivieren Sie dieses Kontrollkästchen, wenn am Anfang eines Druckjobs keine Header-Seite ausgedruckt werden soll.

Bei **lokalen** Druckern sind zusätzlich die folgenden Angaben vorzunehmen:

- Printer Device — Normalerweise `/dev/lp1`. Das ist der Name des Ports, an den der Drucker angeschlossen ist. Serielle Drucker sind in der Regel am Port `/dev/ttyS?` angeschlossen. Beachten Sie, dass Sie serielle Parameter manuell konfigurieren müssen.

Abbildung 3–19 Hinzufügen eines lokalen Druckers

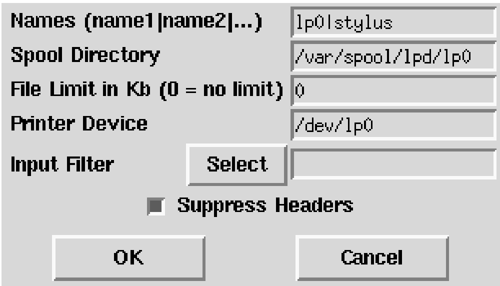
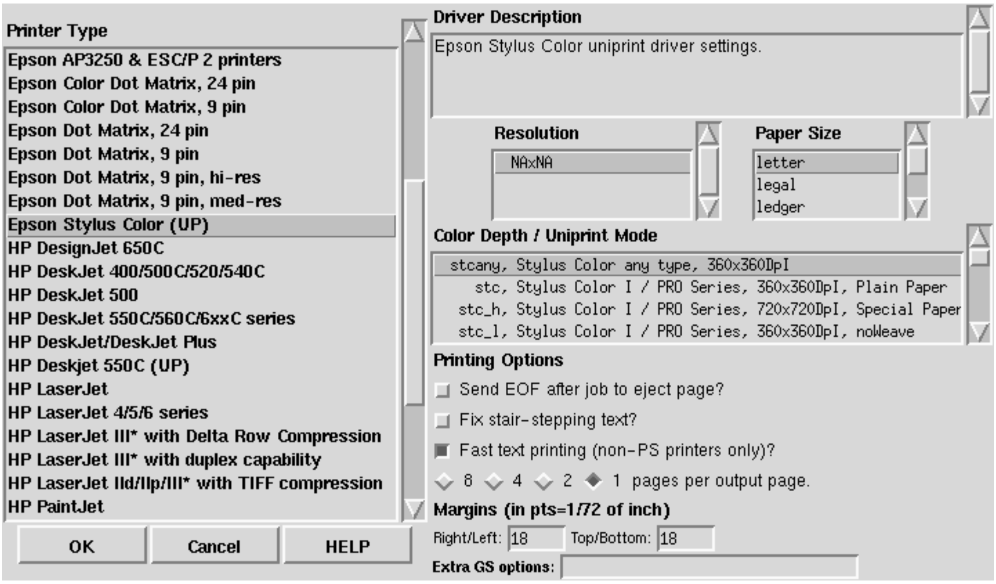


Abbildung 3–20 Konfigurieren eines Druckerfilters



Das Dialogfeld enthält zusätzliche Felder für **Netzwerkdrucker**. Geben Sie die folgenden Informationen ein:

- Remote Host — Hostname des Remote-Computers, der Daten an den Drucker sendet.
- Remote Queue — Bezeichnung der Warteschlange, in die der Remote-Computer drucken soll.

Der Remote-Computer muss so konfiguriert werden, dass der lokale Computer in die gewünschte Warteschlange drucken kann. Normalerweise wird dies von der Datei `/etc/hosts.lpd` gesteuert.

Abbildung 3–21 Hinzufügen eines Netzwerkdruckers

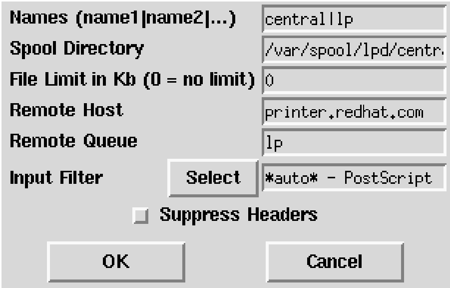


Abbildung 3–22 Hinzufügen eines NCP-Druckers

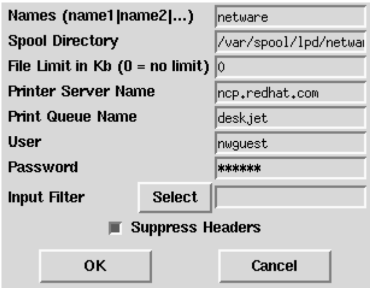
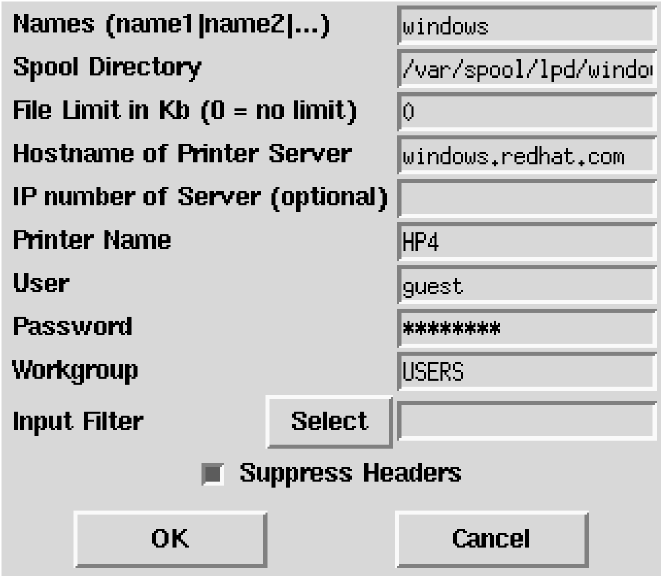


Abbildung 3–23 Hinzufügen eines SMB-Druckers



Geben Sie die folgenden Informationen ein, wenn Sie einen SMB- oder NCP-Drucker haben:

- Hostname of Printer Server — Name des Rechners, an den der zu verwendende Drucker angeschlossen ist.
- IP number of Server — Die IP-Adresse des Rechners, an die der zu verwendende Rechner angeschlossen ist (optional, nur für SMB-Drucker).
- Printer Name — Name des Druckers, über den gedruckt werden soll.
- User — Anmeldename des Benutzers für den Zugriff auf den Drucker (in der Regel `guest` für Windows-Server, oder `nobody` für `Samba`-Server).
- Password — Passwort (falls erforderlich) zum Zugriff auf den Drucker (in der Regel leer). Erfragen Sie das Passwort, falls es Ihnen nicht schon bekannt ist.

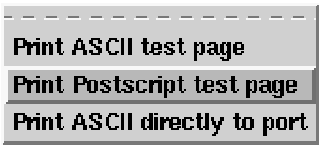
Bitte beachten

Benutzername und Passwort für SMB-Druckerwarteschlangen (LAN-Manager) und NCP-Druckerwarteschlangen (NetWare) werden unverschlüsselt in einem lokalen Skript gespeichert. Folglich können andere Benutzer den Benutzernamen und das Passwort in Erfahrung bringen. Es ist deshalb empfehlenswert, andere Benutzernamen und Passwörter für den Drucker zu vergeben als für das lokale Red Hat Linux System. Die einzige mögliche Sicherheitslücke wäre dann lediglich die unerlaubte Benutzung des Druckers. Für Dateien, die der SMB-Server im Netzwerk bereitstellt, sollte ebenfalls ein anderes Passwort als für die Druckerwarteschlange vergeben werden.

Wenn Sie die Druckerwarteschlange hinzugefügt haben, müssen Sie den Druckerdämon (`lpd`) neu starten. Klicken Sie dazu auf `Restart lpd` im Menü `lpd`.

Für jede von Ihnen konfigurierte Druckerwarteschlange können Sie eine **Testseite** ausdrucken. Wählen Sie im Menü `Tests` aus, welche Testseite Sie drucken möchten.

Abbildung 3–24 Drucken einer Testseite



3.2.2 Laden von Kernelmodulen

Der Linux-Kernel ist modular aufgebaut. Beim Systemstart wird nur ein minimaler **residenter** Kernel in den Arbeitsspeicher geladen. Danach wird immer dann, wenn ein Benutzer ein Funktionsmerkmal anfordert, das nicht im residenten Kernel implementiert ist, ein Kernel-**Modul** dynamisch in den Arbeitsspeicher geladen. Nach einer vorgegebenen Zeit ohne entsprechende Aktivitäten wird das Modul wieder aus dem Arbeitsspeicher entfernt. Durch diesen Ansatz wird Schlankheit und Effizienz erreicht.

Für das dynamische Laden von Modulen ist der Kernel-Thread `kmod` verantwortlich. Wenn der Kernel ein Modul anfordert, wird `kmod` aktiv und ruft `modprobe`(8) auf, um das Modul zu laden.

Bei der Installation von Red Hat Linux wird die Hardware Ihres Systems erkannt, Sie müssen Angaben über den überwiegenden Verwendungszweck des Systems machen und angeben, welche Programme zu laden sind. Aufgrund dieser Angaben und der automatischen Erkennung wird vom Installationsprogramm entschieden, welche Funktionsmerkmale in den residenten Kernel zu kompilieren sind und welche als ladbare Module realisiert werden. Der dynamische Ladevorgang wird so eingerichtet, dass er transparent abläuft. Dieser Vorgang ist in hohem Maße konfigurierbar. Wenn Sie Ihren eigenen benutzerdefinierten Kernel generieren, können Sie diese Entscheidungen alle selbst treffen.

Wenn Sie nach der Installation neue Hardware einbauen, die Unterstützung durch ein Kernelmodul erfordert, müssen Sie den dynamischen Ladevorgang einrichten. Dies geschieht durch Bearbeiten der Modulkonfigurationsdatei `/etc/conf.modules`.

Wenn zum Beispiel bei der Installation von Red Hat Linux eine PCI-Netzwerkkarte vom Typ SMC EtherPower 10 in Ihrem System eingebaut war, enthält die Modulkonfigurationsdatei folgende Zeile: `alias eth0 tulip`. Wenn Sie nach der Installation eine zweite, identische Netzwerkkarte einbauen, müssen Sie in der Datei `/etc/conf.modules` folgende Zeile hinzufügen:`alias eth1 tulip`.

Eine alphabetische Liste der Kernelmodule und der von den Modulen unterstützten Hardware finden Sie in Anhang A, *Allgemeine Parameter und Module*.

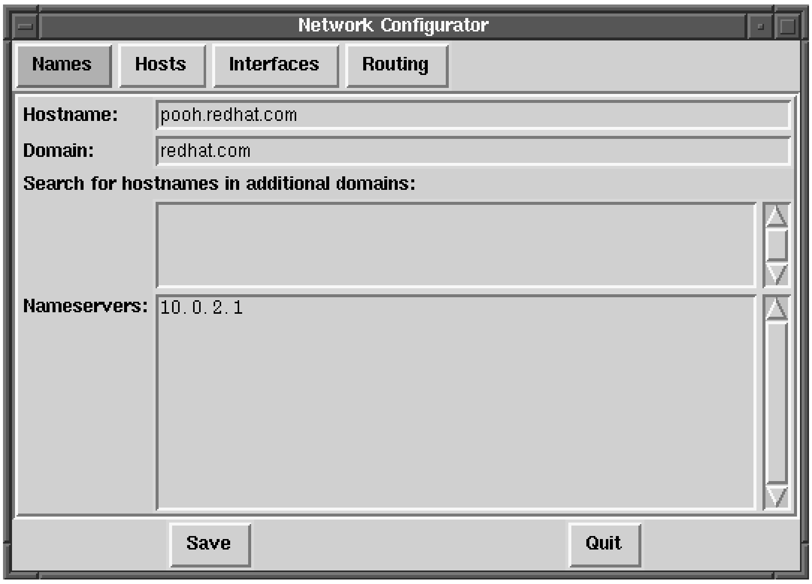
3.2.3 Konfigurieren des Netzwerks

Bitte beachten

Die Dokumentation zur Netzwerkkonfiguration mit Linuxconf finden Sie in Abschnitt 3.1.14, *Konfigurieren des Netzwerks mit* linuxconf.

Das Netzwerkkonfigurationstool (`netcfg`) in Abbildung 3–25, *Fenster Netzwerkkonfiguration* ist für eine einfache Bearbeitung von Parametern wie IP-Adresse, Gateway-Adresse, Netzwerkadresse, Nameserver sowie der Datei `/etc/hosts` gedacht.

Abbildung 3–25 Fenster Netzwerkkonfiguration



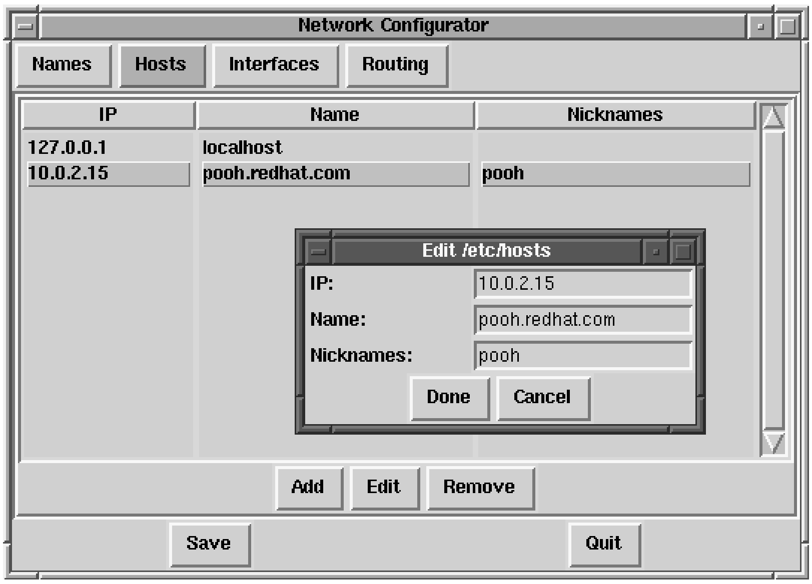
Netzwerkgeräte können hinzugefügt, entfernt, konfiguriert, aktiviert, deaktiviert und mit einem Alias benannt werden. Es werden Geräte für Ethernet, Arcnet, Token Ring, Pocket (ATP), SLIP, PLIP und Loopback unterstützt. Mit den meisten Hardware-Komponenten verträgt sich die SLIP/PLIP-Unterstützung gut. Manche Hardware-Konfigurationen können jedoch Probleme bereiten. Wenn Sie das Netzwerkkonfigurationstool verwenden, klicken Sie auf `Save`, um Ihre Änderungen zu speichern, oder klicken Sie auf `Quit`, um das Programm ohne Speichern der Änderungen zu beenden.

Verwalten von Namen

Das Fenster `Names` des Netzwerkkonfigurationstools dient zwei Hauptzwecken: Zum Eingeben von Name und Domäne Ihres Rechners und zum Festlegen, welcher

Nameserver zum Suchen anderer Rechner im Netzwerk verwendet werden soll. Die Konfigurierung eines Computers als Nameserver ist mit dem Netzwerktool nicht möglich. Zum Bearbeiten und Hinzufügen von Informationen klicken Sie einfach mit der linken Maustaste auf ein Feld und tragen die entsprechenden Informationen ein.

Abbildung 3–26 Hinzufügen/Bearbeiten von Rechnern



Verwalten von Rechnern

Im Fenster `Hosts` können Sie Rechner, die in die Datei `/etc/hosts` eingetragen sind, hinzufügen, bearbeiten oder entfernen. Das Hinzufügen und Bearbeiten von Einträgen geschieht auf die gleiche Weise: Geben Sie im angezeigten Dialogfeld die neuen Informationen ein, und klicken Sie danach auf `Done`. Abbildung 3–26, *Hinzufügen/Bearbeiten von Rechnern* zeigt ein Beispiel.

Hinzufügen einer Netzwerk-Schnittstelle

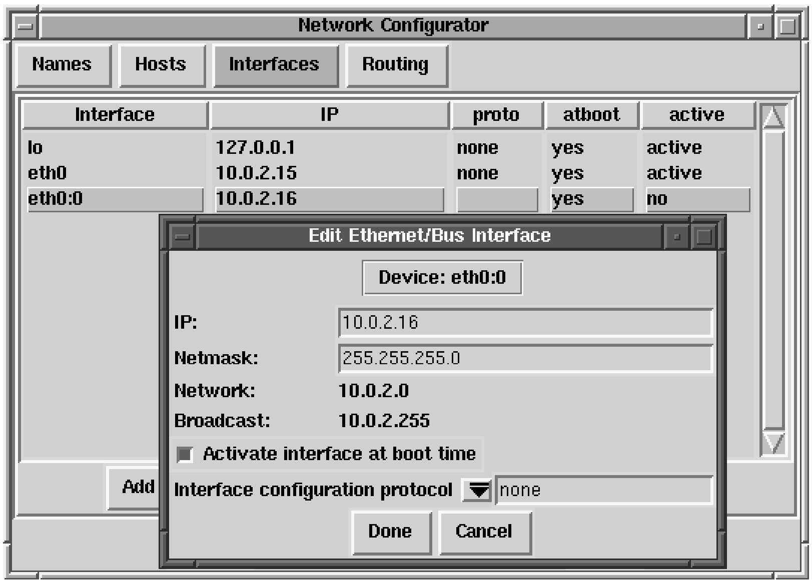
Wenn Sie nach der Installation von Red Hat Linux eine Netzwerk-Schnittstelle hinzugefügt haben oder wenn Sie während der Installation Ihre Ethernet-Karte nicht konfiguriert haben, können Sie hier die Konfiguration mit wenigen Mausklicks vornehmen.

Bitte beachten

Möglicherweise müssen Sie `kerneld` so umkonfigurieren, dass er einen Treiber für die von Ihnen hinzugefügte Netzwerk-Schnittstelle lädt (z.B. `eth0`). Weitere Informationen finden Sie in Abschnitt 3.2.2, *Laden von Kernelmodulen*.

Zum Hinzufügen einer Schnittstelle klicken Sie zuerst auf `Interfaces` im Hauptfenster. Es erscheint ein Fenster, in dem bereits konfigurierte Geräte sowie eine ganze Reihe von Optionen angezeigt werden (siehe Abbildung 3–27, *Konfigurierte Schnittstellen*).

Abbildung 3–27 Konfigurierte Schnittstellen



Um ein Gerät hinzuzufügen, klicken Sie auf den Button `Add`, und wählen Sie aus dem eingeblendeten Feld die Art der zu konfigurierenden Schnittstelle aus.

Bitte beachten

`netcfg` enthält jetzt auch einen Button `Clone`. Mit diesem Button können Sie eine bereits vorhandene Schnittstelle "klonen". Mit Hilfe von geklonten Schnittstellen kann für einen Laptop sowohl eine Ethernet-Schnittstelle für ein LAN im Büro als auch ein geklontes Ethernet-Gerät für ein LAN zu Hause festgelegt werden.

SLIP-Schnittstelle

Um eine SLIP-Schnittstelle zu konfigurieren, müssen Sie zuerst eine Telefonnummer, einen Anmeldenamen und ein Passwort angeben. Daraus werden die für den Aufbau einer SLIP-Verbindung nötigen Anfangsparameter für das Chat-Skript abgeleitet. Wenn Sie auf `Done` klicken, wird ein Dialogfeld mit der Überschrift `Edit SLIP Interface` geöffnet, mit dessen Hilfe Sie die Parameter für Hardware, Kommunikation und Netzwerkparameter für Ihre SLIP-Schnittstelle anpassen können.

PLIP-Schnittstelle

Um Ihrem System eine PLIP-Schnittstelle hinzuzufügen, müssen Sie nur die IP-Adresse, die Remote-IP-Adresse und die Netzmaske angeben. Sie können auch auswählen, ob Sie die Schnittstelle beim Booten aktivieren möchten.

Ethernet-, Arcnet-, Token Ring- und Pocket Adapter-Schnittstellen

Wenn Sie Ihrem Computer einen Ethernet-, Arcnet-, Token Ring- oder Pocket-Adapter hinzufügen, müssen Sie die folgenden Informationen angeben:

- Device — Wird auf Basis der bereits konfigurierten Geräte von netconfig festgelegt.
- IP Address — Geben Sie eine IP-Adresse für Ihr Netzwerkgerät ein.
- Netmask — Geben Sie die Netzmaske für Ihr Netzwerkgerät ein.

Die Netzwerk- und Broadcast-Adressen werden auf der Grundlage der von Ihnen eingegebenen IP-Adresse und Netzmaske automatisch berechnet.

- Activate interface at boot time:

  Aktivieren Sie dieses Kontrollkästchen, wenn das Gerät beim Booten des Systems automatisch konfiguriert werden soll.

- Allow any user to (de)activate interface:

  Aktivieren Sie dieses Kontrollkästchen, wenn jeder Benutzer die Schnittstelle aktivieren oder deaktivieren darf.

- Interface configuration protocol:

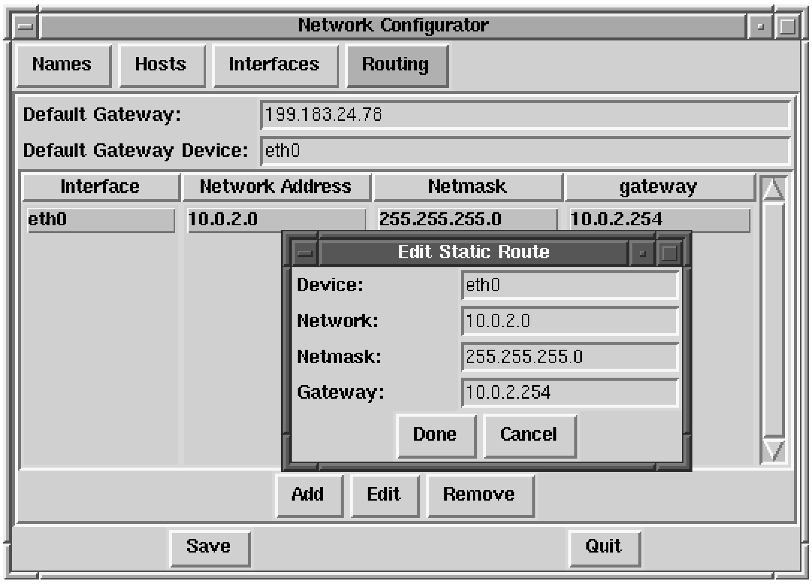
  Wenn sich in Ihrem Netzwerk ein BOOTP- oder DHCP-Server befindet und Sie Ihre Schnittstelle damit konfigurieren möchten, wählen Sie die entsprechende Option aus. Anderenfalls wählen Sie `none` aus.

Wenn Sie die Konfigurationsinformationen für Ihr neues Gerät eingegeben haben, klicken Sie auf `Done`. Das Gerät müsste jetzt in Ihrer Liste `Interfaces` als inaktives Gerät erscheinen. (In der Spalte "active" sollte `no` eingetragen sein.) Um das neue Gerät zu aktivieren, klicken Sie mit der Maus auf die entsprechende Zeile und dann auf den Button `Activate`. Wenn es sich nicht aktivieren lässt, müssen Sie eventuell die Konfiguration ändern, indem Sie auf `Edit` klicken.

Verwalten von Routen

Im Bildschirm Routes management (Routenverwaltung) können Sie statische Netzwerkrouten hinzufügen, bearbeiten oder entfernen. Das Hinzufügen und Bearbeiten von Einträgen erfolgt auf die gleiche Weise wie beim Fenster Hosts: Es wird ein Dialogfeld zum Bearbeiten geöffnet. Geben Sie die neuen Informationen ein, und klicken Sie auf `Done`. Abbildung 3–28, *Hinzufügen/Bearbeiten von Routen* zeigt ein Beispiel.

Abbildung 3–28 Hinzufügen/Bearbeiten von Routen



3.2.4 Datum und Uhrzeit

Mit dem Zeiteinstellungstool Time Machine können Sie die Uhrzeit und das Datum einstellen. Zum Ändern der Werte klicken Sie auf den Bereich der Zeit- und Datumsanzeige, den Sie ändern möchten, und dann auf die Pfeile, um die neuen Werte einzustellen.

Die geänderten Werte werden erst von der Systemuhr übernommen, wenn Sie auf den Button **Set System Clock** klicken.

Um die Uhr in der Time Machine wieder auf die Systemzeit einzustellen, klicken Sie auf **Reset Time**.

Bitte beachten

Eine Änderung der Zeiteinstellungen kann den Ablauf von Programmen gefährden, die auf ein kontinuierliches Fortschreiten der Zeit angewiesen sind. Beenden Sie deshalb so viele Anwendungen und Prozesse wie möglich, bevor Sie die Uhrzeit oder das Datum ändern.

4 PowerTools

4.1 PowerTools-Pakete

Red Hat Die PowerTools sind eine Sammlung von Software-Paketen, die für das Betriebssystem Red Hat Linux 7.0 entwickelt wurden. Die PowerTools enthalten die aktuellen Versionen (Datum der Freigabe dieses Software-Produkts) von Hunderten von Programmen - eine interessante Anwendung sollte also leicht zu finden sein.

Unter anderem sind enthalten: Audioprogramme, Chat-Clients, Entwicklungstools, Editoren, Dateimanager, Emulatoren, Spiele, Grafikprogramme, Produktivitätsanwendungen, Mathematik-/Statistikpakete, Tools für Systemadministration und Netzwerkmanagement sowie Windowmanager.

Da Sie jetzt wissen, was die PowerTools enthalten, möchten Sie die Programme sicher gern installieren. Informationen zur Installation finden Sie in Abschnitt 4.1.2, *Installieren der PowerTools-Pakete*.

4.1.1 Lesen der Inhaltsdatei der CD-ROM

Sie können die Datei mit dem Inhaltsverzeichnis der PowerTools CD-ROM vom Shell Prompt aus lesen (entweder in einem Terminalfenster oder im Konsolenmodus). Mounten Sie die CD-ROM (`mount /mnt/cdrom`). Wechseln Sie anschließend das Verzeichnis mit Hilfe des Befehls `cd /mnt/cdrom`. Geben Sie `less CONTENTS` ein, um die verfügbaren Anwendungen anzuzeigen.

4.1.2 Installieren der PowerTools-Pakete

Installieren der PowerTools unter einer grafischen Benutzeroberfläche

Wenn Sie mit GNOME oder KDE arbeiten, müssen Sie nur die CD in Ihr CD-ROM-Laufwerk einlegen. Sie werden aufgefordert, das Root-Passwort einzugeben (Sie müssen als Root angemeldet sein, um Pakete installieren zu können). Nach der Eingabe des Root-Passworts startet entweder Gnome-RPM- oder das Kpackage-Paketmanagementprogramm automatisch (je nach GUI-Umgebung) und kann zum Installieren der PowerTools verwendet werden.

Genaue Anweisungen zur Verwendung von Gnome-RPM finden Sie in Kapitel 6, *Gnome-RPM*. Unter der Adresse http://www.general.uwa.edu.au/u/toivo/kpackage/ finden Sie weitere Informationen darüber, wie Sie Kpackage verwenden können.

Wenn Sie nicht mit GNOME oder KDE arbeiten, müssen Sie die PowerTools vom Shell Prompt aus installieren. Weitere Informationen finden Sie in *Installieren der PowerTools vom Shell Prompt aus* in Abschnitt 4.1.2.

Installieren der PowerTools vom Shell Prompt aus

Zuerst müssen Sie die PowerTools CD-ROM in Ihrem CD-ROM-Laufwerk mounten.

Legen Sie die PowerTools CD in Ihr CD-ROM-Laufwerk ein. Geben Sie als Root Folgendes ein:

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

Bitte beachten:

Möglicherweise haben Sie oder der Systemadministrator Benutzern Ihres Systems die Möglichkeit eingeräumt, das CD-ROM-Laufwerk zu mounten (dies darf normalerweise nur Root). Benutzer haben diese Berechtigung, wenn die Option `user` in der Zeile `/dev/cdrom` in der Datei `/etc/fstab` enthalten ist. Bedenken Sie jedoch, dass Sie zum Installieren von PowerTools RPMs als Root angemeldet sein müssen.

Wechseln Sie nach dem Mounten des Laufwerks mit `cd` mit dem folgenden Befehl in das Verzeichnis, in dem der Inhalt der CD-ROM gemountet wurde:

```
# cd /mnt/cdrom
```

Wenn Sie den Inhalt der CD mit `ls` auflisten, sehen Sie die folgenden Verzeichnisse: `SRPMS` und `RedHat/` Das Verzeichnis `SRPMS` enthält die PowerTools Quell-RPMs. Das Verzeichnis `RedHat/RPMS` enthält die RPMs für die drei vorgegebenen Betriebssystemarchitekturen.

Der Pfad `RedHat/RPMS` wird im Folgenden als allgemeines Beispiel verwendet. Statt `RedHat/RPMS` ist das Verzeichnis einzusetzen, das Ihrer Architektur und den zu installierenden Paketen entspricht.

Wechseln Sie mit dem Befehl `cd` in das Verzeichnis `RedHat/RPMS`:

```
# cd RedHat/RPMS
#
```

Listen Sie die RPM-Dateien des Verzeichnisses mit dem Befehl `ls` auf, um die vollständige Liste der RPM-Pakete anzuzeigen, die für Intel-kompatible Systeme vorgesehen sind.

Sicher benötigen Sie mehr Informationen über ein spezielles Paket, bevor Sie entscheiden können, ob Sie es installieren möchten. Weitere Informationen über die Pakete, z.B. die Funktionen und die Herkunft, können Sie mit den Abfragemöglichkeiten von RPM abrufen. Anleitungen zum Anzeigen von Informationen zu Paketen mit Hilfe von RPM finden Sie in Abschnitt 5.3, *Freunde beeindrucken mit RPM*.

Nachdem Sie sich für ein bestimmtes Paket entschieden haben, können Sie die Installation mit RPM durchführen. RPM ist ein leistungsfähiges Paketmanagementsystem, das von der Befehlszeile aus bedient wird. Weitere Informationen zur Benutzung von RPM für die Installation und Verwaltung von PowerTools-Paketen finden Sie in Kapitel 5, *Paketverwaltung mit RPM*.

Wenn Sie die Installation Ihrer Pakete abgeschlossen haben, müssen Sie Ihre CD-ROM unmounten. Wechseln Sie zunächst mit dem Befehl `cd ..` in die nächste Verzeichnisebene über `/mnt/cdrom/`. Geben Sie anschließend den Befehl `umount /mnt/cdrom` ein, um die CD-ROM zu unmounten. Geben Sie jetzt `eject /mnt/cdrom` ein. Das CD-ROM-Laufwerk wird geöffnet, damit Sie die CD entnehmen können.

5 Paketverwaltung mit RPM

Der *R*PM *P*ackage *M*anager (RPM) ist ein offenes, frei verfügbares System zur Paketverwaltung, und kann unter Red Hat Linux und anderen Linux- und UNIX-Systemen ausgeführt werden. Red Hat möchte andere Anbieter ausdrücklich dazu ermutigen, sich die Zeit zu nehmen, RPM näher zu betrachten und es für ihre eigenen Produkte zu verwenden. RPM kann gemäß den Lizenzbedingungen der GPL vertrieben werden.

Für den Endbenutzer stellt RPM viele Funktionsmerkmale bereit, die die Systemverwaltung so einfach wie nie zuvor machen. Das Installieren, Deinstallieren und Aktualisieren der RPM-Pakete wird jeweils durch Befehle ausgeführt, die nur eine einzelne Zeile umfassen - um komplizierte Details brauchen Sie sich nicht mehr zu kümmern. RPM verwaltet eine Datenbank mit den installierten Paketen und deren Dateien, die Ihnen das Durchführen effizienter Suchvorgänge und Überprüfungen in Ihrem System ermöglicht.

Während einer Aktualisierung behandelt RPM die Konfigurationsdateien auf besondere Weise, so dass Ihre Benutzereinstellungen nicht mehr verloren gehen können - ein Funktionsmerkmal, das bei gewöhnlichen `.tar.gz`-Dateien nicht möglich ist.

Dem Entwickler bietet RPM die Möglichkeit, Quellcode aus der Software zu extrahieren und ihn in Quell- und Binärpakete für die Endbenutzer zu packen. Dies ist ein recht einfaches Verfahren, das von einer einzelnen Datei sowie von optionalen Patches (von Ihnen erstellt) ausgeführt wird. Dieses einfache Konzept mit den "reinen" Quellen und Ihren Patches und build-Anweisungen erleichtert das Pflegen des Pakets, wenn neue Software-Versionen erscheinen.

Bitte beachten

Obwohl es nicht schadet, das grundlegende Konzept von RPM zu begreifen, gibt es eine Alternative. Wenn Sie statt von der Befehlszeile aus lieber mit einer grafischen Benutzeroberfläche arbeiten, empfehlen wir Ihnen die Verwendung von Gnome-RPM. Weitere Informationen finden Sie in Kapitel 6, *Gnome-RPM*.

5.1 RPM-Entwicklungsziele

Bevor Sie sich mit der Funktionsweise von RPM auseinander setzen, ist es sinnvoll, eine ungefähre Vorstellung von den Entwicklungszielen zu bekommen.

Aktualisierbarkeit

Mit RPM können Sie einzelne Komponenten Ihres Systems aktualisieren, ohne eine komplette Neuinstallation vornehmen zu müssen. Wenn Sie eine neue Version eines auf RPM basierenden Betriebssystems (z.B. Red Hat Linux) erhalten, müssen Sie auf Ihrem Computer keine Neuinstallation vornehmen (wie das bei Betriebssystemen der Fall ist, die auf anderen Paketsystemen basieren). RPM ermöglicht Ihnen eine intelligente, vollautomatische Aktualisierung Ihres vorhandenen Systems. Die Konfigurationsdateien in den Paketen werden während des Aktualisierungsvorgangs geschützt, so dass Sie Ihre Benutzereinstellungen nicht verlieren.

Leistungsstarke Abfragefunktionen

Ein weiteres Entwicklungsziel waren leistungsstarke Abfrageoptionen für RPM. Sie können Suchanfragen nach Paketen oder sogar nach bestimmten Dateien auf Ihre gesamte Datenbank ausdehnen. Außerdem können Sie schnell feststellen, zu welchem Paket eine Datei gehört und woher dieses Paket stammt. Die in einem RPM-Paket enthaltenen Dateien befinden sich in einem komprimierten Archiv zusammen mit einem benutzerdefinierten Binär-Header, der nützliche Informationen über das Paket und seinen Inhalt enthält und somit ein schnelles und einfaches Abfragen einzelner Pakete ermöglicht.

Systemüberprüfung

Ein weiteres leistungsstarkes Funktionsmerkmal ist das Überprüfen von Paketen. Wenn Sie sich Sorgen machen, weil Sie möglicherweise eine für ein bestimmtes Paket wichtige Datei gelöscht haben, können Sie das Paket einfach überprüfen. Sie werden über eventuell festgestellte Unstimmigkeiten benachrichtigt. Sie können dann das Paket neu installieren, falls dies erforderlich sein sollte. Sämtliche von Ihnen bearbeiteten Konfigurationsdateien bleiben während der Neuinstallation erhalten.

Unveränderter Quellcode

Ein wesentliches Entwicklungsziel war die Möglichkeit, den ursprünglichen und unveränderten Quellcode zur Verfügung zu stellen, wie er von den eigentlichen Autoren der Software vertrieben wird. Mit RPM steht Ihnen dieser ursprüngliche Code zusammen mit den verwendeten Patches und den kompletten build-Anweisungen zur Verfügung. Dies ist aus mehreren Gründen sehr vorteilhaft. Wenn beispielsweise eine neue Version eines Programms auf den Markt kommt, müssen Sie nicht unbedingt wieder von vorn anfangen und das Programm kompilieren. Sie schauen sich lediglich den Patch an und wissen, was Sie *möglicherweise* zu tun haben. Auf diese Weise können alle kompilierten Standardwerte und sämtliche Änderungen angezeigt werden, die vorgenommen wurden, um ein korrektes Erstellen der Software zu ermöglichen.

Dieses Ziel mag lediglich Entwicklern wichtig erscheinen, doch die daraus resultierende höhere Qualität der Software kommt auch den Endbenutzern zugute. Wir möchten an dieser Stelle den Mitarbeitern der BOGUS-Distribution danken, von denen das Konzept des unveränderten Quellcodes stammt.

5.2 Verwenden von RPM

RPM verfügt über fünf Grundbetriebsmodi (das Erstellen von Paketen nicht mitgerechnet): Installieren, Deinstallieren, Aktualisieren, Anfragen und Überprüfen. Dieser Abschnitt enthält einen Überblick über jeden dieser Modi. Vollständige Angaben zu den Details und Optionen können Sie mit `rpm --help` aufrufen. Weitere Informationen über RPM finden Sie in Abschnitt 5.4, *Andere RPM-Ressourcen*.

5.2.1 Installieren

RPM-Pakete besitzen normalerweise Dateinamen wie `foo-1.0-1.i386.rpm`, die den Paketnamen (`foo`), die Version (`1.0`), die Release-Nummer (`1`) und die unterstützte Systemarchitektur (`i386`) enthalten. So einfach ist das Installieren von Paketen:

```
# rpm -ivh foo-1.0-1.i386.rpm
foo                       ####################################
#
```

Wie Sie sehen, gibt RPM den Paketnamen (der nicht unbedingt dem Dateinamen entsprechen muss, letzterer könnte beispielsweise auch `1.rpm` lauten) und anschließend bei der Installation des Pakets eine Reihe von Rautenzeichen aus, sozusagen als Fortschrittsanzeige.

Bitte beachten

In der Regel wird der Befehl **`rpm -ivh foo-1.0-1.i386.rpm`** zur Installation verwendet. Sie können jedoch auch **`rpm -Uvh foo-1.0-1.i386.rpm`** verwenden. `-U` wird überlicherweise zum Aktualisieren von Paketen verwendet, kann jedoch auch neue Pakete installieren. Weitere Informationen zum Verwenden des RPM-Befehls `-U` finden Sie in Abschnitt 5.2.3, *Aktualisieren*.

Das Installieren von Paketen ist ein einfacher Vorgang. Dennoch können einige Fehler auftreten:

Paket bereits installiert

Falls das Paket bereits installiert wurde, sehen Sie folgende Anzeige:

```
# rpm -ivh foo-1.0-1.i386.rpm
```

```
foo                     package foo-1.0-1 is already installed
error: foo-1.0-1.i386.rpm cannot be installed
#
```

Wenn Sie das Paket dennoch installieren möchten, können Sie in der Befehlszeile `--replacepkgs` verwenden. RPM ignoriert daraufhin den Fehler.

```
# rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
foo                       ####################################
#
```

Dateikonflikte

Wenn Sie versuchen, ein Paket zu installieren, das eine bereits durch ein anderes Paket installierte Datei enthält, wird folgende Meldung ausgegeben:

```
# rpm -ivh foo-1.0-1.i386.rpm
foo           /usr/bin/foo conflicts with file from bar-1.0-1
error: foo-1.0-1.i386.rpm cannot be installed
#
```

Wenn Sie die Option `--replacefiles` an den Befehl anhängen, ignoriert RPM diesen Fehler:

```
# rpm -ivh --replacefiles foo-1.0-1.i386.rpm
foo                       ####################################
#
```

Ungelöste Abhängigkeiten

RPM-Pakete können von anderen Paketen "abhängig" sein, d.h. sie benötigen andere Pakete, um ordnungsgemäß installiert werden zu können. Falls Sie versuchen, ein Paket zu installieren, für das eine solche ungelöste Abhängigkeit besteht, erscheint folgende Anzeige:

```
# rpm -ivh bar-1.0-1.i386.rpm
failed dependencies: foo is needed by bar-1.0-1
#
```

Um diesen Fehler zu beheben, müssen Sie die angeforderten Pakete installieren. Falls Sie dennoch mit der Installation fortfahren möchten (was nicht zu empfehlen ist, da das Paket vermutlich nicht korrekt ausgeführt werden kann), geben Sie an der Befehlszeile `--nodeps` ein.

5.2.2 Deinstallieren

Das Deinstallieren eines Pakets ist ebenso einfach wie das Installieren:

```
# rpm -e foo
#
```

Bitte beachten

Beachten Sie, dass wir hier den Paket*namen* "`foo`" und nicht den Namen der ursprünglichen Paket *datei* "`foo-1.0-1.i386.rpm`" verwendet haben. Wenn Sie ein Paket deinstallieren möchten, müssen Sie `foo` durch den tatsächlichen Namen der ursprünglichen Paketdatei ersetzen.

Beim Deinstallieren eines Pakets kann ein Abhängigkeitsfehler auftreten, wenn ein anderes installiertes Paket von diesem Paket abhängt. Beispiel:

```
# rpm -e foo
removing these packages would break dependencies: foo is needed by bar-1.0-1
#
```

Wenn RPM den Fehler ignorieren soll und Sie weiterhin das Paket deinstallieren möchten (nicht zu empfehlen, da das abhängige Paket dann wahrscheinlich nicht mehr korrekt ausgeführt werden kann), müssen Sie `--nodeps` in der Befehlszeile eingeben.

5.2.3 Aktualisieren

Das Aktualisieren von Paketen erfolgt ähnlich wie das Installieren.

```
# rpm -Uvh foo-2.0-1.i386.rpm
```

```
foo                        ####################################
#
```

Was Sie oben nicht erkennen können, ist die Tatsache, dass RPM vorhandene alte Versionen des Pakets `foo` automatisch deinstalliert hat. Möglicherweise möchten Sie nun `-U` regelmäßig zum Installieren von Paketen verwenden, da es hervorragend funktioniert, selbst wenn keine vorherigen Versionen des Pakets installiert wurden.

Da RPM ein intelligentes Aktualisieren von Paketen mit Konfigurationsdateien durchführen kann, wird möglicherweise folgende Meldung angezeigt:

```
Saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

Dies bedeutet, dass die Änderungen, die Sie an der alten Konfigurationsdatei vorgenommen haben, möglicherweise nicht "aufwärtskompatibel" zur neuen Konfigurationsdatei des Pakets sind. RPM hat deshalb die ursprüngliche Datei gespeichert und eine neue Datei installiert. Sie sollten nun baldmöglichst die beiden Dateien überprüfen und die Abweichungen ausgleichen, damit Ihr System auch weiterhin korrekt funktioniert.

Da eine Aktualisierung eigentlich aus Deinstallations- und Installationsvorgängen besteht, können sämtliche Fehler aus diesen Modi auftreten. Außerdem kann es zu einem weiteren Fehler kommen: Falls RPM annimmt, dass Sie versuchen, auf ein Paket mit einer *älteren* Versionsnummer zu aktualisieren, erscheint folgende Anzeige:

```
# rpm -Uvh foo-1.0-1.i386.rpm
foo    package foo-2.0-1 (which is newer) is already installed
error: foo-1.0-1.i386.rpm cannot be installed
#
```

Um die "Aktualisierung" dennoch fortzusetzen, müssen Sie in der Befehlszeile `--oldpackage` eingeben:

```
# rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
foo                        ####################################
#
```

5.2.4 Auffrischen

Das Auffrischen eines Pakets ist ein ähnlicher Vorgang wie das Aktualisieren.

```
# rpm -Fvh foo-1.2-1.i386.rpm
foo                       ####################################
#
```

Die Option Auffrischen von RPM überprüft die Versionen der in der Befehlszeile angegebenen Pakete und vergleicht sie mit den Versionen der bereits in Ihrem System installierten Pakete. Wenn eine neuere Version eines bereits installierten Pakets von der Option Auffrischen verarbeitet wird, aktualisiert RPM die ältere Version. Mit der Option Auffrischen kann jedoch kein Paket installiert werden, wenn nicht ein bereits zuvor installiertes Paket des gleichen Namens vorhanden ist. Dies ist der Hauptunterschied zur RPM-Option Aktualisieren, da mit Aktualisieren Pakete installiert *werden*, ganz gleich, ob eine ältere Version des Pakets bereits installiert wurde.

Die RPM-Option Auffrischen funktioniert bei Einzelpaketen oder bei einer Gruppe von Paketen einwandfrei. Besonders nützlich ist sie, wenn Sie gerade eine größere Menge unterschiedlicher Pakete heruntergeladen haben, jedoch nur die Pakete aktualisieren möchten, die bereits in Ihrem System installiert sind. Mit der Option Auffrischen brauchen Sie die heruntergeladenen Pakete nicht mehr zu durchsuchen oder unerwünschte Einträge zu löschen, bevor Sie RPM verwenden.

In diesem Fall können Sie einfach den folgenden Befehl eingeben:

```
# rpm -Fvh *.rpm
```

RPM aktualisiert automatisch die Pakete, die bereits installiert wurden.

5.2.5 Anfragen

Anfragen zu installierten Paketen an die Datenbank werden mit `rpm -q` durchgeführt. Ein einfaches Anwendungsbeispiel ist `rpm -q foo`. Dieser Befehl gibt den Namen, die Versions- und die Release-Nummer des installierten Pakets foo aus:

```
# rpm -q foo
foo-2.0-1
#
```

Statt den Paketnamen anzugeben, können Sie auch die folgenden Optionen mit -q verwenden, um anzugeben, welche Pakete Sie abfragen möchten. Diese Optionen heißen *Paketspezifizierungsoptionen*.

- -a Anfrage zu sämtlichen aktuell installierten Paketen.
- -f <*Datei*> Anfrage zum Paket, zu dem <*Datei*> gehört.
- -p <*Paketdatei*> Anfrage zum Paket <*Paketdatei*>.

Es gibt eine Reihe von Möglichkeiten, um festzulegen, welche Informationen über angefragte Pakete angezeigt werden. Mit den folgenden Optionen können Sie die gewünschten Informationen auswählen. Diese Optionen heißen *Informationsauswahloptionen*.

- -i zeigt Informationen zum Paket an, darunter Name, Beschreibung, Release, Größe, Erstellungsdatum, Installationsdatum, Anbieter und verschiedene andere Informationen.
- -l zeigt die Liste der Dateien an, die das Paket enthält.
- -s zeigt den Status sämtlicher Dateien des Pakets an.
- -d zeigt eine Liste der als Dokumentationen gekennzeichneten Dateien an (man-Seiten, Info-Seiten, README-Dateien usw.).
- -c zeigt eine Liste der als Konfigurationsdateien gekennzeichneten Dateien an. Dies sind die Dateien, die Sie nach der Installation bearbeiten, um das Paket an Ihr System anzupassen (sendmail.cf, passwd, inittab usw.).

Zu den Optionen für die Anzeige von Dateilisten können Sie an der Befehlszeile -v hinzufügen, um die Listen im gleichen Format wie bei der Option ls -l anzuzeigen.

5.2.6 Prüfen

Beim Überprüfen eines Pakets werden die Angaben zu Dateien, die aus einem Paket installiert wurden, mit den Angaben aus dem ursprünglichen Paket verglichen. Bei einer Überprüfung werden u.a. folgende Parameter verglichen: Größe, MD5-Summe, Berechtigungen, Typ, Eigentümer und Gruppe jeder Datei.

Mit dem Befehl `rpm -V` werden Pakete überprüft. Zum Angeben der zu verifizierenden Pakete können Sie alle *Paketauswahloptionen* verwenden, die für Anfragen zur Verfügung stehen. Ein einfaches Anwendungsbeispiel ist `rpm -V foo`. Dieser Befehl überprüft, ob sich alle Dateien im Paket foo noch in dem Zustand befinden, den sie ursprünglich zum Zeitpunkt der Installation hatten. Beispiel:

- So verifizieren Sie ein Paket, das eine bestimmte Datei enthält:

  ```
  rpm -Vf /bin/vi
  ```

- So verifizieren Sie ALLE installierten Pakete:

  ```
  rpm -Va
  ```

- So verifizieren Sie ein installiertes Paket mit Hilfe einer RPM-Paketdatei:

  ```
  rpm -Vp foo-1.0-1.i386.rpm
  ```

  Dies kann nützlich sein, wenn Sie vermuten, dass Ihre RPM-Datenbank beschädigt ist.

Wenn alles überprüft und für korrekt befunden wurde, erfolgt keine weitere Ausgabe. Falls Abweichungen festgestellt wurden, werden diese angezeigt. Das Ausgabeformat besteht aus einer Zeichenkette mit acht Zeichen. Konfigurationsdateien werden durch ein "c" gekennzeichnet, anschließend folgt der Dateiname. Jedes der acht Zeichen steht für das Vergleichsergebnis eines Attributs der Datei mit dem aufgezeichneten Wert für dieses Attribut aus der RPM-Datenbank. Ein einzelner Punkt (".")

bedeutet, dass der Test bestanden wurde. Die folgenden Zeichen kennzeichnen Fehler bei bestimmten Tests:

- 5 - MD5-Prüfsumme
- S - Dateigröße
- L - Symbolische Verknüpfung
- T - Dateibearbeitungszeit
- D - Gerät
- U - Benutzer
- G - Gruppe
- M - Modus (einschließlich Berechtigungen und Dateityp)
- ? -Datei nicht lesbar

Wenn eine Ausgabe angezeigt wird, entscheiden Sie, ob Sie das Paket entfernen oder neu installieren oder das Problem auf andere Weise lösen sollten.

5.3 Freunde beeindrucken mit RPM

RPM ist ein sehr nützliches Tool sowohl für die Verwaltung Ihres Systems als auch für das Diagnostizieren und Beheben von Problemen. Die Anwendungsmöglichkeiten der Optionen werden am ehesten anhand einiger Beispiele deutlich.

- Nehmen wir an, Sie haben versehentlich einige Dateien gelöscht, wissen aber nicht mehr welche. Wenn Sie Ihr gesamtes System überprüfen möchten, um festzustellen, welche Dateien fehlen, können Sie Folgendes eingeben:

  ```
  rpm -Va
  ```

  Falls einige Dateien fehlen oder offenbar beschädigt sind, sollten Sie das Paket entweder neu installieren oder zunächst deinstallieren und anschließend neu installieren.

- Angenommen, Sie stoßen auf eine Datei, die Sie nicht zuordnen können. Um herauszufinden, zu welchem Paket sie gehört, geben Sie Folgendes ein:

```
rpm -qf /usr/X11R6/bin/ghostview
```

Die Ausgabe wird etwa wie folgt aussehen:

```
gv-3.5.8-10
```

- Im folgenden Szenario können wir diese beiden Beispiele kombinieren. Nehmen wir an, Sie haben Probleme mit `/usr/bin/paste`. Sie möchten das Paket, das Eigentümer des Programms ist, überprüfen, wissen aber nicht, um welches Paket es sich handelt. Geben Sie einfach Folgendes ein:

  ```
  rpm -Vf /usr/bin/paste
  ```

  Das entsprechende Paket wird überprüft.

- Wenn Sie ein Programm verwenden und dazu nähere Informationen erhalten möchten, können Sie den folgenden Befehl eingeben, um herauszufinden, welche Dokumentationen zu dem Paket gehören, in dessen "Besitz" sich das Programm befindet (in diesem Fall ispell):

  ```
  rpm -qdf /usr/bin/md5sum
  ```

  Die Ausgabe lautet:

  ```
  /usr/share/doc/textutils-2.0a/NEWS
  /usr/share/doc/textutils-2.0a/README
  /usr/info/textutils.info.gz
  /usr/man/man1/cat.1.gz
  /usr/man/man1/cksum.1.gz
  /usr/man/man1/comm.1.gz
  /usr/man/man1/csplit.1.gz
  /usr/man/man1/cut.1.gz
  /usr/man/man1/expand.1.gz
  /usr/man/man1/fmt.1.gz
  /usr/man/man1/fold.1.gz
  /usr/man/man1/head.1.gz
  /usr/man/man1/join.1.gz
  /usr/man/man1/md5sum.1.gz
  /usr/man/man1/nl.1.gz
  /usr/man/man1/od.1.gz
  /usr/man/man1/paste.1.gz
  ```

```
/usr/man/man1/pr.1.gz
/usr/man/man1/ptx.1.gz
/usr/man/man1/sort.1.gz
/usr/man/man1/split.1.gz
/usr/man/man1/sum.1.gz
/usr/man/man1/tac.1.gz
/usr/man/man1/tail.1.gz
/usr/man/man1/tr.1.gz
/usr/man/man1/tsort.1.gz
/usr/man/man1/unexpand.1.gz
/usr/man/man1/uniq.1.gz
/usr/man/man1/wc.1.gz
```

- Sie finden ein neues RPM-Paket zu sndconfig, wissen jedoch nicht, um was es sich handelt. Um Informationen zu erhalten, geben Sie Folgendes ein:

  ```
  rpm -qip sndconfig-0.48-1.i386.rpm
  ```

  Die Ausgabe lautet:

  ```
  Name        : sndconfig                Relocations: (not relocateable)
  Version     : 0.48                          Vendor: Red Hat
  Release     : 1                         Build Date: Mon 10 Jul 2000 02:25:40
  Install date: (none)                    Build Host: porky.devel.redhat.com
  Group       : Applications/Multimedia   Source RPM: sndconfig-0.48-1.src.rpm
  Size        : 461734                       License: GPL
  Packager    : Red Hat <http://bugzilla.redhat.com/bugzilla>
  Summary     : The Red Hat Linux sound configuration tool.
  Description :
  Sndconfig is a text based tool which sets up the configuration files
  you'll need to use a sound card with a Red Hat Linux system.
  Sndconfig can be used to set the proper sound type for programs which
  use the /dev/dsp, /dev/audio and /dev/mixer devices. The sound
  settings are saved by the aumix and sysV runlevel scripts.
  ```

- Nun möchten Sie sehen, welche Dateien vom RPM-Paket koules installiert werden. Geben Sie Folgendes ein:

  ```
  rpm -qlp sndconfig-0.48-1.i386.rpm
  ```

Die Ausgabe lautet:

```
/usr/sbin/pnpprobe
/usr/sbin/sndconfig
/usr/share/locale/cs/LC_MESSAGES/sndconfig.mo
/usr/share/locale/da/LC_MESSAGES/sndconfig.mo
/usr/share/locale/de/LC_MESSAGES/sndconfig.mo
/usr/share/locale/es/LC_MESSAGES/sndconfig.mo
/usr/share/locale/fr/LC_MESSAGES/sndconfig.mo
/usr/share/locale/hu/LC_MESSAGES/sndconfig.mo
/usr/share/locale/id/LC_MESSAGES/sndconfig.mo
/usr/share/locale/is/LC_MESSAGES/sndconfig.mo
/usr/share/locale/it/LC_MESSAGES/sndconfig.mo
/usr/share/locale/ko/LC_MESSAGES/sndconfig.mo
/usr/share/locale/no/LC_MESSAGES/sndconfig.mo
/usr/share/locale/pt/LC_MESSAGES/sndconfig.mo
/usr/share/locale/pt_BR/LC_MESSAGES/sndconfig.mo
/usr/share/locale/ro/LC_MESSAGES/sndconfig.mo
/usr/share/locale/ru/LC_MESSAGES/sndconfig.mo
/usr/share/locale/sk/LC_MESSAGES/sndconfig.mo
/usr/share/locale/sl/LC_MESSAGES/sndconfig.mo
/usr/share/locale/sr/LC_MESSAGES/sndconfig.mo
/usr/share/locale/sv/LC_MESSAGES/sndconfig.mo
/usr/share/locale/tr/LC_MESSAGES/sndconfig.mo
/usr/share/locale/uk/LC_MESSAGES/sndconfig.mo
/usr/share/man/man8/pnpprobe.8.gz
/usr/share/man/man8/sndconfig.8.gz
/usr/share/sndconfig/sample.au
/usr/share/sndconfig/sample.midi
```

Dies sind nur einige Beispiele. Während Sie sich mit dem System vertraut machen, werden Sie noch viele weitere Anwendungsmöglichkeiten für RPM entdecken.

5.4 Andere RPM-Ressourcen

Weitere Informationen zu RPM finden Sie auf der man-Seite, im Hilfebildschirm (`rpm --help`) sowie in den RPM-Dokumenten unter der Adresse

http://www.rpm.org/

Außerdem ist ein RPM-Buch erhältlich mit dem Titel *Maximum PRM* . Es kann bei Red Hat, über eine Buchhandlung oder über das Internet bezogen werden. Es enthält viele wertvolle Informationen über RPM und wendet sich sowohl an den Endbenutzer als auch an den Paketersteller.

Eine Online-Version des Buchs ist verfügbar unter http://www.rpm.org/.

Daneben gibt es noch eine Mailing-Liste für die Diskussion RPM-bezogener Themen. Die Liste heißt `rpm-list@redhat.com`.

Die Liste wird archiviert unter http://www.redhat.com/support/mailing-lists/. Wenn Sie diese Liste abonnieren möchten, schicken Sie eine E-Mail an `rpm-list-request@redhat.com` und geben in die Betreffzeile das Wort `subscribe` ein.

6 Gnome-RPM

Eines der benutzerfreundlichsten Paketbearbeitungsprogramme ist Gnome-RPM, ein grafisches Tool, das unter dem X Window System ausgeführt wird. Gnome-RPM wurde von James Henstridge geschrieben (`james@daa.com.au`). Die Unterstützung für RPM 3.0 wurde von Red Hat zur Verfügung gestellt, und der zusätzliche rpmfind-Code stammt von Daniel Veillard.

Gnome-RPM (auch als gnorpm bezeichnet) ermöglicht den Endbenutzern den einfachen Umgang mit der RPM-Technologie. Es ist schnell, leistungsfähig und besitzt eine benutzerfreundliche Oberfläche.

Weitere Informationen über die RPM-Technologie finden Sie unter Kapitel 5, *Paketverwaltung mit RPM*.

Gnome-RPM ist "GNOME-kompatibel", d.h. es lässt sich nahtlos in GNOME, der Desktop-Umgebung unter dem X Window System, integrieren.

Mit Gnome-RPM können Sie auf einfache Weise

- RPM-Pakete installieren
- RPM-Pakete deinstallieren
- RPM-Pakete aktualisieren
- neue RPM-Pakete suchen
- RPM-Pakete abfragen
- RPM-Pakete überprüfen

Die Oberfläche enthält ein Menü, eine Symbolleiste, einen Verzeichnisbaum und ein Anzeigefenster für die aktuell installierten Pakete.

In Gnome-RPM können Sie Vorgänge ausführen, indem Sie Pakete suchen und auswählen und anschließend den Typ des auszuführenden Vorgangs auswählen. Dies geschieht durch Klicken auf den gewünschten Button in der Symbolleiste, über das Menü oder durch Klicken mit der rechten Maustaste.

- Beim Installieren eines Pakets werden sämtliche Komponenten dieses Pakets in den richtigen Verzeichnissen in Ihrem System abgelegt.
- Beim Deinstallieren werden sämtliche Bestandteile des Pakets entfernt, ausgenommen die von Ihnen bearbeiteten Konfigurationsdateien.
- Beim Aktualisieren eines Pakets wird die neue Version installiert, und sämtliche alten Version, die installiert wurden, werden deinstalliert. So können Sie Ihre Pakete schnell aktualisieren und immer auf dem neuesten Stand halten. Weitere Informationen zum Ändern der Standardeinstellungen für die Installation und Deinstallation von Paketen finden Sie in Abschnitt 6.4, *Konfiguration*.

Sie können auch mit Hilfe der Option **Websuche** im Internet nach neuen Paketversionen suchen. Sie können Gnome-RPM anweisen, nach bestimmten Distributionen zu suchen, wenn Sie neue Pakete beziehen möchten. (Bei langsamen Verbindungen kann das Ausführen dieser Option eine Weile dauern.) Weitere Informationen über dieses Funktionsmerkmal finden Sie in Abschnitt 6.4, *Konfiguration*.

Bitte beachten

Verwenden Sie die Option **Websuche** mit Vorsicht, da es nicht möglich ist, die Integrität der vielen Pakete zu überprüfen, die in den zahlreichen Software-Sammlungen erhältlich sind. Vor dem Installieren der Pakete sollten Sie eine Anfrage für dieses Paket durchführen, um Hinweise auf seine Zuverlässigkeit zu erhalten. Pakete, die nicht von Red Hat produziert wurden, werden von Red Hat in keinster Weise unterstützt.

Das Ausführen all dieser und vieler weiterer Vorgänge mit Gnome-RPM entspricht dem Verwenden von `rpm` am Shell Prompt. Allerdings erleichtert die grafische Oberfläche von Gnome-RPM diese Vorgänge oft.

Normalerweise arbeiten Sie folgendermaßen mit Gnome-RPM: Sie zeigen die verfügbaren Pakete an, wählen eines oder mehrere Pakete aus und wählen anschließend eine Option in der Symbolleiste oder im Menü aus, die den gewünschten Vorgang ausführt. Durch die Verwendung von **Filtern** kann Gnome-RPM Pakete in verschiedenen Ansichten zeigen. Weitere Informationen zur Verwendung von Filtern zum Identifizieren von Paketen finden Sie in Abschnitt 6.3, *Installieren neuer Pakete*.

Sie können beispielsweise verschiedene Pakete mit nur wenigen Mausklicks installieren, aktualisieren oder deinstallieren. Auf ähnliche Weise können Sie auch Anfragen und Überprüfungen für mehrere Pakete gleichzeitig ausführen. Durch die Integration von Gnome-RPM in GNOME können Sie Installationsvorgänge, Abfragen und Überprüfungen auch vom GNOME Dateimanager aus durchführen.

6.1 Starten von Gnome-RPM

Sie können Gnome-RPM entweder in einem XTerm oder unter GNOME über das Panel starten (**Main Menu Button** => **System** => **GnoRPM**).

Um Gnome-RPM in einem XTerm zu starten, geben Sie am Shell Prompt Folgendes ein:

```
gnorpm &
```

Damit rufen Sie das Gnome-RPM Hauptfenster auf (siehe Abbildung 6–1, *Gnome-RPM Hauptfenster*).

Bitte beachten

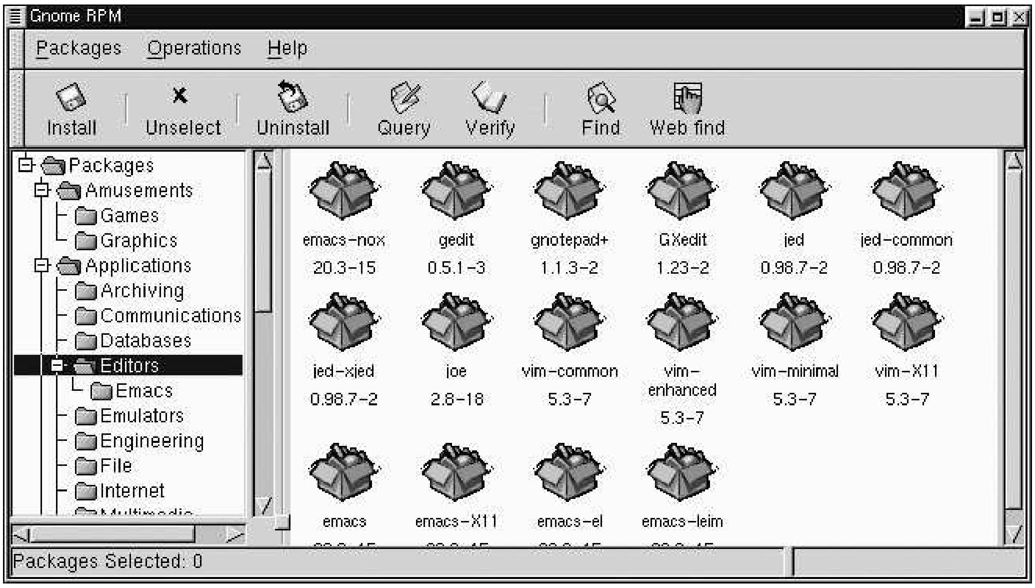
Um Pakete installieren, aktualisieren oder deinstallieren zu können, müssen Sie als Root angemeldet sein. Geben Sie dazu am Shell Prompt einfach `su root` und anschließend das Root-Passwort ein. Für Abfragen und zum Überprüfen von Paketen müssen Sie jedoch nicht als Root angemeldet sein.

Die Gnome-RPM Oberfläche besteht aus mehreren Komponenten.

- Paketteilfenster - Auf der linken Seite. Hier können Sie Pakete in Ihrem System durchsuchen und auswählen.

- Anzeigefenster - Rechts neben dem Paketteilfenster. Zeigt den Inhalt der Ordner im Teilfenster an.
- Symbolleiste - Über dem Display und dem Teilfenster. Ein grafisches Display mit Pakettools.
- Menü - Über der Symbolleiste. Enthält textbasierte Befehle, Hilfeinformationen, Voreinstellungen und andere Einstellungen.
- Statusleiste - Unterhalb des Teilfensters und des Anzeigefensters. Zeigt die Gesamtanzahl der ausgewählten Pakete an.

Abbildung 6–1 Gnome-RPM Hauptfenster



6.2 Die Paketanzeige

Jedes Ordnersymbol in der Baumansicht auf der linken Seite steht für eine Gruppe von Paketen. Jede Gruppe kann Untergruppen enthalten. Gruppen werden verwendet, um Pakete, die ähnliche Funktionen ausführen, an bestimmten Stellen zusammenzufassen. Der Ordner **Editors** enthält beispielsweise Texteditoren wie ed, vim und

GXedit. In der Baumansicht befindet sich unterhalb von **Editors** eventuell ein weiterer Ordner namens **Emacs**. Er enthält sowohl emacs als auch emacs-X11.

Die Baumansicht kann ein- und ausgeblendet werden, was das Navigieren durch die Pakete erleichtert. Ein **+** neben einem Ordner zeigt an, dass innerhalb dieser Kategorie Unterordner vorhanden sind.

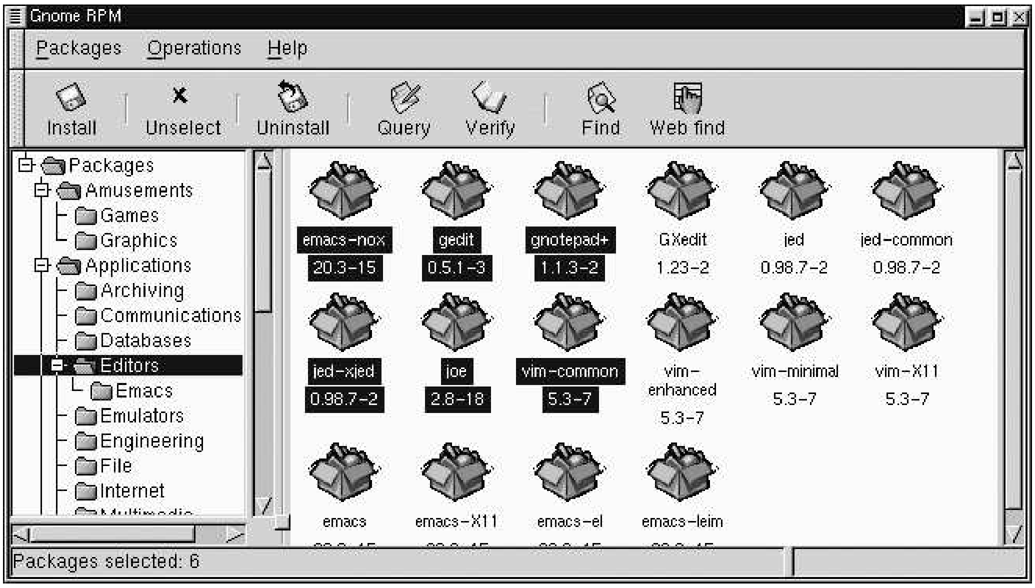
Um die Pakete und Untergruppen innerhalb einer Gruppe anzuzeigen, klicken Sie mit der linken Maustaste auf einen Ordner oder auf **+**. Das Anzeigefenster zeigt nun den Inhalt dieses Ordners an. Standardmäßig werden Symbole angezeigt, die die Pakete repräsentieren. Sie können aber auch eine Liste anzeigen, indem Sie **Als Liste anzeigen** im Register **Schnittstelle** auswählen. Das Register finden Sie unter **Tätigkeiten** => **Einstellungen**. Weitere Informationen zum Anpassen der Einstellungen finden Sie in Abschnitt 6.4, *Konfiguration*.

Auf diese Art und Weise können Sie sich in der Baumansicht bewegen sowie Ordner öffnen und erweitern, die Anwendungen, Spiele, Tools und mehr enthalten. Der Inhalt jedes Ordners wird im rechten Teilfenster angezeigt.

6.2.1 Auswählen von Paketen

Wenn Sie ein einzelnes Paket auswählen möchten, klicken Sie mit der linken Maustaste darauf. Der Titel des Pakets wird nun hervorgehoben dargestellt (siehe Abbildung 6–2, *Auswählen von Paketen in Gnome-RPM*), d.h. es ist aktuell ausgewählt. Um die Auswahl aufzuheben, klicken Sie entweder mit der linken Maustaste auf einen leeren Bereich in der Anzeige, oder Sie klicken auf den Button **Unselect** in der Symbolleiste. Wenn Sie die Auswahl eines Pakets aufheben, verschwindet auch die Hervorhebung wieder.

Abbildung 6–2 Auswählen von Paketen in Gnome-RPM



Sie können mehrere Pakete gleichzeitig aus- bzw. abwählen, die sich auch in unterschiedlichen Ordnern im Fenster mit der Baumansicht befinden können. Um mehrere Pakete nacheinander auszuwählen, halten Sie die [Strg]-Taste gedrückt und klicken mit der linken Maustaste auf die gewünschten Pakete. Jede zusätzliche Auswahl wird hervorgehoben dargestellt.

Um mehr als ein Paket **in Folge**, also einen größeren Bereich innerhalb eines Ordners auszuwählen, klicken Sie mit der linken Maustaste auf das erste Paket und dann, während Sie die [Umschalttaste] gedrückt halten, auf das letzte Paket des auszuwählenden Bereichs. Die Pakete, die sich zwischen dem ersten und letzten Paket Ihrer Auswahl befinden, werden ebenfalls ausgewählt und hervorgehoben dargestellt. Mit dieser Option können Sie schnell ganze Gruppen von Paketen auswählen und müssen nicht jedes Paket einzeln auswählen.

Die Statusleiste im unteren Bereich von Gnome-RPM zeigt die Gesamtanzahl der ausgewählten Pakete an.

6.3 Installieren neuer Pakete

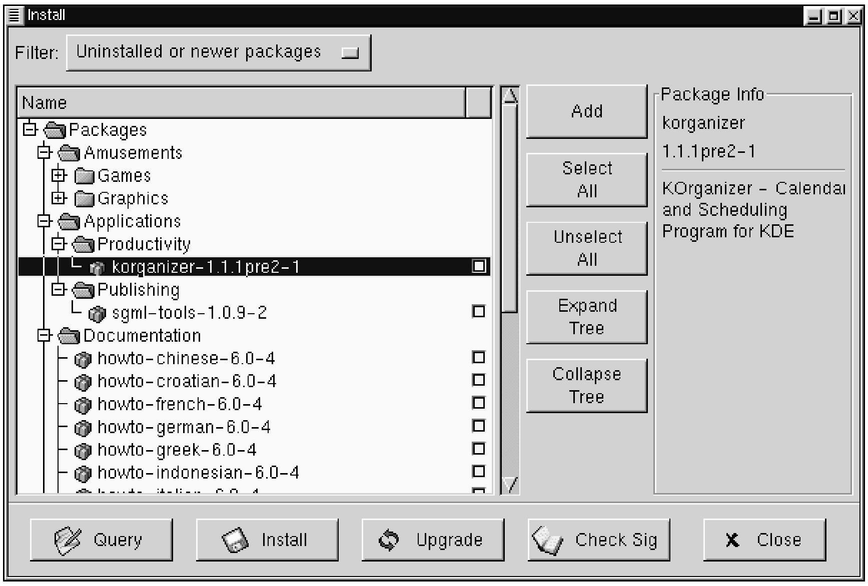
Wenn Sie neue Pakete installieren möchten, klicken Sie auf **Installieren** in der Symbolleiste. Das Fenster **Installieren** wird geöffnet und zeigt Pakete an, die entweder bereits installiert sind, aktueller sind oder anderen Kriterien entsprechen, die in der Dropdown-Liste **Filter** im oberen Bereich des Fensters ausgewählt wurden. Ein Beispiel für ein **Installieren**-Fenster, in dem der Filter "**All but installed packages**" verwendet wird, finden Sie in Abbildung 6–4, *Das Fenster Pakete hinzufügen*.

Mit der **Filter**-Funktion können Sie angeben, welche Pakete Sie anzeigen wollen. Folgende Filter können Sie zum Anzeigen verwenden:

- Alle Pakete
- Alle Pakete außer den installierten Paketen
- Nur deinstallierte Pakete
- Nur aktuellere Pakete
- Deinstallierte oder aktuellere Pakete

Mit der Dropdown-Liste im oberen Bereich des Fensters können Sie zwischen den verschiedenen Kriterien für die Anzeige der Pakete umschalten.

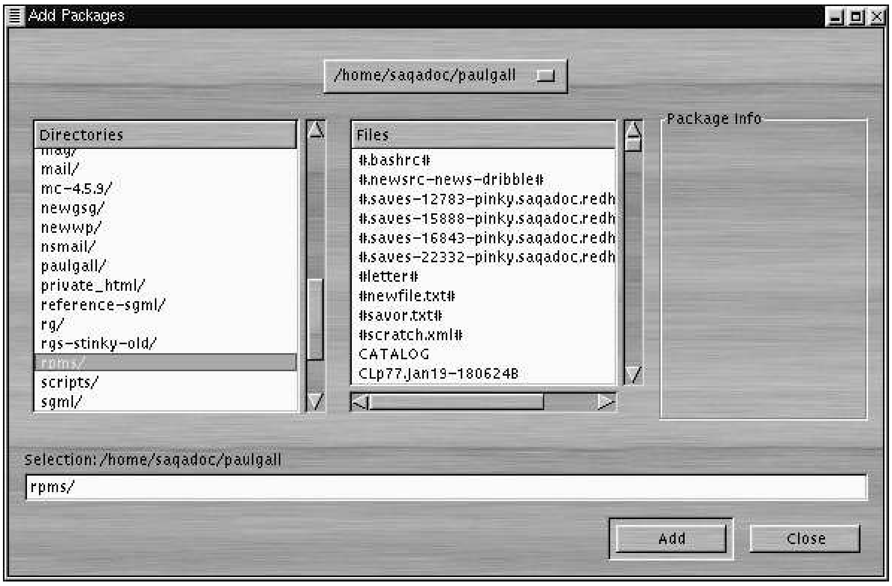
Abbildung 6–3 Das Fenster Installieren



Klicken Sie auf den Button **Hinzufügen**. Wenn Ihre CD-ROM mit einer Red Hat Linux CD-ROM gemountet ist, sucht Gnome-RPM standardmäßig im Verzeichnis `/mnt/cdrom/RedHat/RPMS` nach neuen Paketen. (Sie finden diese Option im Register **Schnittstelle** des Dialogfelds **Einstellungen**. In Abschnitt 6.4, *Konfiguration* finden Sie weitere Informationen über diese Funktion).

Wenn im Standardpfad keine Pakete verfügbar sind, wird das Dialogfeld **Pakete hinzufügen** angezeigt, in dem Sie den entsprechenden Pfad zu Ihrem neuen Paket auswählen können. Zum schnellen Navigieren zu voreingestellten Verzeichnissen können Sie in dieser Ansicht mit der Dropdown-Liste im oberen Bereich des Fensters den richtigen Pfad auswählen. Sie können aber auch im linken Teilfenster des Fensters **Pakete hinzufügen** doppelklicken, um zum richtigen Pfad zu gelangen (wie in Abbildung 6–4, *Das Fenster Pakete hinzufügen*). Sie können den Pfad auch im Textfenster im unteren Bereich des Fensters **Pakete hinzufügen** eingeben.

Abbildung 6–4 Das Fenster Pakete hinzufügen



Bitte beachten

Wenn Sie RPMs herunterladen, werden diese Pakete mit großer Wahrscheinlichkeit im Verzeichnis `rpms` in Ihrem Home-Verzeichnis abgelegt. Wenn Ihr Home-Verzeichnis z.B. `/home/bill` ist, werden die heruntergeladenen RPMs in `/home/bill/rpms` abgelegt.

Wenn Sie auf den Eintrag klicken, erscheint eine kurze Beschreibung des Pakets im Teilfenster **Paketinformation** des Fensters **Installieren.** Aktivieren Sie zum Installieren oder Abfragen eines Pakets das **Kontrollkästchen** neben dem Paket, und klicken Sie dann auf den Button **Installieren.** Sie können den Eintrag auch abfragen, wenn das zugehörige Kontrollkästchen aktiviert ist. Die Installation kann auch vom Fenster **Paketinformation** aus vorgenommen werden (Beispiel siehe Abbildung 6–10, *Anfragefenster* in Abschnitt 6.5.1, *Anfragen von Paketen*).

Um einen Eintrag auszuwählen, doppelklicken Sie mit der linken Maustaste darauf, oder klicken Sie auf den Button **Hinzufügen**. Die ausgewählten Pakete werden in das Fenster **Installieren** übernommen. Sie können auch mehr als ein Paket auf die gleiche Art und Weise installieren. Alle ausgewählten Pakete werden in das Fenster **Installieren** übernommen.

Die Pakete können Sie jedoch nicht nur über das Fenster **Installieren**, sondern auch nach dem Ausführen einer Anfrage des ausgewählten Pakets installieren. Klicken Sie auf **Anfragen**, um das Fenster **Paketinformation** zu öffnen. Hier finden Sie verschiedene Details zu der/den Datei(en), die Sie für die Installation ausgewählt haben. Zu den Angaben gehören der Ursprung des Pakets, das Erstellungsdatum, die Größe usw.

In diesem Fenster **Paketinformation** haben Sie die Möglichkeit, Pakete zu installieren oder zu aktualisieren.

Wenn das Paket in Ihrem System bereits vorhanden ist und Sie die Anfrage für eine neue Version durchführen, stellt Ihnen das Fenster **Paketinformation** den Button **Aktualisieren** zur Verfügung, mit dem Sie eine Aktualisierung auf die neuere Version des Pakets durchführen können.

Sie können Pakete auch per Drag and Drop aus dem GNOME Dateimanager in das Fenster ziehen und dort ablegen. Klicken Sie im Dateimanager mit der linken Maustaste auf die ausgewählte RPM-Datei, und ziehen Sie die Datei bei gedrückter Maustaste in das Fenster **Installieren**. Legen Sie sie dort im Teilfenster **Name** ab.

Wenn Sie Dateien vom Dateimanager in das Fenster **Installieren** ziehen, sehen Sie, dass die Datei während des Ziehens in Richtung von Gnome-RPM als Symbol angezeigt wird. Wenn sich die Datei im Teilfenster **Name** befindet, wird das Paket standardmäßig für die Installation überprüft, und die Paketinformationen erscheinen im Teilfenster **Paketinformation** auf der rechten Seite.

Zum Installieren des Pakets klicken Sie einfach auf den Button **Installieren**.

Während der Installation des Pakets wird eine Fortschrittsanzeige eingeblendet.

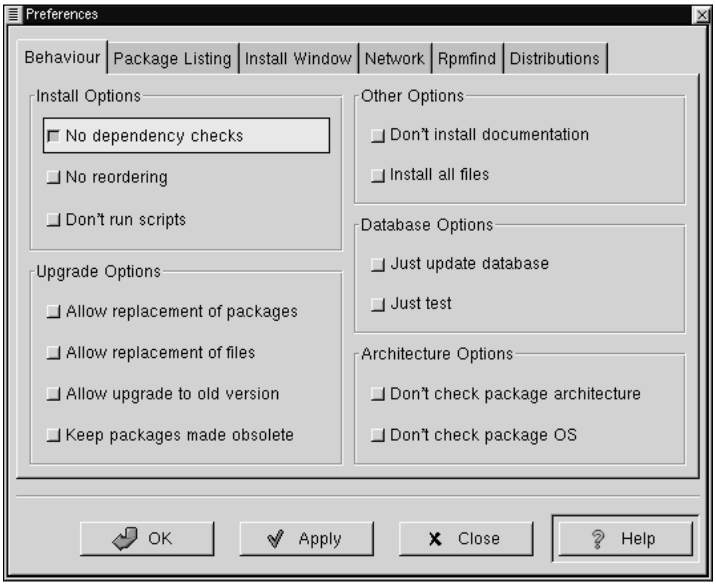
6.4 Konfiguration

Gnome-RPM stellt zahlreiche Optionen für das Installieren und Deinstallieren von Paketen, für die Dokumentation und andere Funktionen zur Verfügung. Im Dialogfeld

Einstellungen können Sie Gnome-RPM Ihren Bedürfnissen anpassen. Zu diesem Dialogfeld gelangen Sie über das Menü **Operations** => **Einstellungen**. Um im Dialogfeld **Einstellungen** eine Auswahl zu treffen, müssen Sie die Kontrollkästchen neben den gewünschten Optionen aktivieren.

Im Register **Verhalten** finden Sie eine Reihe von Optionen, mit denen Sie festlegen können, wie Gnome-RPM Pakete installiert, deinstalliert und aktualisiert. Das Register Verhalten ist in fünf Bereiche unterteilt: Installieren, Aktualisieren, Sonstige, Datenbank und Architektur. Beachten Sie, dass diese Felder in der Standardeinstellung nicht aktiviert sind (siehe Abbildung 6–5, *Das Register Verhalten im Dialogfeld Einstellungen*).

Abbildung 6–5 Das Register Verhalten im Dialogfeld Einstellungen



In **Installieren Option** haben Sie folgende Möglichkeiten:

- **Keine Abhängigkeitsprüfungen** - Wenn diese Option ausgewählt ist, wird ein Paket installiert oder aktualisiert, ohne zu überprüfen, ob das Programm von anderen Dateien abhängig ist, um korrekt funktionieren zu können. Sofern Sie nicht genau wissen, was Sie tun, wird dringend davon abgeraten, diese Option zu verwenden, da einige Pakete möglicherweise von Dateien, Bibliotheken oder Programmen anderer Pakete abhängig sind, um korrekt funktionieren zu können.

- **Keine Neuordnung** - Diese Option ist nützlich, falls RPM die Installationsreihenfolge einiger Pakete nicht ändern kann, um Abhängigkeiten zu entsprechen.
- **Scripts nicht starten** - Vor- und Nach-Installationsskripten sind Befehlsfolgen, die manchmal in Pakete eingefügt werden, um die Installation zu unterstützen. Dieses Kontrollkästchen ist vergleichbar mit der Option `--noscripts` beim Installieren am Shell Prompt.

Unter **Upgrade Optionen** können Sie Folgendes auswählen:

- **Ersetzen von Paketen zulassen** - Ersetzt ein Paket durch eine Kopie dieses Pakets. Vergleichbar mit der Option `--replacepkgs` am Shell Prompt. Diese Option kann nützlich sein, wenn ein bereits installiertes Paket beschädigt wurde oder sonstige Nachbesserungen benötigt, um korrekt funktionieren zu können.
- **Ersetzen von Dateien zulassen** - Erlaubt das Ersetzen von Dateien, die Eigentum eines anderen Pakets sind. Das Äquivalent am Shell Prompt zu dieser RPM-Option ist `--replacefiles`. Diese Option kann manchmal nützlich sein, wenn zwei Pakete den gleichen Dateinamen verwenden, aber unterschiedliche Inhalte haben.
- **Upgrade auf alte Versionen zulassen** - Wie das Shell Prompt-Gegenstück `--oldpackage` ermöglicht auch diese Option das "Aktualisieren" auf ein früheres Paket. Das kann nützlich sein, wenn die aktuelle Version eines Pakets in Ihrem System nicht korrekt funktioniert.
- **Veraltete Pakete behalten** - Verhindert, dass im Veraltet-Header aufgelistete Pakete entfernt werden.

In **Andere Optionen** können Sie Folgendes auswählen:

- **Dokumentation nicht installieren** - Wie `--excludedocs` spart auch diese Option Festplattenplatz, indem Dokumentationen, z.B. man-Seiten und andere, das Paket betreffende Informationen, von der Installation ausgenommen werden.
- **Alle Dateien installieren** - Installiert sämtliche Dateien des Pakets.

Die in **Datenbank Optionen** und in **Architektur Optionen** verfügbaren Optionen ermöglichen es Ihnen u.a. festzulegen, ob eine "Testinstallation" ausgeführt werden soll (die auf mögliche Dateikonflikte prüft, ohne eine wirkliche Installation vorzunehmen), oder ob Sie Pakete für andere Betriebssysteme oder Systemarchitekturen ausschließen möchten.

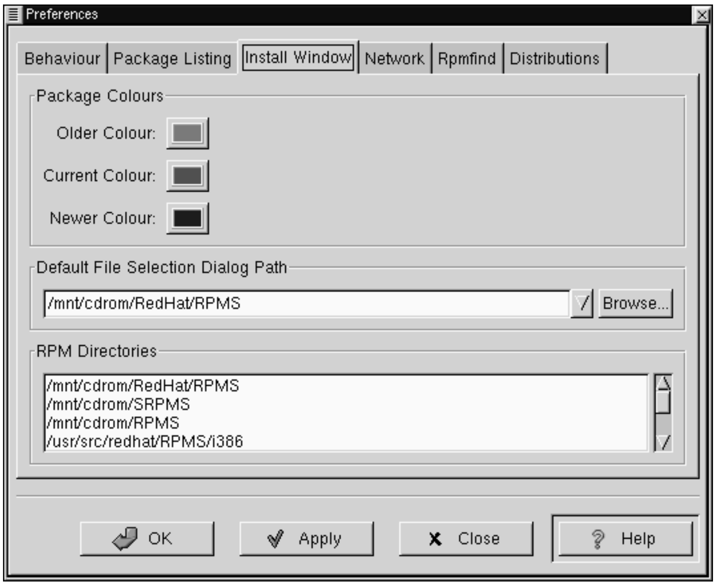
Im Register **Package Listing** stehen Ihnen verschiedene Anzeigeoptionen für Ihre Pakete zur Verfügung: entweder als **Icons**, also auf grafischer Basis, oder in Form einer **Liste**, die zwar nicht grafisch ist, dafür aber mehr Informationen über die Pakete enthalten kann.

Im Fenster **Installieren** können Sie den Pfad angeben, in dem Gnome-RPM neue RPMs in Ihrem System finden kann. Ein Beispiel für diesen Dialog finden Sie in Abbildung 6–6, *Das Fenster Installieren*. Wenn Sie Ihre Red Hat Linux CD-ROM verwenden, ist dies wahrscheinlich folgender Pfad:

```
/mnt/cdrom/RedHat/RPMS
```

oder ein ähnlicher als Standardpfad für Gnome-RPM festgelegter Pfad. Wenn Sie neue RPMs aus dem Internet herunterladen oder RPMs über ein NFS-gemountetes CD-ROM-Laufwerk installieren möchten, ist ein anderer Pfad erforderlich.

Abbildung 6–6 Das Fenster Installieren



Um diesen Pfad zu ändern, geben Sie den vollständigen Pfad zu den RPMs ein, mit denen Sie arbeiten möchten. Wenn Sie auf die Buttons **Übernehmen** oder **OK** klicken, wird der Pfad gespeichert und bei zukünftigen Sitzungen als Standardpfad verwendet. Sie können den Standardpfad auch festlegen, indem Sie auf den Button **Browse...** klicken und durch das Fenster **RPMPath** navigieren.

Wenn Sie den Pfad geändert und das Dialogfeld geschlossen haben, können Sie mit dem Button **Installieren** die im neuen Pfad verfügbaren Pakete anzeigen.

(Falls der Pfad für Ihre RPMs nicht dem Standardpfad in Ihren Einstellungen entspricht, wird ein Browser-Fenster angezeigt, in dem Sie den korrekten Pfad für Ihre neuen RPMs auswählen können.)

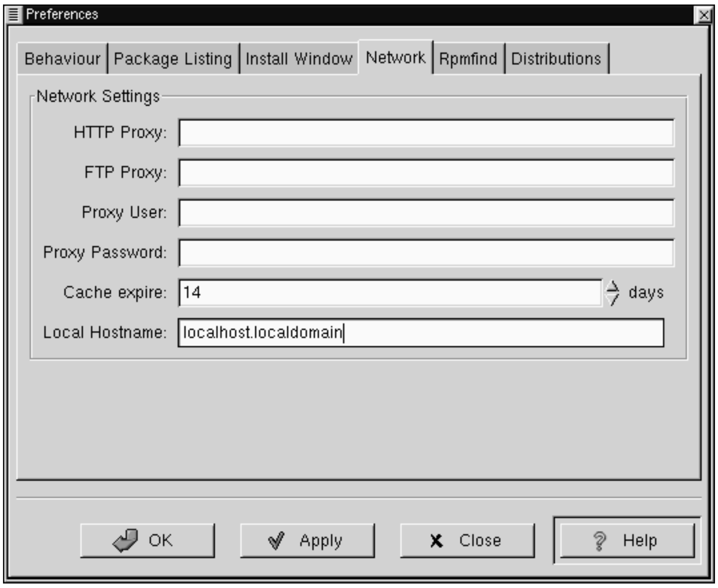
Unter **Package Colors** finden Sie die Farbkodierung für die Pakete. Die Standardeinstellung für ältere Pakete ist grau. Aktuellen Paketen ist die Farbe grün zugeordnet. Pakete, die neuer als die installierten Pakete sind, haben die Farbe blau. Diese Farben können Ihren Bedürfnissen entsprechend angepasst werden.

In **RPM Directories** sind Standardverzeichnisse aufgeführt, in denen Gnome-RPM nach Paketen sucht.

In **Network** können Sie Proxies für die Übertragung mit HTTP und FTP sowie Benutzernamen und Passwörter angeben (siehe Abbildung 6–7, *Netzwerkeinstellungen*). Beachten Sie, dass das Passwort nicht sicher gespeichert wird.

Im Fenster **Cache expire** können Sie festlegen, nach welcher Zeit Daten aus der Datenbank rpmfind als veraltet angesehen werden.

Abbildung 6–7 Netzwerkeinstellungen

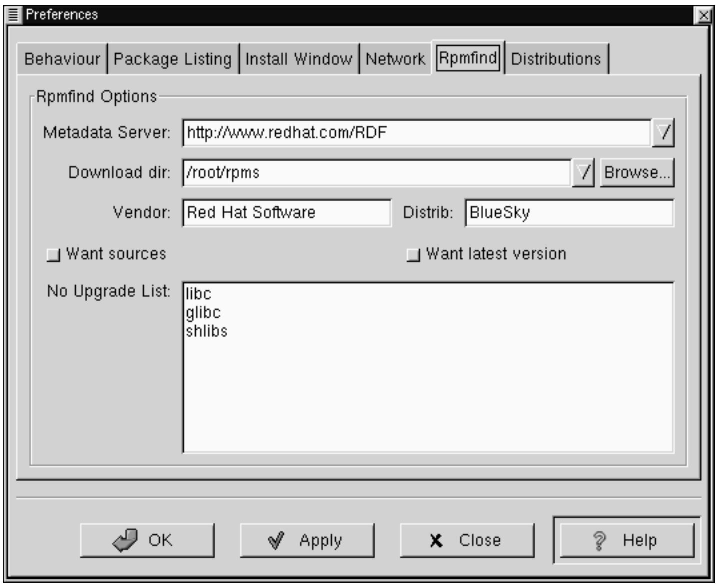


In den Registern **Rpmfind** und **Distributions** finden Sie Einstellungen und Funktionen, die denen der Option **Websuche** entsprechen.

Das Rpmfind-System wurde von Daniel Veillard entwickelt und ermöglicht es dem Benutzer, das Internet unter Angabe des Namens, der Inhaltsangabe, der Architektur usw. nach Paketen zu durchsuchen (siehe Abbildung 6–8, *Das Fenster Rpmfind*).

Dem Benutzer steht es frei, die für sein System am besten geeigneten Pakete herunterzuladen und zu installieren. Weitere Informationen über Rpmfind finden Sie unter http://rpmfind.net/.

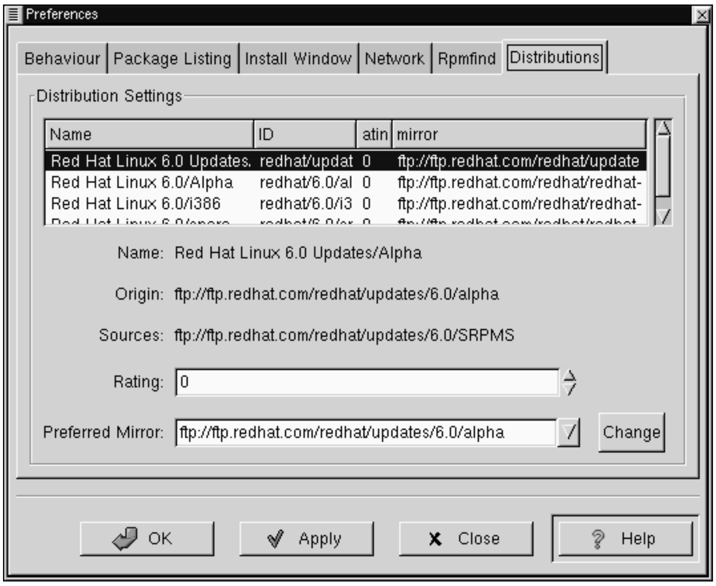
Abbildung 6–8 Das Fenster Rpmfind



Der **Metadata-Server** richtet den Server zur Verwendung bei Suchvorgängen ein. Der Eintrag **Download dir:** ermöglicht es Ihnen anzugeben, wo die Dateien gespeichert werden sollen.

Zusätzlich können Sie den Namen des Händlers und der Distribution eingeben sowie festlegen, ob Quellen und/oder aktuelle Dateien gesucht werden sollen.

Abbildung 6–9 Verteilungseinstellungen in Voreinstellungen



Im Register **Distributionen** können Sie festlegen, nach welchen Kriterien das am besten geeignete Paket aus den von Rpmfind ausgegebenen Suchergebnissen ausgewählt werden soll. Außerdem können Sie angeben, welche Mirror-Site als Alternative für das Herunterladen herangezogen werden soll. Je höher Sie die markierte Datei einstufen (siehe Abbildung 6–9, *Verteilungseinstellungen in Voreinstellungen*), desto höher ist die Priorität, die dieser zugewiesen wird. Wenn Sie hingegen eine niedrige Einstufung vornehmen (z.B. -1), bedeutet dies, dass Sie ein bestimmtes Paket eher nicht verwenden möchten.

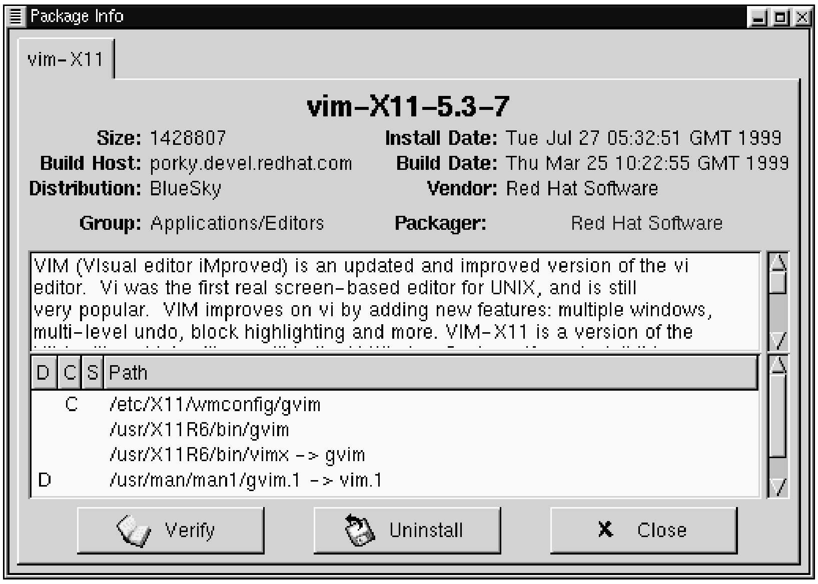
6.5 Bearbeiten von Paketen

6.5.1 Anfragen von Paketen

Die einfachste Methode zum Anfragen von Paketen ist die Verwendung der Menüoption **Anfragen**. Wenn Sie eine Anfrage für mehr als ein Paket durchführen möchten, treffen Sie Ihre Auswahl und klicken auf den Button **Anfragen** im Menü.

Nun wird ein Dialogfeld ähnlich wie in der Abbildung Abbildung 6–10, *Anfragefenster* angezeigt. Je mehr Pakete Sie anfragen, desto mehr "Register" erscheinen im Feld **Anfragen**. Jedes Register repräsentiert ein Fenster **Anfragen** für ein Paket.

Abbildung 6–10 Anfragefenster



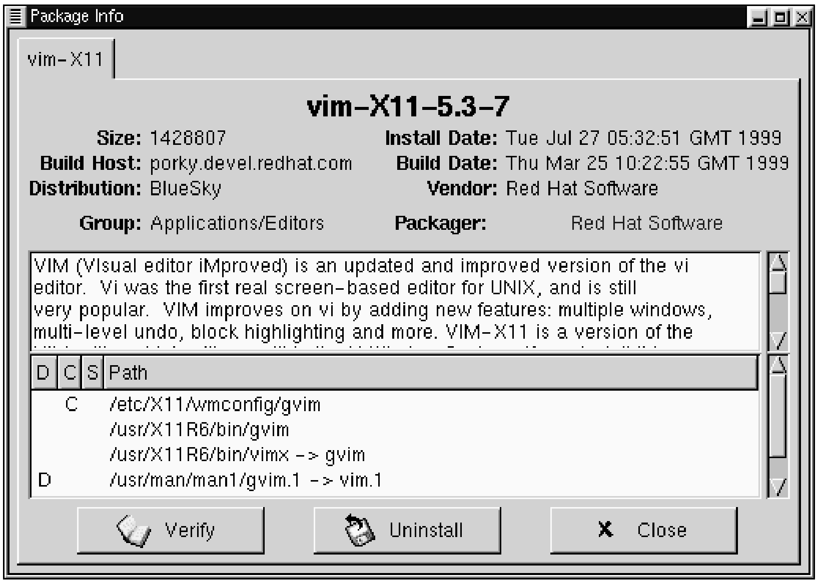
Der Name des Pakets wird oben im Feld angezeigt. Darunter befinden sich zwei Spalten mit aufgelisteten Informationen. Unterhalb dieser Informationen sehen Sie einen Anzeigebereich, in dem die Paketdateien aufgeführt werden.

Die linke Spalte der Informationsliste enthält die Größe der Datei, den Computer, auf dem die Datei gefunden wurde, den Namen der Paket-Distribution und die Gruppe, der das Paket funktionsmäßig zuzuordnen ist.

Die rechte Spalte enthält das Installationsdatum des Pakets auf Ihrem Computer, das Erstellungsdatum des Pakets, den Namen des Händlers und den Namen der Gruppe, die die Software gepackt hat. Wenn das Paket noch nicht auf Ihrem Rechner installiert wurde, steht an dieser Stelle der Hinweis "nicht installiert". Wenn Sie auf den Namen klicken, der auf **Packager** folgt, wird das E-Mail-Programm Ihres Browsers in compse geöffnet, so dass Sie dem Anbieter des Software-Pakets eine E-Mail schreiben können.

Die URL des Entwicklers der Anwendung erscheint zentriert im unteren Bereich der Informationsliste (siehe Abbildung 6–11, *URL im Abfragefenster*). Ähnlich wie bei der E-Mail-Funktion des Eintrags **Packager** wird nach dem Klicken auf die URL der Browser geöffnet und die entsprechende Website aufgerufen.

Abbildung 6–11 URL im Abfragefenster



Unterhalb der Beschreibung wird eine Liste der in dem Paket enthaltenen Dateien angezeigt. Erscheint in der Spalte links neben dem Pfad ein `D`, dann handelt es sich bei der entsprechenden Datei um eine Dokumentationsdatei, die Hilfe zur Verwendung des Programms enthält. Steht dagegen in der entsprechenden Spalte ein `C`, dann ist die Datei eine Konfigurationsdatei. In der Spalte `S` können Sie den "Status" des Pakets sehen. Hier erhalten Sie die notwendigen Informationen, falls Paketdateien als "fehlend" festgestellt wurden (was möglicherweise auf ein Problem mit dem gesamten Paket hinweist).

Wenn Sie ein bereits installiertes Paket anfragen, werden im unteren Bereich des Dialogfelds zwei zusätzliche Buttons angezeigt: **Prüfen** und **Deinstallieren**. Wenn Sie ein noch nicht installiertes Paket anfragen, tragen die Buttons die Beschriftung **Installieren**, **Upgrade** und **Unterschrift prüfen**.

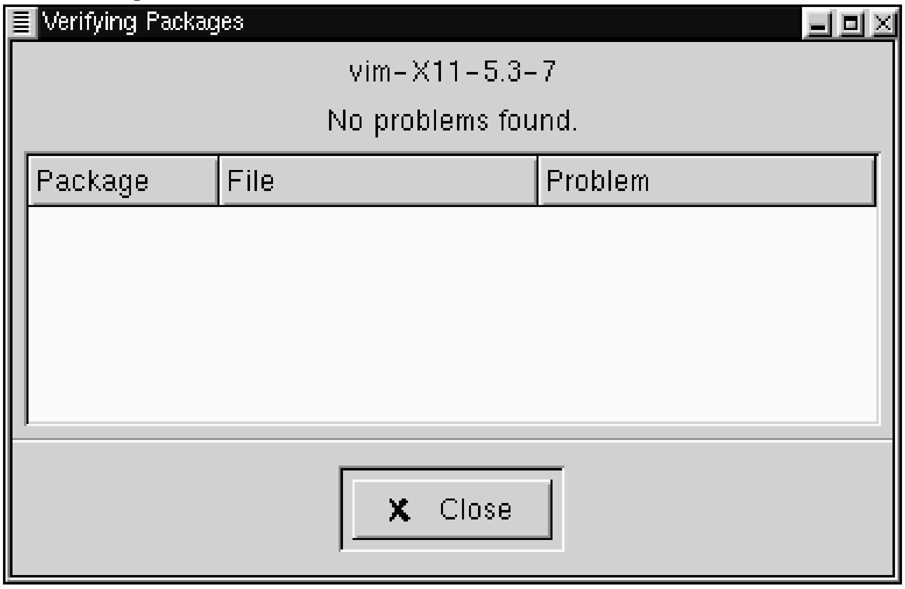
Um das Anfragefenster zu schließen, ohne eine Aktion auszuführen, klicken Sie mit der linken Maustaste oben rechts im Fensterbalken auf das **X**.

6.5.2 Prüfen von Paketen

Beim Überprüfen eines Pakets werden sämtliche Dateien in dem Paket geprüft, um sicherzustellen, dass sie mit den in Ihrem System vorhandenen übereinstimmen. Die Prüfsumme, die Dateigröße, die Berechtigungen und die Eigentümerattribute werden mit den Aufzeichnungen der Datenbank abgeglichen. Diese Überprüfung kann vorgenommen werden, wenn Sie vermuten, dass eine der Dateien des Programms aus irgendeinem Grund beschädigt wurde.

Das Auswählen der Pakete für die Überprüfung ist vergleichbar mit dem Auswählen der Pakete für eine Anfrage. Wählen Sie die Pakete im Anzeigefenster aus, und verwenden Sie den Button **Prüfen** in der Symbolleiste, oder wählen Sie die Menüoption **Pakete** => **Prüfen**. Ein Fenster ähnlich dem in Abbildung 6–12, *Verifikationsfenster* wird geöffnet.

Abbildung 6–12 Verifikationsfenster



Während das Paket überprüft wird, sehen Sie den Fortschritt des Vorgangs im Fenster **Prüfen**. Wenn bei der Überprüfung Probleme festgestellt wurden, werden diese im Hauptanzeigebereich beschrieben.

6.5.3 Deinstallieren von Paketen

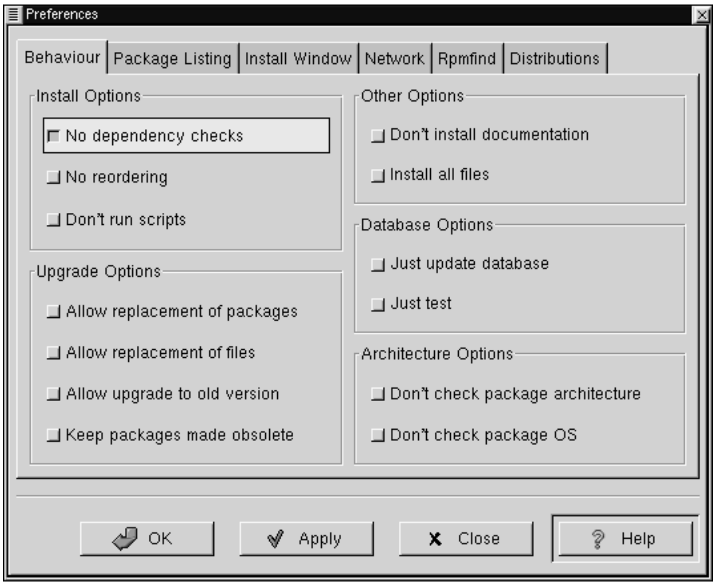
Beim Deinstallieren eines Pakets wird die Anwendung samt der zugeordneten Dateien vom Computer entfernt. Wenn ein Paket deinstalliert wird, werden sämtliche von ihm verwendeten Dateien, die nicht von anderen Paketen in Ihrem System benötigt werden, ebenfalls entfernt. Geänderte Konfigurationsdateien werden in `<Dateiname>.rpmsave` kopiert, so dass Sie sie später erneut verwenden können.

Bitte beachten

Bedenken Sie, dass Sie als Root angemeldet sein müssen, um Pakete deinstallieren zu können.

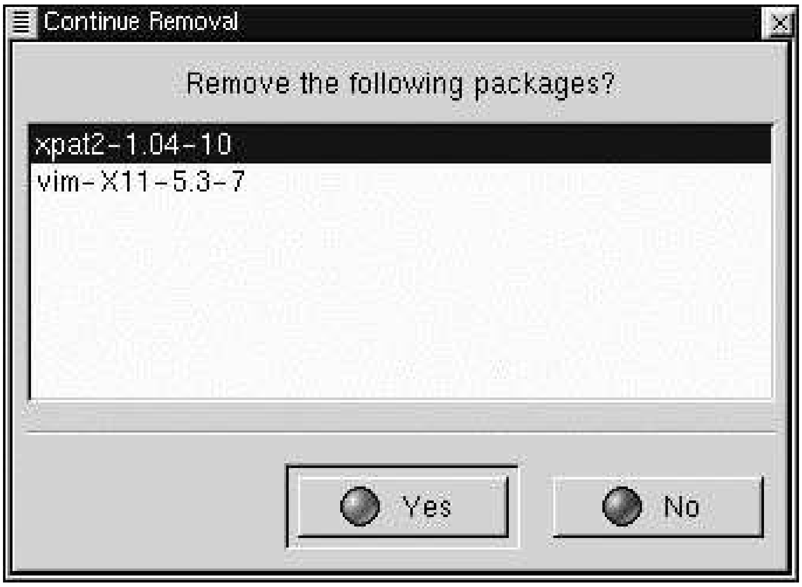
Falls durch die Deinstallation eines Pakets "Abhängigkeiten" verletzt würden (was andere Anwendungen beeinträchtigen könnte, die eine oder mehrere der zu entfernenden Dateien des Pakets benötigen), erscheint ein Dialogfeld, das Sie auffordert, die Löschung zu bestätigen. Dieser Fall tritt ein, wenn Sie das Kontrollkästchen **"Keine Abhängigkeitsprüfung"** im Menü **Einstellungen** nicht aktiviert haben (siehe Abbildung 6–13, *Das Register Verhalten in Einstellungen*).

Abbildung 6–13 Das Register Verhalten in Einstellungen



Es gibt verschiedene Methoden zum Entfernen eines ausgewählten Pakets: im Menü, unter **Pakete**, mit der Symbolleiste und mit der Funktion **Anfrage**. Falls Sie mehr als ein Paket gleichzeitig entfernen möchten, können Sie entweder eine schrittweise oder eine globale Markierung vornehmen. Dies geschieht auf die gleiche Weise wie beim Installieren, beim Anfragen oder beim Prüfen. Angaben zu den markierten Paketen werden in der Statusleiste am unteren Rand des Hauptfensters angezeigt. Da Sie mehr als ein Paket gleichzeitig entfernen können, sollten Sie bei der Auswahl der zu entfernenden Pakete sorgfältig vorgehen.

Abbildung 6–14 Dialogfeld für die Deinstallation



Wenn Sie die Deinstallation gestartet haben, fordert Gnome-RPM Sie auf, den Vorgang zu bestätigen. Dazu wird ein Fenster ähnlich dem in Abbildung 6–14, *Dialogfeld für die Deinstallation* angezeigt. Sämtliche zu deinstallierende Pakete werden aufgelistet. Schauen Sie sich die Auswahl noch einmal genau an, um sicherzustellen, dass keine noch benötigten Dateien gelöscht werden. Durch Klicken auf den Button **Yes** wird der Deinstallationsvorgang endgültig gestartet. Nach der Deinstallation sind die entfernten Pakete und Gruppen aus sämtlichen Fenstern verschwunden, in denen sie sich zuvor noch befanden.

Aktualisieren von Paketen

Wenn eine neue Version eines Pakets erscheint, können Sie sie problemlos auf Ihrem System installieren. Wählen Sie die Pakete aus dem Fenster der verfügbaren Pakete auf die gleiche Weise aus, wie Sie auch Pakete zur Installation auswählen. Sie können den Vorgang sowohl mit dem Button **Upgrade** in der Symbolleiste als auch im Menü **Operations** => **Upgrade** starten. Pakete werden also, wie auch bei der Installation eines neuen Pakets, einfach hinzugefügt (**Hinzufügen**).

Während der Aktualisierung sehen Sie eine Fortschrittsanzeige, ähnlich wie beim Installieren von Paketen. Bei Abschluss des Vorgangs wurden alle alten Versionen der Pakete entfernt, sofern Sie nichts anderes angegeben haben (weitere Informationen finden Sie in Abschnitt 6.4, *Konfiguration*).

Es ist viel vorteilhafter, eine Aktualisierung durchzuführen, als alte Versionen eines Pakets zu deinstallieren und dann die neue Version zu installieren. Wenn Sie die Option Aktualisieren verwenden, stellen Sie dadurch sicher, dass sämtliche Änderungen, die Sie an den Konfigurationsdateien des Pakets vorgenommen haben, ordnungsgemäß erhalten bleiben. Bei einer Deinstallation und einer anschließenden Neuinstallation des aktuellen Pakets könnten diese Änderungen dagegen verloren gehen.

Wenn während der Installation der Festplattenplatz zur Neige geht, kann der Vorgang nicht erfolgreich beendet werden. Das Paket, bei dessen Installation der Fehler auftrat, hat möglicherweise einige Dateien hinterlassen. Sie sollten daher das Paket neu installieren, nachdem Sie ausreichend Festplattenplatz verfügbar gemacht haben.

7 Lightweight Directory Access Protocol (LDAP)

7.1 Was ist LDAP?

LDAP (Lightweight Directory Access Protocol) wurde als offener Standard für globale oder lokale Verzeichnisdienste im Netzwerk und/oder im Internet entwickelt. Ein Verzeichnis wird dabei im Prinzip ähnlich wie ein Telefonbuch betrachtet. LDAP kann auch andere Informationen verarbeiten, doch wird es zurzeit hauptsächlich dazu verwendet, Namen mit Telefonnummern und E-Mail-Adressen zu verknüpfen. Die Verzeichnisse sind so konzipiert, dass ein hohes Anfragevolumen unterstützt wird, wobei sich die Daten im Verzeichnis jedoch nicht sehr häufig ändern sollten.

LDAP ist viel nützlicher als ein Telefonbuch aus Papier, da LDAP von seiner Konzeption her in ähnlicher Weise wie der Domain Name Service (DNS) die Verbreitung über LDAP-Server im gesamten Internet unterstützt. Das DNS-System ist das Adressbuch des Internet, indem es ständig die paarweise Zuordnung von Domänennamen/IP-Adressen auf dem Laufenden hält. DNS-Server teilen Netzwerkrechnern mit, wohin Datenpakete zu verschicken sind. In Zukunft könnte LDAP dieselbe Art von globalem Zugang auf viele verschiedene Arten von Verzeichnisinformationen ermöglichen. Zurzeit sind LDAP-Verzeichnisdienste allerdings eher in einzelnen großen Organisationen wie Hochschulen oder Unternehmen verbreitet.

LDAP ist ein Client-Server-System. Ein LDAP-Client nimmt Verbindung mit einem LDAP-Server auf und ruft entweder Informationen ab oder liefert Informationen, die in das Verzeichnis aufgenommen werden müssen. Der Server beantwortet die Anfrage, gibt anderenfalls die Anfrage an einen anderen LDAP-Server weiter oder übernimmt die Informationen in sein Verzeichnis.

LDAP wird manchmal auch als **X.500 Lite** bezeichnet. X.500 ist ein internationaler Standard für Verzeichnisse. X.500 ist mit umfangreichen Funktionen ausgestattet, doch gleichzeitig sehr komplex und erfordert hohe Rechenleistung und das vollständige OSI-Schichtenmodell. Im Gegensatz dazu kann LDAP ohne weiteres auf einem PC und über TCP/IP ausgeführt werden. LDAP kann auf X.500-Verzeichnisse zugreifen, unterstützt jedoch nicht alle Funktionen von X.500.

In diesem Kapitel wird die Konfiguration und Verwendung von OpenLDAP behandelt, einer offenen LDAP-Implementierung. OpenLDAP enthält `slapd`, einen autonomen LDAP-Server, `slurpd`, einen autonomen LDAP-Replikationsserver, Bibliotheken mit LDAP-Implementierung, Dienstprogramme, Tools und Beispiel-Clients.

7.2 Vor- und Nachteile von LDAP

Der Hauptvorteil von LDAP ist die Verdichtung von bestimmten Informationsarten in Ihrer Organisation. So können zum Beispiel alle Benutzerlisten in Ihrer Organisation in einem LDAP-Verzeichnis untergebracht werden. Das Verzeichnis kann von jedem LDAP-fähigen Anwendungsprogramm abgefragt werden, das diese Informationen benötigt. Daneben kann das Verzeichnis auch von Benutzern verwendet werden, die entsprechende Informationen benötigen.

Weitere Vorteile von LDAP sind die leichte Implementierung (im Vergleich zu X.500) und seine gut durchdachte Anwendungsprogrammierschnittstelle (Application Programming Interface, API). Dadurch ist es wahrscheinlich, dass die Zahl der LDAP-fähigen Anwendungsprogramme und LDAP-Gateways in Zukunft zunehmen wird.

Auf der anderen Seite kann LDAP nur in Verbindung mit LDAP-fähigen Anwendungsprogrammen oder LDAP-Gateways verwendet werden. Wie bereits erwähnt, wird die Verwendung von LDAP zunehmen. Zurzeit sind jedoch erst wenige LDAP-fähige Anwendungsprogramme für Linux verfügbar. Hinzu kommt, dass LDAP die Funktionen zur Zugangskontrolle zwar in bestimmtem Umfang unterstützt, jedoch nicht über so viele Sicherheitsmerkmale wie X.500 verfügt.

7.3 Anwendungsmöglichkeiten für LDAP

Es gibt mehrere Netscape-Anwendungen einschließlich Netscape Roaming Access, die LDAP-fähig sind. Sendmail kann über LDAP Adressen abfragen. In Ihrer Organisation kann LDAP als organisationsweites Verzeichnis und/oder als Namensdienst verwendet werden (anstelle von NIS oder normalen Dateien). Sie können sogar mit einem persönlichen LDAP-Server Ihr E-Mail-Adressbuch aktuell halten (siehe Abschnitt 7.10, *LDAP-Ressourcen im Internet*).

Über das Modul pam_ldap kann LDAP als Authentifizierungsdienst verwendet werden. LDAP wird häufig als zentraler Authentifizierungsserver verwendet. Dadurch können die Benutzer des Systems eine einheitliche Anmeldeprozedur für Konsolen, POP-Server, IMAP-Server, Rechner mit Samba-Netzwerkanbindung und sogar Windows NT-Rechner verwenden. Mit LDAP kann für die Anmeldung auf diesen Systemen dieselbe Benutzer-ID und dasselbe Passwort verwendet werden. Das Modul pam_ldap ist im Paket nss_ldap enthalten.

7.4 LDAP-Terminologie

Ein **Eintrag** (Entry) stellt in einem LDAP-Verzeichnis eine Einheit dar. Ein Eintrag wird durch seinen **eindeutigen Namen** (Distinguished Name, DN) identifiziert bzw. referenziert.

Ein Eintrag besitzt Attribute, bei denen es sich wiederum um direkt mit dem Eintrag verbundene einzelne Informationen handelt. Eine Organisation könnte zum Beispiel ein LDAP-Eintrag sein. Mit dieser Organisation verknüpfte Attribute können zum Beispiel die Faxnummer, die Adresse usw. sein. Auch Mitarbeiter können Einträge in einem LDAP-Verzeichnis sein. Übliche Attribute für Mitarbeiter sind Telefonnummern und E-Mail-Adressen.

Bestimmte Attribute sind obligatorisch, während andere Attribute optional sind. In einer **Objektklasse** (Objectclass) ist festgelegt, welche Attribute obligatorisch und welche optional sind. Die Objektklassendefinitionen sind in der Datei slapd.oc.conf abgelegt.

Das **LDAP-Datenaustauschformat** (LDAP Data Interchange Format, LDIF) ist ein ASCII-Textformat für LDAP-Einträge. Dateien, die Daten von einem LDAP-Server importieren oder zu einem LDAP-Server exportieren, müssen im LDIF-Format vorliegen. Ein LDIF-Eintrag sieht folgendermaßen aus:

```
[<id>]
dn: <eindeutiger Name>
<Attributtyp>: <Attributwert>
<Attributtyp>: <Attributwert>
<Attributtyp>: <Attributwert>
```

Ein Eintrag kann so viele Paare <Attributtyp>: <Attributwert> haben, wie erforderlich sind. Eine leere Zeile markiert das Ende eines Eintrags und den Beginn eines neuen Eintrags.

Alle Angaben innerhalb der spitzen Klammern (< >) sind variabel und können mit Ausnahme von <id> beim Hinzufügen eines LDAP-Eintrags von Ihnen festgelegt werden. Die <id> ist eine Zahl, die normalerweise von LDAP-Tools festgelegt wird, wenn Sie einen Eintrag hinzufügen. In der Regel müssen Sie diese Zahl nicht selbst festlegen.

7.5 OpenLDAP Dateien

Die Konfigurationsdateien von OpenLDAP werden im Verzeichnis `/etc/openldap` installiert. Wenn Sie im Verzeichnis `/etc/openldap` den Befehl `ls` eingeben, wird etwa Folgendes angezeigt:

```
ldap.conf        ldapsearchprefs.conf  slapd.at.conf  slapd.oc.conf
ldapfilter.conf  ldaptemplates.conf    slapd.conf
```

Die für Sie wichtigen Dateien sind `slapd.conf`, `slapd.at.conf` und `slapd.oc.conf`. Die Datei `slapd.conf` enthält Konfigurationsinformationen für den Dämon `slapd` und für alle Datenbank-Backends. Vor dem Start des Dämons `slapd` müssen einige Änderungen an der Datei `slapd.conf` vorgenommen werden.

Die Datei `slapd.at.conf` enthält **Attributsyntaxdefinitionen** für das LDAP-Verzeichnis. Attributsyntaxdefinitionen beschreiben den Informationstyp des Attributs. Es gibt fünf Möglichkeiten:

- bin - binäre Informationen
- ces - Zeichenkette, bei der zwischen Groß- und Kleinschreibung unterschieden wird
- cis - Zeichenkette, bei der zwischen Groß- und Kleinschreibung nicht unterschieden wird
- tel - eine Telefonnummer (Leerzeichen und Bindestriche werden ignoriert)
- dn - der eindeutige Name

Hier als Beispiel Attributsyntaxdefinitionen aus einer typischen Datei `slapd.at.conf`:

```
attribute       photo                                   bin
attribute       personalsignature                       bin
attribute       jpegphoto                               bin
attribute       audio                                   bin
attribute       labeledurl                              ces
attribute       ref                                     ces
attribute       userpassword                            ces
attribute       telephonenumber                         tel
```

Manche LDAP-fähigen Anwendungsprogramme erfordern die Anpassung der Datei `slapd.at.conf`. In den meisten Fällen sind spezielle Attributsyntaxdefinitionen hinzuzufügen.

Die Datei `slapd.oc.conf` enthält die **Objektklassendefinitionen** für ein LDAP-Verzeichnis. Die Objektklassendefinitionen geben für spezielle Objektklassen an, welche Attribute obligatorisch und welche optional sind.

Der folgende Auszug einer typischen Datei `slapd.oc.conf` enthält die Objektklassendefinitionen für die Objektklassen top, alias und referral:

```
objectclass top
        requires
                objectClass

objectclass alias
        requires
                aliasedObjectName,
                objectClass

objectclass referral
        requires
                ref,
                objectClass
```

Je nachdem, wie Sie Ihr LDAP-Verzeichnis verwenden wollen, kann es erforderlich sein, die Objektklassendefinitionen in Ihrer Datei `slapd.oc.conf` zu ändern. Wenn Sie zum Beispiel ein LDAP-Verzeichnis von Mitarbeitern für die Verwendung in Ihrer Organisation erstellen, gibt es wahrscheinlich für bestimmte Objektklassen spezielle obligatorische Attribute, die außerhalb Ihrer Organisation keine Verwendung finden (z.B. könnte eine Mitarbeiteridentitätsnummer innerhalb Ihrer Organisation ein obligatorisches Attribut für eine Objektklasse "Mitarbeiter" sein).

7.6 OpenLDAP Dämonen und Dienstprogramme

Das Paket OpenLDAP enthält zwei Dämonen: `slapd` und `slurpd`. Der Dämon `slapd` ist der autonome LDAP-Dämon, der für die Ausführung von LDAP erforderlich ist.

Der Dämon `slurpd` steuert die Replikation von LDAP-Verzeichnissen über ein Netzwerk. `Slurpd` teilt den Slave-Verzeichnissen Veränderungen im Master-LDAP-Verzeichnis mit. Die Ausführung von `slurpd` ist nur erforderlich, wenn mehr als ein LDAP-Server an Ihr Netzwerk angeschlossen ist. Bei mehreren LDAP-Servern muss `slurpd` zur Synchronisierung der LDAP-Verzeichnisse ausgeführt werden.

OpenLDAP enthält außerdem einige Dienstprogramme zum Hinzufügen, Ändern und Löschen von Einträgen in einem LDAP-Verzeichnis. Das Tool `ldapmodify` dient zum Ändern von Einträgen in einer LDAP-Datenbank. Das Dienstprogramm `ldapadd` wird zum Hinzufügen von Einträgen zu Ihrem Verzeichnis verwendet (`ldapadd` ist eigentlich ein Hardlink mit `ldapmodify -a`). `Ldapsearch` dient zum Suchen nach Einträgen und `ldapdelete` zum Löschen von Einträgen. Das Tool `ldif2ldbm` konvertiert eine LDIF-Datei in eine LDBM-Datenbank.

Weitere Informationen zu diesen Dienstprogrammen finden Sie in den jeweiligen man-Seiten.

7.7 Module zum Hinzufügen von zusätzlichen Funktionen zu LDAP

Red Hat Linux enthält die folgenden Pakete mit zusätzlichen Funktionen für LDAP:

Das Modul `nss_ldap` ist ein LDAP-Modul für den **Solaris Nameservice Switch** (NSS). Bei NSS handelt es sich um eine Reihe von C-Bibliotheks-Erweiterungen, die für den Zugriff auf Informationen in LDAP-Verzeichnissen erforderlich sind. Dies kann den Namensdienst **Network Information Service** (NIS) und/oder konventionelle Dateien ersetzen oder ergänzen. Das Modul `nss_ldap` wird für die Verwendung von LDAP als Linux-spezifischer Namensdienst benötigt.

Das Modul `pam_ldap` wird für die Integration der LDAP-Authentifizierung in die API der einfügbaren Authentifizierungsmodule (Pluggable Authentication Modules, PAM) benötigt. Bei Verwendung von `pam_ldap` können die Benutzer ihr Passwort mit Hilfe von LDAP-Verzeichnissen bestätigen lassen bzw. ändern. Die Module `nss_ldap` und `pam_ldap` sind im Paket `nss_ldap` enthalten.

Red Hat Linux enthält außerdem die LDAP-Module für den Apache Web-Server. Das Modul `auth_ldap` führt die Authentifizierung von HTTP-Clients im Vergleich mit den Benutzereinträgen in einem LDAP-Verzeichnis durch. Das Modul `php-ldap` macht die Skriptsprache PHP4, die in HTML eingebettet werden kann, LDAP-fähig. Die Module `auth_ldap` und `php-ldap` müssen als **Dynamic Shared Objects** (DSOs) in Apache einkompiliert werden.

7.8 LDAP-HowTo (Bedienungsanleitung): Kurzüberblick

Dieser Abschnitt gibt einen Kurzüberblick über die nötigen Schritte zur Aktivierung eines LDAP-Verzeichnisses.

1. Stellen Sie sicher, dass das RPM-Paket `openldap` und alle weiteren von LDAP benötigten RPM-Pakete installiert sind.
2. Eine Anleitung zur Verwendung von LDAP in Ihrem System finden Sie sowohl im Quick Start Guide auf der OpenLDAP-Website (http://www.openldap.org/faq/data/cache/172.html, beginnen Sie mit "Create configuration file for slapd", da die LDAP-Dateien bereits installiert sind) als auch in den Linux-LDAP-HOWTOs (http://www.linux-doc.org/HOWTO/LDAP-HOWTO.html). In beiden Dokumentationen werden die weiteren Schritte beschrieben.
3. Passen Sie die Datei `slapd.conf` an Ihr System an.
4. Starten Sie `slapd`.

5. Erstellen Sie Ihr LDAP-Verzeichnis (Beispiele zu LDAP-Einträgen finden Sie auf der Website von PADL Software unter http://www.padl.com/ldap_examples.html).
6. Fügen Sie Einträge mit Hilfe von `ldapadd` oder eines Skripts in Ihr LDAP-Verzeichnis ein.
7. Mit `ldapsearch` können Sie testen, ob `slapd` funktioniert.
8. Wenn Sie an diesem Punkt angelangt sind, sollte Ihr LDAP-Verzeichnis eingerichtet sein. Der nächste Schritt ist die Konfiguration Ihrer LDAP-fähigen Anwendungsprogramme für die Verwendung des LDAP-Verzeichnisses.

7.9 Konfigurieren Ihres Systems für die Authentifizierung mit OpenLDAP

Dieser Abschnitt gibt einen kurzen Überblick über die Konfiguration Ihres Red Hat Linux-Systems für die Authentifizierung mit OpenLDAP. Wenn Sie kein OpenLDAP-Experte sind, benötigen Sie wahrscheinlich eine weiter gehende Dokumentation, als wir Ihnen hier bieten können. Weitere Informationen finden Sie in den in Abschnitt 7.10, *LDAP-Ressourcen im Internet* angegebenen Literaturhinweisen.

7.9.1 Installieren der erforderlichen LDAP-Pakete

Zuerst müssen Sie sowohl auf dem LDAP-Server als auch auf dem LDAP-Client überprüfen, ob die entsprechenden Pakete installiert sind. Für den LDAP-Server wird das Paket `openldap` benötigt.

Auf den LDAP-Client-Rechnern müssen die folgenden Pakete installiert sein: `openldap`, `auth_ldap` und `nss_ldap`.

7.9.2 Anpassen der Konfigurationsdateien

Anpassen von `/etc/openldap/slapd.conf`

Die Datei `slapd.conf` ist in `/etc/openldap` abgelegt und enthält die Konfigurationsinformationen für Ihren LDAP-Server `slapd`. Sie müssen diese Datei an Ihre Domäne und Ihren Server anpassen.

Die suffix-Zeile gibt die Domäne an, für die der LDAP-Server Informationen bereitstellt. Die Suffix-Zeile sollte wie folgt geändert werden:

```
suffix   "dc=Ihre-Domäne, dc=com"
```

Hier muss der Name Ihrer Domäne eingetragen werden. Beispiel:

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

oder

```
suffix   "dc=acmeuniversity, dc=org"
```

Der Eintrag rootdn ist der eindeutige Name (DN) für einen Benutzer, dem von den Parametern der Zugangskontrolle oder Benutzerverwaltung keine Beschränkungen für die Verwaltung des LDAP-Verzeichnisses auferlegt sind. Der Benutzer rootdn ist sozusagen Root für das LDAP-Verzeichnis. Die rootdn-Zeile lautet standardmäßig:

```
rootdn  "cn=root, dc=Ihre-Domäne, dc=com"
```

in einen Eintrag der Form:

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

oder

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

Ändern Sie die rootpw-Zeile von:

```
rootpw   secret
```

in zum Beispiel:

```
rootpw  {crypt}s4L9sOIJo4kBM
```

Im obigen Beispiel wird ein verschlüsseltes Passwort verwendet, eine viel bessere Lösung, als das Root-Passwort im Klartext in der Datei `slapd.conf` abzuspeichern. Zum Erstellen dieser verschlüsselten Zeichenkette müssen Sie diese entweder aus der Datei `passwd` kopieren oder Perl verwenden:

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

In der obigen Perl-Zeile ist `salt_string` eine aus zwei Zeichen bestehende Salt-Zeichenkette und `passwd` die Klartextversion des Passworts.

Sie könnten auch einen passwd-Eintrag aus /etc/passwd kopieren. Das funktioniert allerdings nicht, wenn der passwd-Eintrag ein MD5-Passwort ist (Standard in Red Hat Linux 7.0).

Anpassen von ldap.conf

Passen Sie die Dateien ldap.conf in /etc und in /etc/openldap auf dem LDAP-Server und den -Clients an.

Passen Sie /etc/ldap.conf, die Konfigurationsdatei für nss_ldap und pam_ldap, an Ihre Organisation und Suchdatenbank an. Die Datei /etc/openldap/ldap.conf ist die Konfigurationsdatei für Befehlszeilentools wie ldapsearch, ldapadd usw. und muss ebenfalls im Rahmen der LDAP-Einrichtung angepasst werden. Auf den Client-Rechnern müssen beide Dateien an Ihr System angepasst werden.

Anpassen von /etc/nsswitch.conf

Um nss_ldap verwenden zu können, müssen Sie ldap in den entsprechenden Feldern in der Datei /etc/nsswitch.conf hinzufügen. (Vorsicht beim Bearbeiten dieser Datei. Hier sind genaue Kenntnisse der Zusammenhänge erforderlich.) Beispiel:

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

PAM und LDAP

Führen Sie authconfig aus, und wählen Sie die Option **Use LDAP** aus, damit Sie standardmäßige PAM-fähige Anwendungsprogramme LDAP für die Authentifizierung verwenden können. (Auf PAM können wir im Rahmen dieses Überblicks über LDAP nicht eingehen. Informationen dazu finden Sie in Abschnitt 2.6, *Benutzerauthentifizierung mit PAM* und/oder in den man-Seiten zu PAM.)

7.9.3 Umwandeln Ihrer alten Authentifizierungsinformationen in das LDAP-Format

Das Verzeichnis /usr/share/openldap/migration enthält mehrere Shell- und Perl-Skripten zur Umwandlung Ihrer alten Authentifizierungsinformationen in das LDAP-Format. (Diese Skripten erfordern einen lauffähigen Perl-Interpreter auf Ihrem System.)

Zuerst müssen Sie die Datei `migrate_common.ph` an Ihre Domäne anpassen. Die Standard-DNS-Domäne muss geändert werden von:

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

in einen Eintrag der Form:

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

Die Standardannahme muss ebenfalls geändert werden von:

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

in einen Eintrag der Form:

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

Als Nächstes müssen Sie sich entscheiden, welches Skript verwendet werden soll. Die folgende Tabelle hilft Ihnen bei Ihrer Entscheidung:

Tabelle 7–1 LDAP-Umwandlungsskripten

Vorhandener Namensdienst	Wird LDAP ausgeführt?	Verwenden Sie dieses Skript:
`/etc` konventionelle Dateien	Ja	`migrate_all_online.sh`
`/etc` konventionelle Dateien	Nein	`migrate_all_offline.sh`
NetInfo	Ja	`migrate_all_netinfo_online.sh`
NetInfo	Nein	`migrate_all_netinfo_offline.sh`

Vorhandener Namensdienst	Wird LDAP ausgeführt?	Verwenden Sie dieses Skript:
NIS (YP)	Ja	`migrate_all_nis_online.sh`
NIS (YP)	Nein	`migrate_all_nis_offline.sh`

Führen Sie das Ihrem vorhandenen Namensdienst entsprechende Skript aus.

Weitere Details finden Sie in der Datei `README` und den Dateien `migration-tools.txt` im Verzeichnis `/usr/share/openldap/migration`.

7.10 LDAP-Ressourcen im Internet

Im Internet werden viele nützliche Informationen über LDAP angeboten. Sie sollten diese Quellen nutzen, insbesondere die OpenLDAP -Website und die LDAP HOWTOs, bevor Sie LDAP in Ihrem System konfigurieren.

OpenLDAP

http://www.openldap.org

University of Michigan

http://www.umich.edu/~dirsvcs/ldap/

The SLAPD and SLURPD Administrator's Guide

http://www.umich.edu/~dirsvcs/ldap/doc/guides/slapd

Innosoft/Critical Angle

http://www.innosoft.com/ldapworld

LDAP Road Map und FAQ von Jeff Hodges

http://www.kingsmountain.com/ldapRoadmap.shtml

PADL (nss_ldap, pam_ldap and ypldapd)

http://www.padl.com/

auth_ldap

http://www.rudedog.org/auth_ldap/1.4/auth_ldap.html

Die LDAP-HOWTO

http://www.linuxdoc.org/HOWTO/LDAP-HOWTO.html

Sendmail — mit LDAP zur Adressenabfrage

http://www.stanford.edu/~bbense/Inst.html

Verwendung eines persönlichen LDAP-Servers, des Apache Web-Servers und von PHP zur Verwaltung Ihres persönlichen E-Mail-Adressbuchs

http://www.webtechniques.com/archives/1999/05/junk/junk.shtml

Weitere Informationen zu den verschiedenen LDAP-Dämonen und -Dienstprogrammen finden Sie in den jeweiligen man-Seiten.

8 Verwenden von Kerberos 5 in Red Hat Linux

Kerberos ist ein sicheres System, das Authentifizierungsdienste für Netzwerke bereitstellt. Authentifizierung bedeutet:

- die Identität der Objekte im Netzwerk wird überprüft
- es wird überprüft, ob der Netzwerkverkehr von der Quelle ausgeht, die sich als Sender ausgibt

Kerberos verwendet Benutzerpasswörter, um die Identität der Benutzer zu überprüfen. Diese Passwörter werden allerdings nie unverschlüsselt im Netzwerk versendet.

8.1 Wozu Kerberos verwenden?

Die meisten herkömmlichen Netzwerksysteme verwenden Passwort-basierte Authentifizierungsschemata. Wenn sich ein Benutzer bei einem Dienst anmelden möchte, der auf einem Netzwerkserver ausgeführt wird, muss er für jeden Dienst, für den eine Authentifizierung erforderlich ist, sein Passwort eingeben. Das Passwort wird über das Netzwerk versendet, und der Server überprüft die Identität des Benutzers mit Hilfe des Passwortes.

Werden Passwörter auf diesem Weg im Klartext übertragen (wie es allgemein üblich ist), besteht ein sehr großes Sicherheitsrisiko. Jeder Cracker, der Zugriff auf das Netzwerk und einen Paketanalysierer (Packet Sniffer) hat, kann auf diese Weise versendete Passwörter knacken.

Primäres Ziel von Kerberos ist es daher, sicherzustellen, dass Passwörter *nie* unverschlüsselt über das Netzwerk versendet werden bzw. dass sie möglichst überhaupt nicht über das Netzwerk verschickt werden. Durch die korrekte Verwendung von Kerberos wird jede Gefahr ausgeschaltet, dass solche Packet Sniffers die Passwörter in Ihrem Netzwerk abfangen.

8.2 Weshalb sollte man Kerberos nicht verwenden?

Dank Kerberos wird eine Bedrohung, die ganz allgemein für die Sicherheit im Netzwerk besteht, ausgeschaltet. Weshalb also wird Kerberos dann nicht in jedem Netzwerk verwendet? Die Implementierung von Kerberos kann sich aus mehreren Gründen schwierig gestalten:

- Es existiert keine schnelle und standardisierte skriptbasierte Lösung für das Übertragen von Benutzerpasswörtern von einer standardmäßigen UNIX-Passwortdatenbank in eine Kerberos-Passwortdatenbank. Zwar ist die Übertragung technisch möglich, doch stehen für Kerberos keine Konvertierungsskripten zur Verfügung. Weitere Informationen hierzu siehe Kerberos FAQ Question 2.23.
- Kerberos ist nur teilweise mit dem Pluggable Authentication Modules-System (PAM-System) kompatibel, das die meisten Server in Red Hat Linux verwenden. Weitere Informationen hierzu siehe Abschnitt 8.7, *Kerberos und Pluggable Authentication Modules (PAM)*.
- Damit eine Anwendung Kerberos verwenden kann, müssen ihre Quellen so modifiziert werden, dass die geeigneten Aufrufe an die Kerberos-Bibliotheken gesendet werden können. Bei einigen Anwendungen ist der hierfür erforderliche Programmieraufwand möglicherweise zu groß. Bei anderen Anwendungen müssen an dem von den Netzwerkservern und ihren Clients verwendeten Protokoll Änderungen vorgenommen werden. Auch das kann unter Umständen einen zu großen Aufwand bedeuten. Zudem besteht die Möglichkeit, dass einige Closed Source-Anwendungen einfach nicht mit Kerberos arbeiten können.
- Falls Sie sich für den Einsatz von Kerberos in Ihrem Netzwerk entscheiden, müssen Sie sich außerdem bewusst sein, dass Kerberos "entweder ganz oder gar nicht" eingesetzt wird. Wenn also noch *irgendwelche* Dienste in Verwendung bleiben, die Passwörter im Klartext übermitteln, dann besteht weiterhin Gefahr, dass Ihre Passwörter abgehört werden können, d.h., es ergibt sich für Ihr Netzwerk keinerlei Vorteil aus der Verwendung von Kerberos. Wenn Sie Ihr Netzwerk durch Kerberos sichern möchten, müssen Sie entweder **alle** Anwendungen, die Passwörter im Klartext versenden, *kerberisieren* (sie so einrichten, dass sie mit Kerberos arbeiten können), oder ganz auf die Verwendung dieser Anwendungen in Ihrem Netzwerk verzichten.

8.3 Kerberos-Terminologie

Wie jedes andere System verfügt auch Kerberos über seine eigene Terminologie. Daher sollten Sie sich zunächst mit den im Folgenden aufgeführten Begriffen vertraut machen, bevor Sie sich mit der Funktionsweise von Kerberos beschäftigen:

- ciphertext — verschlüsselte Daten
- Client — Ein Objekt im Netzwerk (ein Benutzer, ein Host oder eine Anwendung), das von Kerberos ein Ticket erhalten kann
- Credential Cache oder Ticket File — Eine Datei, die die Keys für die Verschlüsselung der Kommunikation zwischen einem Benutzer und verschiedenen Netzwerkdiensten enthält. Kerberos 5 stellt zwar einen Rahmen für die Verwendung anderer Cache-Typen (wie z.B. gemeinsam genutzten Speicher) zur Verfügung, allerdings werden Dateien besser unterstützt
- Key — Ein Datenblock, der zum Verschlüsseln bzw. Entschlüsseln von Daten verwendet wird. Verschlüsselte Daten lassen sich ohne den richtigen Key nicht bzw. nur durch wirklich leistungfähige Programme zum Herausfinden von Passwörtern entschlüsseln
- Key Distribution Center (KDC) — Ein Rechner, der Kerberos-Tickets ausgibt (manchmal auch als Ticket Granting Server oder TGS bezeichnet)
- keytab — Kurzform für **key table**, eine Datei, die eine unverschlüsselte Liste aller Principals und ihrer Keys enthält. Server holen sich die benötigten Keys aus keytab-Dateien, statt `kinit` zu verwenden. Die standardmäßige keytab-Datei ist `/etc/krb5.keytab`, wobei `kadmind` der einzige bekannte Dienst ist, der eine andere Datei verwendet (er verwendet `/var/kerberos/krb5kdc/kadm5.keytab`)
- Klartext — Unverschlüsselte Daten
- Principal — Ein Benutzer oder Dienst, der sich mit Hilfe von Kerberos authentifizieren kann. Der Name eines Principal hat das Format "*root*[/*instance*]@*REALM*". Bei einem typischen Benutzer entspricht *root* seiner Login-ID; *instance* ist dagegen optional. Wenn ein Principal über einen Instance verfügt, ist dieser von Root durch einen Schrägstrich ("/") getrennt. Bei dem

leeren String ("") handelt es sich zwar um einen gültigen Instance (der sich vom Standardinstance *NULL* unterscheidet), allerdings kann seine Verwendung zu Verwirrung führen. Alle Principals innerhalb eines Realms verfügen über ihren eigenen *Key*, der sich entweder aus ihrem Passwort (bei Benutzern) ableitet oder nach dem Zufallsprinzip erzeugt wird (bei Diensten)

- Realm (Gültigkeitsbereich) — Ein Netzwerk, das Kerberos verwendet und aus einem oder einigen Servern (auch als KDCs bezeichnet) sowie einer (potentiell sehr großen) Zahl von Clients besteht
- Service (Dienst) — Ein Programm oder Computer auf das/den über das Netzwerk zugegriffen werden kann
- Ticket — Ein temporärer Satz an elektronischen Berechtigungsnachweisen (Credentials), die die Identität eines Client für einen bestimmten Dienst verifizieren
- Ticket Granting Ticket (TGT) — Ein spezielles Ticket, das es dem Client ermöglicht, zusätzliche Tickets zu erhalten, ohne diese beim KDC anfordern zu müssen

8.4 Funktionsweise von Kerberos

Nachdem Sie sich mit einigen in Kerberos verwendeten Begriffen vertraut gemacht haben, hier nun eine vereinfachte Erläuterung der Funktionsweise des Kerberos-Authentifizierungssystems:

Wenn ein Benutzer in einem "normalen" Netzwerk, das Passwörter zur Benutzerauthentifizierung verwendet, einen Netzwerkdienst anfordert, für den eine Authentifizierung erforderlich ist, dann wird der Benutzer aufgefordert, sein Passwort einzugeben. Dieses Passwort wird dann im Klartext im Netzwerk gesendet, und der Benutzer erhält Zugriff auf den gewünschten Netzwerkdienst.

Wie bereits an anderer Stelle erwähnt, besteht das Hauptproblem darin, wie Passwörter verwendet werden können, ohne dass sie zur Authentifizierung im Netzwerk versendet werden müssen. Für dieses Problem bietet Kerberos die Lösung. In einem kerberisierten Netzwerk sind die Principals und ihre Keys in der Kerberos-Datenbank enthalten (bei Benutzern werden diese Keys von den Benutzer-Passwörtern abgeleitet). Außerdem enthält die Kerberos-Datenbank die Keys für alle Netzwerkdienste.

Wenn sich ein Benutzer in einem kerberisierten Netzwerk an seiner Workstation anmeldet, wird sein Principal für die Anforderung eines TGT an den KDC gesendet. Diese Anforderung kann entweder vom Anmeldeprogramm (also für den Benutzer transparent) oder - nachdem sich der Benutzer angemeldet hat - vom Programm `kinit` gesendet werden.

Der KDC sucht dann in seiner Datenbank nach diesem Principal. Sobald der Principal gefunden wurde, erstellt der KDC ein TGT, verschlüsselt es unter Verwendung des zu diesem Benutzer gehörenden Key und sendet es an den Benutzer zurück.

Das Anmeldeprogramm oder `kinit` entschlüsselt das TGT mit Hilfe des Benutzer-Key (den es aus dem Passwort des Benutzers errechnet). Das TGT, das nur für eine bestimmte Zeitspanne gültig ist, wird in Ihrem Credential Cache gespeichert. Die Gültigkeitsdauer ist so eingerichtet, dass ein TGT immer nur während einer bestimmten Zeitspanne (in der Regel acht Stunden) verwendet werden kann - im Gegensatz zu einem Passwort, das so lange verwendet werden kann, bis es geändert wird. Der Benutzer braucht sein Passwort erst wieder einzugeben, wenn das TGT abgelaufen ist oder er sich ab- und dann wieder neu anmeldet.

Wenn der Benutzer auf einen Netzwerkdienst zugreifen möchte, fordert das TGT beim Ticket Granting Service (TGS), der auf dem KDC ausgeführt wird, ein Ticket für den betreffenden Dienst an. Der TGS stellt ein Ticket für den gewünschten Dienst aus, das zur Authentifizierung des Benutzers verwendet wird.

Wie Sie sicherlich bereits vermutet haben, handelt es sich bei dieser Erläuterung natürlich nur um eine sehr vereinfachte Darstellung. Eine detaillierte Beschreibung der Funktionsweise von Kerberos, siehe Abschnitt 8.8, *Weitere Informationen zu Kerberos*.

Bitte beachten:

Kerberos benötigt verschiedene Netzwerkdienste, um korrekt zu arbeiten. Zunächst ist für Kerberos eine Zeitsynchronisierung zwischen den Rechnern in Ihrem Netzwerk erforderlich. Falls Sie für Ihr Netzwerk bisher kein Programm zur Zeitsynchronisierung eingerichtet haben, müssen Sie ein solches Programm einrichten. Da Kerberos zum Teil auch auf den Domain Name Service (DNS) angewiesen ist, müssen Sie sich außerdem vergewissern, dass die DNS-Einträge und -Hosts in Ihrem Netzwerk korrekt eingerichtet sind. Weitere Informationen hierzu finden Sie im *Kerberos V5 System Administrator's Guide*, der unter `/usr/share/doc/krb5-server-`*`Versionsnummer/`* im PostScript- und im HTML-Format zur Verfügung steht.

8.5 Einrichten von Kerberos 5 Servern in Red Hat Linux 7.0

Wenn Sie Kerberos einrichten, müssen Sie zuerst den/die Server installieren. Falls Sie Slave-Server benötigen, finden Sie detaillierte Informationen zum Einrichten der Beziehungen zwischen Master- und Slave-Servern im *Kerberos 5 Installation Guide* (unter `/usr/share/doc/krb5-server-`*`Versionsnummer/`*).

So installieren Sie einen Kerberos-Server:

1. Installieren Sie die Pakete `krb5-libs`, `krb5-server` und `krb5-workstation` auf dem dedizierten Rechner, auf dem Ihr KDC ausgeführt werden soll. Dieser Rechner muss sicher sein — falls möglich, sollten außer dem KDC keine weiteren Dienste auf ihm ausgeführt werden.

   Falls Sie ein GUI-Dienstprogramm (Graphical User Interface, GUI) für die Verwaltung von Kerberos verwenden möchten, sollten Sie auch das Paket `gnome-kerberos` installieren. `gnome-kerberos` enthält `krb5`, ein GUI-Tool für das Verwalten von Tickets, und `gkadmin`, ein GUI-Tool für das Verwalten von Kerberos-Realms.

2. Bearbeiten Sie die Konfigurationsdateien `/etc/krb5.conf` und `/var/kerberos/krb5kdc/kdc.conf`, so dass der Name Ihres Realms und Ihre Zuordnungen Domäne/Realm darin wiedergegeben werden. Sie können einen einfachen Realm erzeugen, indem Sie die Instances von *EXAMPLE.COM* und *example.com* durch den Namen Ihrer Domäne ersetzen (behalten Sie die Groß- und Kleinschreibung bei) und den KDC *kerberos.example.com* in den Namen Ihres Kerberos-Servers ändern. Es herrscht die Konvention, alle Namen von Realms in Großbuchstaben und alle DNS-Rechnernamen und Domänennamen in Kleinbuchstaben anzugeben. Details zu den Formaten dieser Dateien finden Sie auf den entsprechenden man-Seiten.

3. Erstellen einer Datenbank mit Hilfe des Dienstprogramms `kdb5_util` von einem Shell Prompt aus:

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

   Der Befehl `create` erstellt die Datenbank, in der die Keys für Ihren Kerberos-Realm gespeichert werden. Die Erweiterung `-s` erzwingt das Erstellen einer **stash**-Datei, in der der Key des Master-Servers gespeichert ist. Ist keine stash-Datei vorhanden, aus der der Key ausgelesen werden könnte, fordert der Kerberos-Server (`krb5kdc`) den Benutzer bei jedem Start auf, das Passwort des Master-Servers einzugeben (das zum Regenerieren des Key verwendet werden kann).

4. Bearbeiten Sie die Datei `/var/kerberos/krb5kdc/kadm5.acl`. `kadmind` verwendet diese Datei, um festzustellen, welche Principals Zugriff auf die Kerberos-Datenbank haben und über welche Art von Zugriff sie verfügen. Für die meisten Organisationen reicht eine einzelne Zeile aus:

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

   Die meisten Benutzer werden in der Datenbank durch einen einzelnen Principal repräsentiert (mit einem Instance vom Typ *NULL*; z.B.: *joe@EXAMPLE.COM*). Bei dieser Konfiguration haben Benutzer, die über einen zweiten Principal mit einem Instance vom Typ *admin* verfügen (z.B.: *joe/admin@EXAMPLE.COM*), umfassenden Zugriff auf die Kerberos-Datenbank des Realms.

Sobald kadmind auf dem Server gestartet wurde, kann jeder Benutzer auf die Serverdienste zugreifen, indem er auf einem beliebigen Client oder Server im Realm kadmin oder gkadmin ausführt. Allerdings können nur in der Datei kadm5.acl aufgeführte Benutzer die Datenbank beliebig modifizieren (davon ausgenommen sind Änderungen an ihrem eigenen Passwort).

Bitte beachten:

Die Dienstprogramme kadmin und gkadmin kommunizieren mit dem kadmind-Server über das Netzwerk. Bevor Sie zu Verwaltungszwecken über das Netzwerk eine Verbindung mit dem Server herstellen können, müssen Sie einen Principal erzeugen. Verwenden Sie dazu den Befehl kadmin.local:

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

5. Starten Sie Kerberos mit Hilfe der folgenden Befehle:

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

6. Fügen Sie für Ihre Benutzer Principals hinzu. Verwenden Sie dazu den kadmin-Befehls addprinc oder die gkadmin-Menüoption **Principal** => **Add** (Hinzufügen).

7. Überprüfen Sie, ob der Server Tickets ausstellt. Führen Sie zunächst kinit aus, um ein Ticket zu erhalten, und speichern Sie es in einer Credential Cache-Datei. Zeigen Sie anschließend mit klist eine Liste der in Ihrem Cache enthaltenen Berechtigungsnachweise (Credentials) an, und löschen Sie den Cache und die darin enthaltenen Berechtigungsnachweise mit Hilfe von kdestroy.

Bitte beachten:

Standardmäßig verwendet `kinit` für Ihre Authentifizierung den Anmeldenamen des Benutzers, als der Sie aktuell angemeldet sind. Entspricht der Benutzer, unter dem Sie sich angemeldet haben, keinem der Principals in Ihrer Kerberos-Datenbank, wird eine Fehlermeldung ausgegeben. In diesem Fall brauchen Sie `kinit` nur den Namen Ihres Principal als Argument in der Befehlszeile anzugeben.

Sobald Sie die oben beschriebenen Schritte durchgeführt haben, sollte Ihr Kerberos-Server vollständig eingerichtet sein und laufen. Als Nächstes müssen Sie die Kerberos-Clients einrichten.

8.6 Einrichten von Kerberos 5 Clients in Red Hat Linux 7.0

Das Einrichten eines Kerberos 5 Clients ist weniger aufwendig als das Einrichten eines Servers. Die Mindestvoraussetzung besteht darin, die Client-Pakete zu installieren und Ihren Clients eine gültige Konfigurationsdatei `krb5.conf` zur Verfügung zu stellen. Die kerberisierten Versionen von `rsh` und `rlogin` erfordern ebenfalls einige Konfigurationsänderungen.

1. Installieren Sie die Pakete `krb5-libs` und `krb5-workstation` auf allen Clients in Ihrem Realm. Es ist erforderlich, dass Sie für Ihre Client-Workstations Ihre eigene Version von `/etc/krb5.conf` zur Verfügung stellen. In der Regel kann es sich um dieselbe `krb5.conf` handeln, die vom KDC verwendet wird.
2. Bevor Benutzer über eine Workstation in Ihrem Realm mit kerberisiertem `rsh` und `rlogin` eine Verbindung herstellen können, muss auf der betreffenden Workstation das Paket `xinetd` installiert worden sein, und die Workstation muss in der Kerberos-Datenbank über einen eigenen Host-Principal verfügen. Außerdem müssen die Serverprogramme `kshd` und `klogind` Zugriff auf die Keys haben, die für den Principal ihres Dienstes gelten.

Verwenden Sie `kadmin`, um einen Host-Principal für die Workstation hinzuzufügen. In diesem Fall besteht der Instance aus dem Hostnamen der Workstation. Da Sie das Passwort für diesen Principal wahrscheinlich nie wieder einzugeben brauchen und Sie sich deshalb vermutlich keine großen Gedanken um ein besonderes Passwort machen möchten, können Sie für den kadmin-Befehl `addprinc` einfach die Option `-randkey` verwenden, um den Principal zu erstellen und ihm ein Zufallspasswort zuzuweisen:

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

Nachdem Sie den Principal erzeugt haben, können Sie nun die Keys für die Workstation extrahieren. Führen Sie dazu `kadmin` *direkt auf der Workstation aus*, und verwenden Sie den `kadmin`-Befehl `ktadd`:

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

Um die kerberisierten Versionen von `rsh` und `rlogin` verwenden zu können, müssen Sie entweder ntsysv oder `chkconfig` benutzen, um `klogin`, `eklogin` und `kshell` zu aktivieren.

3. Darüber hinaus müssen auch andere kerberisierte Netzwerkdienste gestartet werden. Um den kerberisierten `telnet`-Dienst verwenden zu können, müssen Sie ktelnet mit Hilfe von `ntsysv` oder `chkconfig` aktivieren.

   Falls Sie außerdem FTP-Zugang zur Verfügung stellen möchten, müssen Sie einen Key für einen Principal erzeugen und extrahieren. Der Root dieses Key muss FTP lauten, und als Instance muss der Rechnername des FTP-Servers angegeben sein. Verwenden Sie anschließend ntsysv oder `chkconfig`, um `gssftp` zu aktivieren.

   Der im Paket `imap` enthaltene IMAP-Server verwendet mit Hilfe von Kerberos 5 die GSS-API-Authentifizierung, sofern er den entsprechenden Key in `/etc/krb5.keytab` findet. Der Root für den Principal sollte imap lauten. Der CVS gserver verwendet einen Principal mit dem Root cvs; ansonsten ist er identisch mit einem pserver.

Dies sind alle Informationen, die Sie benötigen, um einen einfachen Kerberos-Realm einzurichten.

8.7 Kerberos und Pluggable Authentication Modules (PAM)

Zurzeit verwenden die kerberisierten Dienste keinerlei PAM — ein kerberisierter Server überspringt PAM vollständig. Anwendungen, die PAM verwenden, können Kerberos zur Passwortüberprüfung nutzen, sofern das Modul pam_krb5 installiert ist (im Lieferumfang des Paketes `pam_krb5` enthalten). Das Paket `pam_krb5` enthält Beispielkonfigurationsdateien, durch die Dienste wie `login` und `gdm` in der Lage sind, Benutzer zu authentifizieren und unter Verwendung ihrer Passwörter erste Berechtigungsnachweise zu erhalten. Unter der Voraussetzung, dass der Zugriff auf Netzwerkserver immer über kerberisierte Dienste vorgenommen wird (oder über Dienste, die GSS-API verwenden, wie z.B. IMAP), kann das Netzwerk als relativ sicher bezeichnet werden.

Vorsichtige Systemadministratoren werden keine Kerberos-Passwortüberprüfung zu den Netzwerkdiensten hinzufügen, da die meisten von diesen Diensten verwendeten Protokolle das Passwort vor der Versendung über das Netzwerk nicht verschlüsseln — und gerade das möchten Sie schließlich vermeiden.

8.8 Weitere Informationen zu Kerberos

Falls Sie weitere Informationen zu Kerberos wünschen, so stehen Ihnen im Internet einige gute Informationsquellen zur Verfügung:

http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html

Kerberos FAQs - eine Seite mit den häufigsten Fragen zu Kerberos

http://web.mit.edu/kerberos/www/

Die Kerberos-Homepage auf der Website von MIT

ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS

Steiner, Jennifer G./Neuman, Clifford/Schiller, Jeffrey I: *Kerberos: An Authentication Service for Open Network Systems* — die Original-Beschreibung zu Kerberos; im PostScript-Format

http://web.mit.edu/kerberos/www/dialogue.html

Designing an Authentication System: a Dialogue in Four Scenes; 1988 von Bill Bryant verfasst, 1997 von Theodore Ts'o überarbeitet. Das Dokument enthält ein Gespräch zwischen zwei Entwicklern, die über die Schaffung eines Authentifizierungssystems in der Art von Kerberos nachdenken. Dank seines Gesprächscharakters und dadurch, dass zunächst die Grundlagen diskutiert werden, eignet sich dieses Dokument besonders für Benutzer, die noch nicht mit Kerberos vertraut sind.

http://www.ornl.gov/~jar/HowToKerb.html

Praktische Ratschläge zur Kerberisierung Ihres Netzwerks

Wenn Sie die Kerberos RPM-Pakete installieren, werden der *Kerberos V5 Installation Guide* und der *Kerberos V5 System Administrator's Guide* in den Formaten PostScript und HTML ebenfalls installiert. Sie finden sie unter `/usr/share/doc/krb5-server-`*`versionnumber/`*. Der *Kerberos V5 UNIX User's Guide* wird unter `/usr/share/doc/krb5-workstation-`*`versionnumber/`* im PostScript- und HTML-Format installiert.

9 Grundlegendes zum Credit Card Verification System (CCVS)

Das Credit Card Verification System (CCVS) verwendet Ihren Computer und Ihr Modem, um ein Kreditkartenlesegerät zu simulieren (auch als Point-of-Sale- [POS] Terminal bekannt). CCVS ist ein eigenständiges Produkt, das verschiedene APIs (API, Application Programming Interfaces) umfasst. Dadurch wird die benutzerspezifische Anpassung oder die Integration von Software-Anwendungen und Datenbankprodukten anderer Hersteller vereinfacht.

CCVS ist sicher und benutzerfreundlich. CCVS wurde in ANSI C geschrieben und erfüllt die POSIX-Standards. Es ist portierbar und lässt sich schnell und einfach in moderne Betriebssysteme, Programmiersprachen und ins Internet integrieren. Für eine leichte Skripterstellung und Programmierung konzipiert, kann CCVS dazu verwendet werden, die Verarbeitung von Stapeldateien zu automatisieren oder Anwendungen zu erweitern, die eine Kreditkartenbearbeitung erfordern.

CCVS kann außerhalb der USA verwendet werden, wenn Ihre Bank oder Ihr Geschäftspartner eines der von CCVS unterstützten Protokolle ebenfalls unterstützt. In Kanada unterstützt CCVS das NDC-Protokoll, das von jeder Bank in Kanada verwendet werden kann, um Ihren Merchant Account zu konfigurieren. In allen anderen Ländern erfragen Sie das erforderliche Protokoll bitte bei Ihrem Geschäftspartner. Bei folgendem von CCVS unterstütztem Protokoll ist die Wahrscheinlichkeit, dass es von einem Geldinstitut außerhalb der USA unterstützt wird, am größten: Visa 2nd Generation ‘‘K Format’’ (VITAL).

Eine Demo-Version von CCVS ist im Lieferumfang von Red Hat Linux enthalten. Diese Demo-Version ist voll funktionsfähig und kann dazu verwendet werden, um CCVS auf Ihrem System zu testen. Diese Demo-Version enthält alle Funktionen der Vollversion. Allerdings stellt sie keine Verbindung zu Ihrem Geldinstitut her. Falls Sie sich entscheiden, CCVS zu erwerben, um Kreditkarten zu verarbeiten, wenden Sie sich bitte an Red Hat, um einen Lizenzierungsschlüssel zu beziehen. Unter http://www.redhat.com/products/ccvs/ finden Sie weitere Informationen darüber, wie Sie CCVS aktivieren können.

Beispiele für die Verwendung von CCVS (je nach dem von Ihnen verwendeten Protokoll — unter www.redhat.com/products/ccvs/support/CCVS3.3docs/protocol-specific.html finden Sie weitere Informationen zu den verschiedenen Protokollen, die unterstützt werden):

- CCVS kann ein System für Telefon-Operatoren unterstützen, die Katalogbestellungen über das Telefon aufnehmen. Die Tcl-Erweiterungen von CCVS können dazu verwendet werden, eine grafische Tcl/Tk-Benutzeroberfläche zu erzeugen, die eine einfache Oberfläche für Telefon-Operatoren zur Verfügung stellt. Die Operatoren können in diesem Fall einfache X-Terminals verwenden. Die gesamte Software läuft auf dem zentralen Server. CCVS muss nur auf einem einzigen Computer installiert zu werden, und die Operatoren brauchen nicht auf eine freie Telefonleitung zu warten — alle Transaktionen werden über dieselbe Verbindung getätigt.
- CCVS kann zur Automatisierung der Rechnungserstellung eingesetzt werden. So kann ein Internet-Diensteanbieter (Internet Service Provider, ISP) z.B. eine Kundendatenbank auf einem Datenbankserver abgelegt haben. Der Datenbankadministrator des ISP könnte nun ein Perl-Skript schreiben, in dem er das Perl-Modul von CCVS mit einem Modul des Datenbanksystems kombiniert. Dieses Skript würde dann z.B. jeden Monat ausgeführt. Das Skript liest die Kundendaten, bearbeitet die in dem jeweiligen Monat angefallenen Rechnungen und aktualisiert die Datensätze in der Datenbank, um anzuzeigen, ob Zahlungen vorgenommen wurden.

Dies sind nur zwei Beispiele für die vielen Funktionen, die CCVS bietet. CCVS kann dazu verwendet werden, jeden Aspekt Ihrer Vorgänge, die eine Kreditkartenbearbeitung erforderlich machen, zu erweitern. Die vielen Funktionsmerkmale von CCVS umfassen u.a.:

- Eine C-Bibliothek mit dokumentierter API ermöglicht es Benutzern, CCVS nahtlos in bestehende Anwendungen zu integrieren.
- Eine Tcl-Erweiterung ermöglicht die Verwendung von CCVS mit serverseitigem Tcl, wie z.B. NeoWebScript.
- Ein Modul Perl 5.0 ermöglicht es, dass CCVS mit der heutzutage am weitesten verbreiteten CGI-Programmiersprache arbeiten kann.

- Mit Hilfe von Tcl/Tk lassen sich schnell und einfach benutzerdefinierte GUIs erstellen — die Entwicklungszeit beträgt typischerweise weniger als einen Tag.
- Python-, PHP3- und Java-Module ermöglichen es, dass CCVS mit anderen verbreiteten Programmiersprachen arbeiten kann.
- CLI-Programme für interaktive Nutzung (Command Line Interface, CLI). Rufen Sie Programme von einer beliebigen UNIX-Shell auf, und programmieren Sie in der von Ihnen bevorzugten UNIX-Sprache.
- AVS-Schutz vor Kreditkartenbetrug ermöglicht es Händlern, zu überprüfen, ob es sich bei einer Kreditkarte um eine gestohlene Karte handelt. Viele Clearingstellen bieten Händlern, die AVS verwenden, bessere Tarife an - selbst bei Bestellungen, die über das Telefon angenommen wurden.
- Unterstützung für mehrere Merchant Accounts, so dass Benutzer ihre eigenen virtuellen Einkaufspassagen mit einer unbegrenzten Zahl von Storefronts eröffnen können. Bei einem "Merchant Account" handelt es sich um eine besondere Art von Bankkonto, das es einem Unternehmen ermöglicht, Kreditkartenzahlungen seiner Kunden zu akzeptieren. Auf dem Merchant Account gehen die Erlöse aus den Kreditkartentransaktionen ein.
- In einer einzelnen Sitzung kann eine Vielzahl von Transaktionen ausgeführt werden, wodurch die Leistung von Standleitungen erreicht wird (zwei Sekunden pro Transaktion!), ohne dass zusätzliche Kosten entstehen oder komplexe Maßnahmen notwendig würden.
- Die Sicherheit, das Produkt jederzeit testen und neuprogrammieren zu können, ohne dass dabei tatsächlich existierende Kreditkarten belastet werden.

9.1 Verifizieren einer Kreditkarte

Wie kann nun ein Händler anhand dieser kleinen Plastikkarte feststellen, ob Sie sich z.B. den Fernseher mit Großbildschirm tatsächlich leisten können?

Zunächst legt der Käufer dem Händler seine Kreditkartenangaben vor. Der Händler überträgt diese Daten zusammen mit seinem Händler-ID-Code an eine Clearingstelle (auch als Verrechnungs- oder Abrechnungsstelle bezeichnet). Bei dieser Clearingstelle kann es sich um eine Bank handeln, die dem Händler ein Kreditkartenkonto eingerichtet hat. In den meisten Fällen handelt es sich jedoch eher um ein Unternehmen, das mit der Bank des Händlers vertraglich vereinbart hat, alle Belastungen zu verrechnen. Dafür erhält es im Gegenzug eine Gebühr und einen bestimmten Prozentsatz von jedem bearbeiteten Vorgang.

Die Daten werden übertragen, indem die Karte und die Nummer des Händlers über das Telefon gelesen oder ein Kreditkarten-POS-Terminal oder CCVS oder eine andere Software verwendet werden, mit der Informationen von einem Computer an einen anderen übertragen werden können.

Die Clearingstelle setzt sich nun mit der Bank in Verbindung, die die Kreditkarte des Käufers ausgestellt hat, und fragt nach, ob der eingeräumte Kredit für die Zahlung des Kaufpreises ausreicht. Wenn dies der Fall ist, sendet die Clearingstelle die entsprechende Bestätigung an den Händler. Gleichzeitig reduziert sich der Kredit, der dem Käufer auf seiner Kreditkarte zur Verfügung steht, um die Summe der gerade getätigten Transaktion.

Am Ende eines Geschäftstages kontaktiert der Händler (genauer gesagt, der Computer oder das Kreditkartenterminal des Händlers) die Clearingstelle und überprüft noch einmal alle Transaktionen dieses Tages, um sicherzustellen, dass die vom System des Händlers für diesen Tag verzeichneten Transaktionen mit den von der Clearingstelle verzeichneten Transaktionen übereinstimmen. Sobald festgestellt wurde, dass beide dieselben Transaktionen verzeichnet haben, überweist die Clearingstelle das Geld von der Kreditkartenbank auf das Bankkonto des Händlers.

9.2 Was benötigen Sie, um mit CCVS arbeiten zu können?

Um CCVS ausführen zu können, benötigen Sie ein Modem und einen Merchant Account. Außerdem müssen Sie einige Richtlinien befolgen, damit CCVS korrekt arbeitet.

9.2.1 Modems

Sie benötigen mindestens ein Modem, das für CCVS reserviert ist. Kreditkartenprotokolle unterstützen bei Modemverbindungen keine Komprimierung oder Fehlerkorrektur, daher können Sie die Funktionen zur Komprimierung und Fehlerkorrektur nicht verwenden. Wir stellen Ihnen gern Informationen darüber zur Verfügung, wie diese Funktionen bei den folgenden Modems deaktiviert werden:

- Hayes Optima
- US Robotics Courier
- US Robotics Sportster
- Chase Research PCI-RAS

Bitte beachten

Bitte verwenden Sie nur Modems aus der oben aufgeführten Liste!

Wenn Sie ein Modem verwenden, das nicht unterstützt wird (d.h., irgendein anderes Modem, das nicht in der obigen Liste enthalten ist), kann es sehr schwierig werden, CCVS mit diesem Modem ans Laufen zu bringen. Bitte lesen Sie sich daher die Listen der mit Red Hat Linux-kompatiblen Hardware durch, um sicherzustellen, dass Ihr Modem mit Red Hat Linux arbeitet. Sie finden diese Listen unter http://www.redhat.com/support/hardware/.

Wenn Ihr Modem nicht in dieser Liste enthalten ist, lesen Sie bitte im Handbuch zu Ihrem Modem nach, mit welchem String Sie die Komprimierung und Fehlerkorrektur ausschalten können und mit welchem String Sie Ihr Modem später wieder für den normalen Betrieb zurücksetzen können. Diese beiden Strings müssen Sie bei der Konfiguration von CCVS angeben.

9.2.2 Merchant Accounts

Wenn Sie einen Merchant Account einrichten oder einen bestehenden Merchant Account ändern, um CCVS zu verwenden, kann es vorkommen, dass das Institut, das Ihnen den Merchant Account zur Verfügung stellt, den Beweis wünscht, dass CCVS tatsächlich mit dem von diesem Institut verwendeten Protokoll arbeiten kann. Zertifizierungsschreiben für spezielle Protokolle stehen Ihnen unter http://www.redhat.com/certifications.html zur Verfügung. Drucken Sie alle Seiten des Schreibens aus, das sich auf das von Ihnen verwendete Protokoll bezieht, und legen Sie es dem Institut vor, von dem Ihnen der Merchant Account eingeräumt wird.

Das Institut muss eines der von CCVS unterstützten Protokolle verwenden:

- ETC-PLUS-Protokoll (auch bekannt als FDR7, ETC+, ETC7, "Omaha") von First Data Corporation
- South-Platform-Protokoll (auch bekannt als "Nabanco") von First Data Corporation
- MAPP-Protokoll (auch bekannt als "St. Louis") von Global Payment Systems
- NDC-Protokoll (auch bekannt als "Atlanta") von Global Payment Systems
- VITAL-Protokoll (auch bekannt als VisaNet, Visa 2nd generation, "K format") von Visa International
- UTF-Protokoll (auch bekannt als GENSAR) von Paymentech
- NOVA Information Systems-Protokoll

Wenn das Institut, das Ihnen den Merchant Account einräumt, mit einem dieser Protokolle arbeitet, können Sie CCVS einsetzen.

Sobald Sie festgestellt haben, mit welchem Protokoll Sie arbeiten werden, lesen Sie sich bitte noch einmal die gesamten unter http://www.redhat.com/CCVS3.3docs/protocol-specific.html zur Verfügung stehenden Informationen zu diesem Protokoll durch, bevor Sie mit dem Konfigurieren von CCVS beginnen. Der unter dem angegebenen Link zur Verfügung stehende *CCVS Protocol Guide* beschreibt die Funktionalitäten, die von den verschiedenen Protokollen unterstützt werden.

9.2.3 Richtlinien für den Einsatz von CCVS auf Ihrem System

Wenn die folgenden Voraussetzungen erfüllt sind, arbeitet CCVS einwandfrei und effizient. Bitte vergewissern Sie sich, dass Sie alle Richtlinien befolgt haben, bevor Sie versuchen, CCVS auszuführen.

Exklusive Verwendung der Modems während des Betriebs von CCVS

Führen Sie keine anderen Software-Anwendungen aus, die auf das Modem zugreifen müssen, während Sie CCVS ausführen. Dadurch kann der Betrieb von CCVS gestört werden.

Berechtigungen, Privilegien und Zugriff auf das Modem

Die meisten Berechtigungen, die für CCVS erforderlich sind, werden während des Installationsvorgangs durch Erzeugen einer speziellen Gruppe mit dem Namen "ccvs" eingerichtet. Einige Aspekte betreffen jedoch Systemberechtigungen, über die Sie Bescheid wissen sollten.

Alle Vorgänge für eine bestimmte CCVS-Konfiguration müssen von einem Einzelbenutzeraccount aus ausgeführt werden. Es ist ein Account erforderlich, damit der Dateibesitz und alle Berechtigungen korrekt eingerichtet und geschützt werden. Dieser Benutzeraccount muss (von Ihnen oder Ihrem Systemadministrator) zur Gruppe ccvs hinzugefügt werden, bevor Sie das Konfigurationsprogramm ausführen.

Führen Sie, nachdem Sie den Benutzer zur Gruppe ccvs hinzugefügt haben, das CCVS-Konfigurationsprogramm unter diesem Benutzer aus. Nachdem Sie das Konfigurationsprogramm ausgeführt haben, müssen die CCVS-Befehle für diese Konfiguration unter demselben Benutzer ausgeführt werden.

Wenn CCVS mit einem Modem arbeiten soll, müssen die Benutzer in der Gruppe ccvs auch zur Gruppe uucp hinzugefügt werden. Doch möglicherweise reicht es nicht aus, lediglich Mitglied der Gruppe uucp zu sein, um mit den Modems arbeiten zu können. Falls es sich nicht auf Ihrem System befindet, müssen Sie sicherstellen, dass die Mitglieder der Gruppe ccvs auch Zugriff auf den seriellen Modem-Port haben, mit dem CCVS arbeitet.

Wenn Sie PHP zusammen mit CCVS verwenden, muss der Web-Server in der Lage sein, CCVS -Befehle auszuführen. Um das zu erreichen, muss der Benutzer des Web-Servers ein Mitglied der Gruppe ccvs werden. In der Regel muss der Benutzer des Web-Servers auch Mitglied der Gruppe uucp sein.

Wenn Sie PHP nicht verwenden, aber den Web-Server trotzdem in die Lage versetzen möchten, CCVS auszuführen, stehen Ihnen neben der Möglichkeit, den Benutzer des Web-Servers zu einem Mitglied der Gruppe ccvs zu machen, noch weitere Optionen zur Verfügung (z.B. `suexec`, `setuid`). Sie können ihn ganz nach Wunsch einrichten, so lange Sie kein PHP verwenden.

Software-Versionen

CCVS benötigt Tcl ab Version 7.6, um die enthaltene grafische Benutzeroberfläche (GUI) auszuführen oder die enthaltenen Tcl/Tk-APIs für die Entwicklung einer eigenen grafischen Oberfläche einzusetzen. Tcl Version 8.3 ist im Lieferumfang von Red Hat Linux 7.0 enthalten.

CCVS benötigt Perl ab Version 5.0, um die enthaltenen Perl APIs verwenden zu können. Perl Version 5.6 ist im Lieferumfang von Red Hat Linux 7.0 enthalten.

9.3 Installieren von CCVS

Die RPM-Pakete von CCVS stehen auf der Linux Applications Library Workstation-CD zur Verfügung.

Sie können RPM, Gnome-RPM oder Kpackage zum Installieren der CCVS-Pakete verwenden:

- `CCVS` — Die CCVS-Kernprogramme
- `CCVS-devel` — Entwicklerkit für C
- `CCVS-perl` — Perl-Schnittstelle für CCVS
- `CCVS-python` — Python-Schnittstelle für CCVS
- `CCVS-php3` — PHP3-Schnittstelle für CCVS
- `CCVS-tcl` — Tcl-Schnittstelle für CCVS
- `CCVS-java` — Java-Schnittstelle für CCVS (als Quellcode enthalten)
- `CCVS-examples` — Beispielquellcode, erforderlich für die Entwicklung

9.4 Bevor Sie mit dem Konfigurieren von CCVS beginnen

Bevor Sie CCVS konfigurieren, müssen Sie verschiedene Fragen über Ihr System und zur Einrichtung von CCVS beantworten. Um den Konfigurationsvorgang vorzubereiten, befolgen Sie bitte unbedingt die folgenden Schritte:

1. Bitte lesen Sie sich die gesamte Dokumentation und alle Errata durch, die mit dem Programm geliefert wurden.

2. Füllen Sie `setup.txt` aus. Bei der Datei `setup.txt` handelt es sich um ein Formular, das die verschiedenen Informationen erläutert, die erforderlich sind, wenn CCVS für den Einsatz mit bestimmten Protokollen konfiguriert werden soll. Wenn Sie `setup.txt` ausfüllen, haben Sie dadurch sämtliche für die Konfiguration erforderlichen Informationen zur Hand. Sie finden die Datei im Verzeichnis `/usr/share/doc/CCVS-`*`<Version>`*. Alternativ dazu können Sie `setup.txt` auch unter http://www.redhat.com/products/ccvs/support/CCVS3.3docs/setup.txt finden.

Bitte beachten

Im Setup-Formular werden Sie nach einigen protokollspezifischen Informationen gefragt. Sie müssen nur die Informationen für das Protokoll angeben, das Sie benutzen möchten. Für die anderen Protokolle brauchen Sie keine Informationen anzugeben.

3. Das CCVS-Installationsprogramm stellt Ihnen verschiedene Fragen zu Ihrem Modem. Halten Sie deshalb die erforderlichen Angaben bereit. Derzeit dokumentiert CCVS nur die init-Strings für drei Modems:

Hayes Optima oder ACCURA

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

U.S. Robotics Sportster oder Courier

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

Chase Research PCI-RAS

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

Falls Ihr Modem nicht in dieser Liste enthalten ist, lesen Sie bitte im Handbuch zu Ihrem Modem nach, welcher String die Komprimierung und Fehlerbehebung deaktiviert und welcher String Ihr Modem wieder für den normalen Betrieb zurücksetzt. Während des Konfigurationsvorgangs müssen Sie diese beiden Modemstrings einstellen.

9.5 Konfigurieren von CCVS

Sie müssen CCVS für Ihr System konfigurieren, und zwar entweder im Demo-Modus oder für die Verarbeitung von echten Daten.

Verwenden Sie `su`, um zu dem Benutzeraccount zu wechseln, den Sie für diese Konfiguration erstellt haben (ein Mitglied der Gruppe ccvs).

Führen Sie das CCVS-Konfigurationsprogramm mit folgendem Befehl aus:

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

Der restliche Teil dieses Abschnitts führt Sie nun durch das CCVS-Konfigurationsprogramm. Sie sollten nun einen Begrüßungsbildschirm sehen. Drücken Sie die [Eingabetaste], um die CCVS-Softwarelizenz zu lesen. Sie können die standardmäßigen Scroll- und Paging-Befehle von `more` verwenden (oder das Paging-Programm, das von Ihrer Umgebungsvariablen $PAGER eingestellt wurde), um die Lizenz durchzulesen.

Wenn Sie die Lizenz gelesen und den Pager verlassen haben, sehen Sie:

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

Geben Sie das Wort **`accept`** ein, um die Lizenzvereinbarung anzunehmen, und fahren Sie dann mit der Konfiguration von CCVS fort. Falls Sie etwas anderes als accept eingeben, wird das Programm beendet.

Sie sehen nun folgenden Bildschirm:

```
This program creates the configuration file for CCVS functions.
To do this, you will require the following information:
1: The clearing protocol you will be using. This may be MAPP,
ETC+, or any of the other protocols which CCVS supports. There
is also a demo protocol; if you have downloaded the free demo of
CCVS, you will be using the demo protocol.
2: The unique number which identifies you to the clearing
house. This may be your merchant account number or a terminal id
number, depending on what protocol you will be using. This number
will be supplied when you set up your merchant account.
3: Your modem type, and the serial port your modem is attached
to. You will also need modem configuration strings. (We can
supply modem configuration strings for many popular modems.)
4: The location of your data directory. This is where the
configuration file and data directories will be placed.
5: Other information as needed for particular protocols. This
information will generally be supplied when you set up your
merchant account.

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

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

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

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

Drücken Sie auf [Y], um fortzufahren. Falls Sie mit dem Befehl `su` zum Root gewechselt haben, sehen Sie stattdessen nun die folgende Fehlermeldung. (Wenn dieser Fall eintritt, sollten Sie mit `su` zum CCVS-Benutzer wechseln und dann `ccvs_configure` erneut ausführen.)

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

Wenn Sie fortfahren, fordert das Programm Sie auf, Informationen einzugeben. Sie können zu jedem beliebigen Zeitpunkt zu einem vorherigen Prompt zurückkehren, indem Sie einfach **.** (einen Punkt) eingeben und dann die [Eingabetaste] drücken.

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

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

Sofern Sie keinen Software-Key und keine Lizenz für CCVS erworben haben, geben Sie nun [Y] ein. Dadurch wird eine Demo-Konfiguration installiert, die weder das Modem anwählt noch einen echten Merchant Account verwendet. Wenn Sie eine Lizenz erworben haben und jetzt so weit sind, eine vollfunktionsfähige Konfiguration zu installieren, geben Sie [N] ein.

```
Where do you want to place the CCVS configuration files and
transaction queues? This should be a directory name which is
writable by the current user.
The default is "/var/ccvs".
Enter directory, or Return for default value, or . by itself to
back up.
>
```

Sofern keine besonderen Gründe vorliegen, um die CCVS-Konfigurationsdateien und Transaktionswarteschlangen zu verschieben, sollten Sie sie in ihren Standardverzeichnissen belassen. Falls Sie sie verschieben müssen, denken Sie bitte daran, dass Sie in dann auch eine Umgebungsvariable einstellen müssen.

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

Sie können z.B. eine Konfiguration mit der Bezeichnung **`tshirt`** für einen Händler haben, der T-Shirts verkauft, und eine Konfiguration mit der Bezeichnung **`music`** für einen Musikgroßhändler. Der hier eingegebene Name wird dazu verwendet, zwischen den beiden Konfigurationen zu unterscheiden.

Für die Demo-Version von CCVS sind nun keine weiteren Informationen erforderlich. Falls Sie sich für die Demo-Version entschieden haben, sehen Sie nun folgende Meldung:

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

The CCVS system is now configured.
```

Sie können nun mit dem Testen der Demo-Software beginnen. Die Demo-Version funktioniert genauso wie die Vollversion der CCVS-Software, mit der Ausnahme, dass keine Verbindung zum Modem oder zu einem tatsächlich existierenden Merchant Account hergestellt wird.

Wenn Sie eine Lizenz für die Vollversion von CCVS erworben haben und sich dann dazu entscheiden, eine echte Konfiguration zu installieren, dann sehen Sie nun folgende Meldung:

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

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

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

Wählen Sie das Protokoll aus, für das Sie eine CCVS -Lizenz und einen gültigen Merchant Account besitzen.

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

Diese Nummer sollte Ihnen zusammen mit Ihrem Merchant Account zur Verfügung gestellt worden sein.

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

Diese Nummer wurde Ihnen zusammen mit Ihrer CCVS-Lizenz zur Verfügung gestellt.

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

Diese Nummer wurde Ihnen ebenfalls zusammen mit Ihrer CCVS-Lizenz zur Verfügung gestellt.

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

Möglicherweise müssen Sie für bestimmte Protokolle noch einige andere Fragen beantworten. Wenn Sie das Formular `setup.txt` für das von Ihnen gewählte Protokoll ausgefüllt haben, sollten Sie für die folgenden Fragen ausreichend vorbereitet sein. So werden für VITAL noch weitere Prompts eingeblendet, die Sie nach dem Namen Ihres Unternehmens, Ihrer Adresse, Bankverbindung usw. fragen. Diese Informationen sollten Sie bereits beim Einrichten Ihres VITAL Merchant Accounts abgeklärt haben.

Sie müssen nun angeben, wie die Kommunikation mit Ihrem Modem erfolgen soll. Die Modem-Konfigurationsinformationen sind sehr wichtig. Vergewissern Sie sich daher, dass Sie die korrekten Informationen für Ihr System-Setup eingeben; CCVS arbeitet nicht, wenn das Modem nicht korrekt eingerichtet wurde.

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

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

Falls Sie über mehrere identische Modems verfügen, können Sie CCVS so konfigurieren, dass alle (als Pool) verwendet werden. Jeder CCVS-Prozess, der ein Modem benötigt, kann dann aus diesem Pool ein gerade verfügbares Modem auswählen. Auf diese Weise können mehrere CCVS-Konfigurationen eine Gruppe von Modems gemeinsam verwenden. Außerdem können Sie eine einzelne Konfiguration mit zwei Modems konfigurieren, so dass Authorisierungen und Stapelverarbeitung gleichzeitig ablaufen können.

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

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

Das Programm testet den von Ihnen angegebenen seriellen Port. Wenn Sie mehr als einen Port konfigurieren, testet es jeden dieser Ports. Fügen Sie `/dev/` nicht ein. Dieser Schritt kann bis zu dreißig Sekunden in Anspruch nehmen, wenn das Modem nicht antwortet.

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

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

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

Sie werden nun aufgefordert, die Strings für die Modeminitialisierung sowie für Wählen und Auflegen anzugeben. (Wenn Sie einen Modem-Pool konfigurieren, müssen alle darin enthaltenen Modems identisch sein und alle dieselben Strings verwenden.) Sobald CCVS die geeigneten Strings für Ihr Modem kennt, werden Ihnen diese vorgeschlagen, und Sie brauchen nur die [Eingabetaste] zu drücken.

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

The modem dial string should dial the modem. (Do not include a
phone number.)
What string do you want to use?
A string which works for your modem is:
```

```
 ATDT
Enter string, or Return for suggested value.
>

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

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

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

Möglicherweise wird Ihnen nicht exakt derselbe Bildschirm angezeigt, wie oben angegeben. Das liegt daran, dass die vorgeschlagenen Standardeinstellungen je nach ausgewähltem Modem variieren.

Anschließend wird nach der Baudrate gefragt:

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

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

Wenn Sie alle Konfigurationsinformationen eingegeben haben, erscheint folgende Meldung:

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

The CCVS system is now configured.
```

9.6 Mehrere Merchant Accounts

Falls Sie mehrere Merchant Accounts unterstützen müssen, brauchen Sie dazu einfach nur noch einmal die Konfiguration auszuführen. Verwenden Sie für jeden Merchant Account einen anderen Konfigurationsnamen.

Verschiedene Konfigurationen können sich denselben seriellen Port bzw. denselben Pool von seriellen Ports teilen. Die Modems werden der Reihe nach bedient.

9.7 Starten von CCVS

Um CCVS für eine bestimmte Anwendung auszuführen, müssen Sie mit dem Befehl `su` zu dem Account wechseln, den diese Konfiguration erstellt hat.

Als Benutzer dieses Accounts müssen Sie, um CCVS ausführen zu können, den `ccvsd`-Dämon für jeden Merchant Account starten und das Programm `cvupload` regelmäßig ausführen (es empfiehlt sich, `cron` zu verwenden, um `cvupload` jeden Tag auszuführen).

9.7.1 Der ccvsd-Dämon

Um CCVS auszuführen, müssen Sie den `ccvsd`-Dämon ausführen. Der `ccvsd`-Dämon ist derjenige, der alle Telefonanrufe und Transaktionen durchführt. Auf den Befehl `ccvsd` muss der Name des Accounts folgen, den Sie beim Konfigurieren des Accounts angegeben haben.

Wenn Sie beispielsweise die Bearbeitung von Transaktionen für den im vorhergehenden Abschnitt genannten Musikgroßhändler starten möchten und die Software in dem Standardverzeichnis `/usr/sbin` installiert haben, geben Sie folgenden Befehl ein, um `ccvsd` zu starten:

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

Wann immer Sie einen Merchant Account hinzufügen möchten, müssen Sie `ccvsd` für diesen Account starten, falls Sie Transaktionen für diesen Account bearbeiten möchten.

Weitere Informationen zu `ccvsd` finden Sie in der man-Seite `ccvsd`.

9.7.2 Der Befehl `cvupload`

Einige Transaktionen (wie z.B. Authorisierungen) werden vorgenommen, sobald die Kreditkarte vorgelegt wird. Andere Transaktionen (z.B. Verkäufe oder Umtausch/Rückgabe) werden gespeichert und nicht sofort bearbeitet. Diese Transaktionen werden zu Stapeln zusammengefasst und dann als Gruppe bearbeitet.

CCVS verwendet für diese Stapelverarbeitung das Programm `cvupload` . Wir empfehlen, `cvupload` mindestens täglich als `cron`-Job aufzurufen, so dass `cvupload` automatisch jeden Tag ausgeführt wird, ohne dass Sie eingreifen müssen.

Für die regelmäßige Bearbeitung des Musikgroßhändlers würden Sie z.B. folgenden Befehl ausgeben:

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

Weitere Informationen zu `cvupload` finden Sie in der man-Seite `cvupload`.

9.8 Hinweise zu den Programmiersprachen

- C — Die C-Bibliothek von CCVS ist im Paket `CCVS-devel` enthalten. Wenn Sie C-Programme kompilieren, die CCVS verwenden, müssen Sie das `-lccvs`-Flag zur Verknüpfungszeile hinzufügen.
- Java — Unter http://www.redhat.com/CCVS3.3docs/AdminJava.html finden Sie weitere Informationen zum Erstellen der CCVS -Java-Schnittstelle. Der Quellcode für die Java-Schnittstelle ist im Paket `CCVS-java` enthalten.
- Perl — Die Perl-Schnittstelle ist im Paket `CCVS-perl` enthalten.
- Python — Die Python-Schnittstelle ist im Paket `CCVS-python` enthalten.
- PHP — Das Paket `CCVS-php3` enthält die PHP3-Schnittstelle.
- Tcl — Die Tcl-Schnittstelle ist im Paket `CCVS-tcl` enthalten.

9.9 Support für CCVS

Sie können bei Red Hat Support für CCVS erhalten. Achten Sie beim Erwerb des Keys zum Aktivieren von CCVS auf die zur Verfügung stehenden Support-Optionen.

Weitere Informationen zum Erwerb des Keys und zu den Support-Optionen finden Sie unter http://www.redhat.com/products/ccvs/.

Falls Sie die Hilfe benötigen, achten Sie bitte darauf, folgende Informationen zur Hand zu haben, bevor Sie den Support kontaktieren:

- Name Ihres Unternehmens
- Die CCVS-Version, mit der Sie arbeiten
- Ihre Händlernummer
- Ihre CCVS-Kundennummer
- Ihr Betriebssystem und die Version

Red Hat Unser technischer Support wird versuchen, alle Fragen zu klären, die CCVS direkt betreffen. Wir können keine Produkte anderer Hersteller unterstützen, es sei denn, es handelt sich um Fragen, die die Integration in CCVS betreffen.

Teil II Referenzinformationen zum sicheren Web-Server

10 Installieren von Red Hat Linux Secure Web Server

10.1 Einführung

Die folgenden Kapitel sollen Ihnen als Einführung in den Betrieb des Apache World Wide Web (WWW oder Web)-Servers Version 1.3.12 mit dem mod_ssl-Sicherheitsmodul sowie der OpenSSL-Bibliothek und dem zugehörigen Toolkit dienen. Die Kombination dieser drei mit Red Hat Linux mitgelieferten Komponenten wird in diesem Handbuch als Red Hat Linux Secure Web Server bezeichnet (oder kurz sicherer Server).

Web-Server stellen Browsern (z.B. Netscape Navigator, Microsoft Internet Explorer) die angeforderten Webseiten bereit. Technisch ausgedrückt: Web-Server unterstützen das HyperText Transfer Protocol (HTTP), den Internet-Standard für die Web-Kommunikation. Ein Web-Server sendet mit dem HTTP-Protokoll auf Anforderung HyperText Markup Language (HTML)-Webseiten und CGI-Skripten (und andere Arten von Skripten) zum Browser. Wenn ein Benutzer auf einer Webseite auf einen Link klickt, wird eine Anforderung für den von der Verknüpfung benannten Inhalt zu einem Web-Server geschickt. Der Web-Server empfängt die Anforderung und liefert den angeforderten Inhalt (z.B. eine HTML-Seite, ein interaktives Skript, eine dynamisch aus einer Datenbank erstellte Webseite usw.), oder er schickt eine Fehlermeldung zurück. Apache, der in diesem Softwarepaket mitgelieferte Web-Server, ist der heute am häufigsten im Internet verwendete Web-Server (siehe http://www.netcraft.net/survey/).

Das Modul mod_ssl ist ein Sicherheitsmodul für den Apache Web-Server. Das Modul mod_ssl verwendet die vom OpenSSL-Projekt zur Verfügung gestellten Tools für eine sehr wichtige Funktion von Apache — die Verschlüsselung der Kommunikation. Dagegen werden die zwischen Browser und Web-Server ausgetauschten Daten bei "normaler" HTTP-Übertragung unverschlüsselt übertragen und könnten auf der Übertragungsstrecke zwischen dem Browser und dem Server abgefangen und mitgelesen werden.

Das OpenSSL-Projekt enthält ein Toolkit, in dem die Protokolle Secure Sockets Layer (SSL) und Transport Layer Security (TLS) sowie eine universelle Verschlüsselungsbibliothek implementiert sind. Das SSL-Protokoll wird heute zur sicheren Datenübertragung über das Internet verwendet. Das TLS-Protokoll ist ein im Vorschlagsstadium befindlicher Internetstandard für die private (sichere) und zuverlässige Kommunikation über das Internet. OpenSSL-Tools werden vom mod_ssl-Modul für die sichere Web-Kommunikation verwendet.

Diese Kapitel sind nicht als vollständige und ausschließliche Dokumentation für irgendeines dieser Programme zu verstehen. Wenn möglich, wird in diesem Handbuch auf geeignete Quellen verwiesen, in denen Sie detailliertere Informationen zu speziellen Themenbereichen finden können.

In diesem Handbuch werden die Installation der mitgelieferten Programme sowie die grundlegenden Konfigurationsmöglichkeiten Ihres Apache Web-Servers beschrieben. Weiterhin werden die Schritte beschrieben, die notwendig sind, um ein Zertifikat von einer Zertifizierungsstelle (Certificate Authority, CA) zu erhalten, ein eigenes selbstunterzeichnetes Zertifikat zu erstellen sowie ein Zertifikat zu installieren, das Sie für Ihren sicheren Web-Server verwenden können.

10.2 Danksagungen

Der Red Hat Linux Secure Web Server enthält u.a. folgende Komponenten:

- Von der Apache Group entwickelte Software für die Verwendung im Apache HTTP-Server-Projekt (http://www.apache.org/httpd.html)
- Das mod_ssl-Sicherheitsmodul, entwickelt von Ralf S. Engelschall (http://www.modssl.org/)
- Das OpenSSL-Toolkit, entwickelt von Mark J. Cox, Ralf S. Engelschall, Dr. Stephen Henson und Ben Laurie (http://www.openssl.org/)
- Auf dem Apache SSL HTTP-Serverprojekt basierende Software, entwickelt von Ben Laurie (http://www.apache-ssl.org/)
- Auf der SSLeay-Verschlüsselungssoftware basierende Software, geschrieben von Eric Young und Tim Hudson

Red Hat bedankt sich für die genannten Beiträge zu diesem Software-Produkt.

10.3 Überblick über die Installation

In diesem Kapitel finden Sie Informationen über die RPM-Pakete für den Red Hat Linux Secure Web Server und ihre Installation. Mit dem Red Hat Linux Secure Web Server werden auch optionale Pakete mitgeliefert, die Sie installieren können, falls Sie deren Funktionalität nutzen möchten.

Je nach Konfiguration Ihres Systems gibt es drei verschiedene Möglichkeiten, den Red Hat Linux Secure Web Server zu installieren. Alle sind einfach durchzuführen. Je nachdem, wie Sie das Red Hat Linux-Betriebssystem installieren, sollten Sie jedoch die für Ihre Situation geeignete Variante wählen:

1. Installation von Red Hat Linux mit dem Installationsprogramm — da der Red Hat Linux Secure Web Server mit dem Red Hat Linux-Betriebssystem mitgeliefert wird, ist die einfachste Variante die Installation des Servers während der Installation von Red Hat Linux. Wenn Sie eine neue Installation von Red Hat Linux vornehmen möchten, sollten Sie Ihren sicheren Server auf diese Weise installieren. Weitere Informationen zur Installation von Red Hat Linux Secure Web Server im Zusammenhang mit einer Neuinstallation von Red Hat Linux finden Sie in Abschnitt 10.5, *Installieren von Red Hat Linux Secure Web Server während der Installation von Red Hat Linux*.

2. Aktualisieren von Red Hat Linux mit dem Installationsprogramm — wenn auf Ihrem System bereits eine frühere Version von Red Hat Linux läuft und Sie diese auf Red Hat Linux 7.0 aktualisieren möchten, müssen Sie die Pakete für den sicheren Server während des Aktualisierungsprozesses installieren. Wichtige Informationen, was bei der Aktualisierung von Red Hat Linux zu beachten ist, finden Sie in Abschnitt 10.7, *Aktualisieren einer älteren Version von Red Hat Linux*.

3. Installation des sicheren Servers nach der Installation von Red Hat Linux 7.0 — wenn Sie Red Hat Linux 7.0 vorher installiert haben und zu einem späteren Zeitpunkt die Funktionalität des sicheren Servers nutzen möchten, können Sie die Pakete für den sicheren Server mit dem RPM Package Manager (RPM), mit Gnome-RPM oder mit Kpackage von einer Red Hat Linux-CD installieren.

Wenn Sie eine frühere Version von Apache aktualisieren (einschließlich aller früheren Versionen von Red Hat Linux Secure Web Server), benötigen Sie außerdem bestimmte Informationen zum Aktualisierungsprozess. Informieren Sie sich dazu in Abschnitt 10.6, *Aktualisieren einer älteren Version von Apache*, bevor Sie den Installationsprozess beginnen, wenn Sie Apache aktualisieren.

10.4 Auswählen der zu installierenden Pakete

Zum Installieren des sicheren Servers müssen mindestens drei Pakete installiert werden:

`apache`

Das Paket `apache` enthält den Apache Web-Server.

`mod_ssl`

Das Paket `mod_ssl` enthält das Modul mod_ssl, das über die Protokolle Secure Sockets Layer (SSL) und Transport Layer Security (TLS) eine starke Verschlüsselung für den Apache Web-Server ermöglicht.

`openssl`

Das Paket `openssl` enthält das OpenSSL-Toolkit. Darin sind die Protokolle SSL und TLS implementiert. Es enthält außerdem eine universelle Verschlüsselungsbibliothek.

Zusätzlich können weitere, bei Red Hat Linux mitgelieferte Softwarepakete zusätzliche Funktionen für den sicheren Server bereitstellen (diese sind jedoch nicht unbedingt für die Funktion des sicheren Servers erforderlich):

OpenSSH

Das Paket `openssh` enthält die OpenSSH-Netzwerkkonnektivitätstools für die Anmeldung und die Ausführung von Befehlen auf einem Remote-Rechner. OpenSSH-Tools verschlüsseln den gesamten Datenverkehr (einschließlich Passwörter), um das Mithören, den Missbrauch der Verbindung und andere Angriffe auf die Kommunikation zwischen Ihrem Rechner und dem Remote-Rechner unmöglich zu machen.

Das Paket `openssh` enthält folgende OpenSSH-Clients: `ssh`, ein sicheres Programm zum Ersatz von `rsh`; `slogin`, ein sicheres Programm zum Ersatz von `rlogin` (Remote-Anmeldung), `telnet` (Kommunikation mit einem anderen Rechner über das TELNET-Protokoll), `scp`, ein sicheres Programm zum Ersatz von `rcp` (zum Kopieren von Dateien zwischen Rechnern) und `ftp` (zum Übertragen von Dateien zwischen Rechnern).

Das Paket `openssh-askpass` unterstützt die Anzeige eines Dialogfensters, das den Benutzer bei der Verwendung eines OpenSSH-Agenten mit RSA-Authentifizierung zur Eingabe eines Passworts auffordert.

Das Paket `openssh-askpass-gnome` zeigt ein Dialogfenster für die GNOME Benutzeroberfläche an, wenn OpenSSH-Programme den Benutzer zur Angabe eines Passworts auffordern. Wenn Sie GNOME ausführen und OpenSSH-Dienstprogramme verwenden, sollten Sie dieses Paket installieren.

Das Paket `openssh-server` enthält den `sshd` Secure Shell Dämon und die entsprechende man-Seite. Beim Secure Shell Dämon handelt es sich um den serverseitigen Teil der OpenSSH-Programmsuite. Dieser Dämon muss auf Ihrem Rechner installiert werden, wenn Sie SSH-Clients die Verbindung mit Ihrem Rechner ermöglichen möchten.

Das Paket `openssh-clients` enthält die für verschlüsselte Verbindungen mit SSH-Servern erforderlichen Client-Programme.

Weitere Informationen zu OpenSSH finden Sie auf der OpenSSH-Website unter http://www.openssh.com/.

Stunnel

Das Paket `stunnel` enthält den Stunnel SSL-Wrapper. Stunnel unterstützt die SSL-Verschlüsselung von TCP-Verbindungen und ermöglicht daher die Verschlüsselung für Dämonen und Protokolle, die nicht SSL-kompatibel sind (z.B. POP, IMAP, LDAP), ohne dass Änderungen am Code des Dämonen vorgenommen werden müssen.

apache-devel

Das Paket `apache-devel` enthält die Apache Include-Dateien, Header-Dateien und das APXS-Dienstprogramm. Wenn Sie zusätzliche Module laden möchten, die nicht bereits in diesem Softwareprodukt enthalten sind, benötigen Sie alle genannten Komponenten. Weitere Informationen zum Laden von Modulen in den Red Hat Linux Secure Web Server mit der DSO-Funktionalität von Apache finden Sie in Abschnitt 12.2, *Hinzufügen von Modulen zu Ihrem Server*.

Wenn Sie keine weiteren Module in den Red Hat Linux Secure Web Server laden möchten, muss dieses Paket nicht installiert werden.

`apache-manual`

Das Paket `apache-manual` enthält das *Benutzerhandbuch für Apache 1.3* im HTML-Format. Dieses Handbuch ist auch unter http://www.apache.org/docs/ im Web verfügbar.

`openssl-devel`

Das Paket `openssl-devel` enthält die statischen Bibliotheken und die Include-Datei, die zum Kompilieren von Anwendungen erforderlich sind, die verschiedene Verschlüsselungsalgorithmen und Protokolle unterstützen. Sie müssen dieses Paket nur installieren, wenn Sie Anwendungen mit SSL-Unterstützung entwickeln — für die ausschließliche Verwendung von SSL wird dieses Paket nicht benötigt.

10.5 Installieren von Red Hat Linux Secure Web Server während der Installation von Red Hat Linux

Wenn Sie Red Hat Linux und den Red Hat Linux Secure Web Server gleichzeitig installieren, folgen Sie bitte den Anleitungen in Kapitel 15, *Installieren von Red Hat Linux über die grafische Benutzeroberfläche*, um mit der Installation von Red Hat Linux zu beginnen. Gehen Sie bis zu dem Punkt nach der Anleitung vor, an dem eine Installationsklasse auszuwählen ist: Workstation, Server oder Benutzerdefiniert.

1. Wenn Sie sich für die Installationsklasse Server entscheiden, werden die Pakete für den sicheren Server (`apache`, `mod_ssl` und `openssl`) automatisch ausgewählt. Die Pakete `stunnel` und `openssh` enthalten sicherheitsrelevante Funktionen und werden ebenfalls mit ausgewählt.

2. Wenn Sie sich für die Installationsklasse Workstation entscheiden, werden die Pakete für den sicheren Server nicht automatisch für die Installation ausgewählt, Sie können diese jedoch während des Paketauswahlprozesses installieren.

3. Wenn Sie sich für eine benutzerdefinierte Installation entscheiden, müssen Sie die zu installierenden Pakete für den sicheren Server und sicherheitsrelevanten Pakete selbst auswählen.

Nachdem Sie eine Installationsklasse ausgewählt haben, folgen Sie bitte den Installationsanleitungen zum Partitionieren und Konfigurieren Ihres Systems. Wenn Sie die Auswahl der Paketgruppen vornehmen müssen, wählen Sie die Paketgruppe **Web-Server**. **Web-Server** enthält die Pakete `apache` und `mod_ssl`, die Sie installieren müssen, um den sicheren Server ausführen zu können. Da `openssl` eine Abhängigkeit für das Paket `mod_ssl` darstellt, wird `openssl` ebenfalls für die Installation ausgewählt.

Wenn Sie eines der in Abschnitt 10.4, *Auswählen der zu installierenden Pakete* beschriebenen zusätzlichen sicherheitsrelevanten Pakete installieren möchten, müssen Sie dies im Installationsprogramm angeben. Wählen Sie dazu **Auswahl einzelner Pakete** im gleichen Bildschirm **Paketgruppenauswahl**.

Wählen Sie die zu installierenden sicherheitsrelevanten Pakete aus. Gehen Sie dazu nach den Anleitungen im *Offiziellen Red Hat Linux Installationshandbuch* vor. Als Suchhilfe ist eine Tabelle mit den entsprechenden Verzeichnissen als Tabelle 10–1, *Sicherheitspakete* angegeben.

Überprüfen Sie noch einmal, ob die richtigen Pakete ausgewählt sind, und fahren Sie dann mit dem Installationsprozess fort.

10.6 Aktualisieren einer älteren Version von Apache

Wenn Sie Red Hat Linux und Apache aktualisieren (einschließlich aller Versionen von Red Hat Linux Secure Web Server), müssen Sie zwei wichtige Punkte beachten:

- In der in Red Hat Linux 7.0 enthaltenen Version von Apache ist `/var/www/html` `DocumentRoot`.

- Möglicherweise haben Sie Ihre Apache Konfigurationsdatei angepasst (`httpd.conf`). Sicher möchten Sie wissen, was damit während des Aktualisierungsprozesses geschieht (lesen Sie dazu bitte weiter).

10.6.1 Wo befindet sich DocumentRoot?

Prinzipiell ist `DocumentRoot` das Verzeichnis auf Ihrem System, das die meisten der von Ihrem Apache Web-Server angebotenen Web-Seiten enthält. `DocumentRoot` wird über eine Konfigurationsanweisung in der Apache Konfigurationsdatei `httpd.conf` festgelegt. Falls Sie wenig Erfahrung mit der `DocumentRoot`-Konfigurationsanweisung haben, finden Sie in Abschnitt 12.1.28, *`DocumentRoot`* eine detailliertere Erklärung.

In früheren Versionen des mit Red Hat Linux ausgelieferten Apache Web-Servers war `DocumentRoot` auf `/home/httpd/html` eingestellt. In der Standardversion (ohne Verschlüsselung) der Apache Konfigurationsdatei ist `DocumentRoot` auf `/usr/local/apache/htdocs` eingestellt. Es ist auch möglich, dass Sie (oder ein Vorgänger) ein ganz anderes Verzeichnis als `DocumentRoot` festgelegt haben. Wichtig ist — in Red Hat Linux 7.0 ist die Standardeinstellung für `DocumentRoot` jetzt `/var/www/html`.

Ist das für Sie von Bedeutung? Es ist dann von Bedeutung, wenn Sie eine frühere Version von Apache als Server für Web-Seiten verwendet haben. Alle Web-Seiten, die vorher in einer anderen `DocumentRoot` untergebracht waren, werden von dem mit Red Hat Linux 7.0 ausgelieferten Apache in der Standardkonfiguration nicht mehr gefunden (bzw. nicht mehr vom Server zum Abruf angeboten). Deshalb müssen Sie eine der folgenden Aktionen durchführen:

Verschieben Sie alle Daten in der alten `DocumentRoot` (`/home/httpd/html`, `/usr/local/apache/htdocs` bzw. das entsprechende Verzeichnis) in das neue Verzeichnis (`/var/www/html`).

oder

Editieren Sie die Apache Konfigurationsdatei, und ändern Sie alle Referenzen auf `DocumentRoot` zurück auf den alten Verzeichnispfad.

Die von Ihnen gewählte Lösung hängt von Ihrer Systemkonfiguration ab. Wenn Sie auf Ihrem System `/home` automatisch mounten, ist es ungünstig, `DocumentRoot` in /home unterzubringen. Wenn Sie in /var andererseits wenig freien Speicherplatz haben, ist /var ebenfalls nicht der richtige Platz für DocumentRoot. Die Entscheidung über die beste Lösung liegt bei Ihnen bzw. Ihrem Systemadministrator und muss auf der Grundlage Ihrer Systemkonfiguration und den Anforderungen Ihres Web-Servers getroffen werden. Die Standardkonfiguration von Red Hat Linux Secure Web Server wurde so ausgelegt, dass sie den Anforderungen der meisten Webmaster entspricht. Leider ist es nicht möglich, eine für jede individuelle Situation optimale Konfiguration anzugeben.

10.6.2 Was passiert mit meinen alten Konfigurationsdateien?

Wenn Sie vorher eine andere Version von Apache installiert hatten und die Konfigurationsdateien angepasst haben, werden die Konfigurationsdateien während der Installation von Apache mit der Erweiterung .rpmsave in ihrem Verzeichnis gespeichert. Wenn Sie vorher eine andere Version von Apache installiert hatten, die Konfigurationsdateien aber nicht geändert haben, werden diese während der Installation überschrieben.

Nach der Installation von Apache können Sie mit Ausschneiden und Einfügen Ihre Änderungen aus der alten Apache Konfigurationsdatei (httpd.conf.rpmsave) in die neu installierte httpd.conf Konfigurationsdatei für den sicheren Server übertragen.

10.7 Aktualisieren einer älteren Version von Red Hat Linux

Wenn bereits eine ältere Version von Red Hat Linux auf Ihrem System läuft, müssen Sie Ihr Betriebssystem auf Red Hat Linux 7.0 aktualisieren (eine vollständige Installation ist nicht erforderlich). Wenn eine Aktualisierung erforderlich ist, müssen Sie statt einer Installationsklasse (Server, Workstation oder Benutzerdefiniert) **Aktualisieren** wählen. Folgen Sie den Anleitungen im *Offiziellen Red Hat Linux Installationshandbuch* zum Aktualisieren Ihres Systems. Während der Aktualisierung ist es erforderlich, dass Sie überprüfen, ob die Pakete für den sicheren Server vom Installationsprogramm ausgewählt werden.

Wenn Sie Ihr Red Hat Linux System aktualisieren, prüft das Installationsprogramm, welche Pakete bereits installiert sind. Diese Pakete werden während des Aktualisierungsprozesses automatisch auf die Versionen von Red Hat Linux 7.0 aktualisiert. Pakete, die noch nicht installiert waren, werden vom Installationsprogramm also nicht installiert — es sei denn, Sie passen Ihre Aktualisierung entsprechend an.

Wenn Sie eine US-amerikanische/kanadische Version von Red Hat Linux Professional aktualisieren, müssen Sie die Aktualisierung anpassen und die Pakete für den sicheren Server für die Installation auswählen. Falls `apache` bereits bei Ihnen installiert ist, fehlen `mod_ssl` und `openssl`, da sie vor Red Hat Linux 7.0 nicht in Red Hat Linux enthalten waren. Daher müssen Sie die Aktualisierung anpassen und zumindest `mod_ssl` und `openssl` auswählen. Eine Anleitung zum Finden der auszuwählenden Pakete finden Sie in Abschnitt 10.7.1, *Anpassung der Aktualisierung für die Installation des sicheren Servers*.

Wenn Sie eine internationale Version von Red Hat Linux Professional aktualisieren und die Pakete `apache`, `mod_ssl` und `openssl` bereits installiert sind, werden diese Programme automatisch vom Installationsprogramm ausgewählt und aktualisiert.

Wenn Sie eine internationale Version von Red Hat Linux Professional aktualisieren, die Pakete `apache`, `mod_ssl` oder `openssl` jedoch nicht installiert sind, müssen Sie die Aktualisierung anpassen und diese Pakete für die Installation auswählen. Anleitungen zum Finden der auszuwählenden Pakete finden Sie in Abschnitt 10.7.1, *Anpassung der Aktualisierung für die Installation des sicheren Servers*.

Wenn Sie Red Hat Linux Secure Web Server Version 1.0 oder 2.0 aktualisieren und Sie Ihren alten Schlüssel und Ihr altes Zertifikat weiter verwenden möchten, müssen Sie diese in das richtige Verzeichnis verschieben. Weitere Informationen darüber, wie mit in Red Hat Linux Secure Web Server Version 1.0 und 2.0 verwendeten Schlüsseln und Zertifikaten zu verfahren ist, finden Sie in Abschnitt 11.1, *Verwenden vorhandener Schlüssel und Zertifikate*.

10.7.1 Anpassung der Aktualisierung für die Installation des sicheren Servers

Wenn Sie den Aktualisierungsprozess anpassen müssen, folgen Sie bitte den Aktualisierungsanleitungen im *Offiziellen Red Hat Linux Installationshandbuch* . Im Prinzip ist **Upgraden** als **Installationstyp** und dann **Zu aktualisierende Pakete auswählen** auszuwählen. Anschließend müssen Sie die zu aktualisierenden Pakete auswählen, wie im Offiziellen Red Hat Linux Installationshandbuch beschrieben. Zur Erleichterung der Auswahl ist in Tabelle 10–1, *Sicherheitspakete* angegeben, wo jedes Server-relevante Paket abgelegt ist und ob es optional ist.

Tabelle 10–1 Sicherheitspakete

Paketbezeichnung	Enthalten in Gruppe	Optional?
`apache`	Systemumgebung/Dämonen	Nein
`mod_ssl`	Systemumgebung/Dämonen	Nein
`openssl`	Systemumgebung/Bibliotheken	Nein
`apache-devel`	Entwicklung/Bibliotheken	Ja
`apache-manual`	Dokumentation	Ja
`openssh`	Anwendungen/Internet	Ja
`openssh-askpass`	Anwendungen/Internet	Ja
`openssh-askpass-gnome`	Anwendungen/Internet	Ja
`openssh-clients`	Systemumgebung/Dämonen	Ja
`openssh-server`	Systemumgebung/Dämonen	Ja
`openssl-devel`	Entwicklung/Bibliotheken	Ja
`stunnel`	Anwendungen/Internet	Ja

10.8 Installieren des sicheren Servers nach der Installation von Red Hat Linux

Wenn Sie Red Hat Linux 7.0 ohne die Pakete für den sicheren Server installiert haben, können Sie den sicheren Server auch später nachinstallieren. Die einfachste Möglichkeit dafür ist die Installation der auf der Red Hat Linux-CD enthaltenen RPM-Pakete mit RPM, Gnome-RPM oder Kpackage.

Der Red Hat Linux Secure Web Server wird im RPM (RPM Package Manager)-Format geliefert. RPM ist ein System zur Zusammenstellung von Software-Paketen, mit dem Software-Pakete einfach installiert, deinstalliert, aktualisiert und abgefragt werden können. Wenn Sie Software ausschließlich mit RPM installieren, protokolliert RPM die auf Ihrem System installierten Pakete sowie die enthaltenen Dateien.

10.8.1 Anhalten aller laufenden Web-Server-Prozesse

Falls auf Ihrem System Web-Server ausgeführt werden, müssen alle Serverprozesse angehalten werden, bevor Sie mit der Installation von Red Hat Linux Secure Web Server beginnen können. Wenn Sie einen Apache Web-Server haben, können Sie als Root den Serverprozess durch Eingabe des entsprechenden Befehls bzw. der entsprechenden Befehle anhalten:

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

Für einen sicheren Web-Server auf Apache-Basis ist zum Anhalten des Serverprozesses der erste Befehl zu verwenden. Für einen normalen Apache Web-Server (ohne Verschlüsselung) ist der zweite Befehl zu verwenden. Wenn beide Servervarianten auf Ihrem System ausgeführt werden, sind beide Befehle anzugeben.

10.8.2 Verwenden von Gnome-RPM oder Kpackage

Wenn Sie GNOME oder KDE ausführen, können Sie ein GUI-Programm wie Gnome-RPM oder Kpackage zum Installieren der Pakete für den sicheren Server verwenden. Als Alternative können Sie auch RPM einsetzen.

Weitere Informationen zur Verwendung von Gnome-RPM finden Sie in Kapitel 6, *Gnome-RPM* und im *Offiziellen Red Hat Linux Handbuch Erste Schritte*. Anleitungen zur Verwendung von Kpackage finden Sie auf der *Kpackage Handbook*-Web-Seite unter http://www.general.uwa.edu.au/u/toivo/kpackage/.

10.8.3 Verwenden von RPM

Die Pakete für den Red Hat Linux Secure Web Server werden im RPM-Format geliefert, und daher können Sie die Pakete mit RPM installieren.

Mounten der CD-ROM

Zu Beginn des Installationsprozesses muss zuerst die CD-ROM gemountet werden. Legen Sie die entsprechende Red Hat Linux-CD in Ihr CD-ROM-Laufwerk. Geben Sie als Root den folgenden Befehl zum Mounten der CD ein:

```
mount /mnt/cdrom
```

Dieser Befehl wird erfolgreich ausgeführt, wenn die Datei `/etc/fstab` einen Eintrag für das CD-ROM-Laufwerk enthält. Wenn aus irgendeinem Grund nach der Eingabe des Befehls eine Fehlermeldung ausgegeben wird, können Sie folgenden Befehl versuchen:

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

um die CD-ROM zu mounten. Sie oder der Systemadministrator können auch anderen Benutzern (zusätzlich zu Root) das Mounten des CD-ROM-Laufwerks erlauben. Zum Installieren der Pakete mit RPM müssen Sie aber auf jeden Fall als Root angemeldet sein.

Wechseln Sie nach dem Mounten des CD-ROM-Laufwerks im nächsten Schritt mit `cd` in das Verzeichnis auf der CD, das die RPMs enthält.

```
cd /mnt/cdrom/RedHat/RPMS
```

Installieren Sie danach mit RPM die gewünschten Pakete. Sie müssen `apache`, `openssl` und `mod_ssl` installieren.

Um zum Beispiel das Paket `apache` zu installieren, müssen Sie sich als Root anmelden (wenn Sie es nicht bereits sind) und den folgenden Befehl eingeben:

```
# rpm -Uvh apache-1.3.12-3.i386.rpm
```

```
apache                      ###########################
```

Das Paket `apache` wird installiert. Dieser Befehl muss für alle zu installierenden Pakete wiederholt werden.

Bitte beachten

Die vollständigen Anleitungen zur Verwendung von RPM finden Sie im Kapitel 5, *Paketverwaltung mit RPM*. (Eine zusammengefasste Version derselben Anleitungen finden Sie im *Offiziellen Red Hat Linux Handbuch Erste Schritte*.) RPM ist ein leistungsfähiges Paketmanagementsystem. Bitte lesen Sie alle Anleitungen zur Verwendung von RPM durch, wenn Sie Fragen zur Verwendung haben.

Wenn Sie die Installation Ihrer Pakete abgeschlossen haben, müssen Sie Ihre CD-ROM unmounten. Wechseln Sie dazu zuerst mit `cd ..` in das Verzeichnis `/mnt/cdrom` eine Ebene höher. Geben Sie anschließend den Befehl `umount /mnt/cdrom` ein, um die CD-ROM zu unmounten. Geben Sie jetzt `eject /mnt/cdrom` ein. Das CD-ROM-Laufwerk wird geöffnet, damit Sie die CD entnehmen können.

Nach der Installation der erforderlichen Pakete wird im nächsten Schritt Ihr Schlüssel erstellt und ein Zertifikat angefordert. Bitte lesen Sie zur Erstellung ihres Schlüssels und des Zertifikats in Kapitel 11, *Beantragen eines Zertifikats für Ihren sicheren Server* weiter.

10.9 Hilfe und Dokumentation

Wenn Sie nach den in Kapitel 10, *Installieren von Red Hat Linux Secure Web Server* angegebenen Schritten vorgegangen sind, dabei aber ein Problem aufgetreten ist, sollten Sie als Erstes den Bereich Red Hat Errata der Red Hat-Website unter http://www.redhat.com/support/errata konsultieren.

Wenn Sie ein offizielles Red Hat-Software-Produkt einschließlich Support erworben haben, können Sie den technischen Support in Anspruch nehmen. Auf der Red Hat

Support-Website http://www.redhat.com/support sollten Sie sich für den Support registrieren.

10.9.1 Nützliche Informationsquellen

Hier eine Auswahl weiterer Informationsquellen zu Apache und mod_ssl:

- Die Tipps, FAQs und HOWTO-Dokumente auf der Red Hat-Website unter http://www.redhat.com/support/docs/howto/
- Die Red Hat Linux Apache Centralized Knowledgebase unter http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html
- Auf Ihrem Rechner wurde bei der Installation von Red Hat Linux Secure Web Server auch die Dokumentation installiert. Nach der erfolgreichen Installation von Red Hat Linux Secure Web Server, doch vor dem Wechsel Ihrer Homepage, können Sie auf die HTML-Dokumentation auf Ihrem Rechner über die URL Ihrer Domäne (http://ihre_domäne) zugreifen.
- Auf der Apache Website finden Sie die vollständige Dokumentation für den Apache Web-Server unter http://www.apache.org/docs/
- Die mod_ssl-Website (http://www.modssl.org/ ist die beste Quelle für Informationen zu mod_ssl. Auf dieser Website wird eine Fülle von Dokumentationen angeboten, darunter ein *User Manual* (Benutzerhandbuch) unter http://www.modssl.org/docs/.
- Die Mailingliste redhat-secure-server. Unter http://www.redhat.com/community/list_subscribe.html können Sie sich in diese Mailingliste eintragen.

  Sie können sich auch in die Mailingliste redhat-secure-server eintragen, indem Sie eine E-Mail an `redhat-secure-server-request@redhat.com` schicken und in die Betreffzeile "subscribe" eintragen (ohne Anführungszeichen).
- Nach der Installation eines Pakets befindet sich die Dokumentation für jedes Paket (falls eine Dokumentation existiert) in `/usr/share/doc/`*`<Paketname> <Versionsnummer>/`*.

10.10 Deinstallieren von Red Hat Linux Secure Web Server

Wenn Sie Red Hat Linux Secure Web Server deinstallieren müssen, können Sie die folgenden Befehle verwenden (als Root): `rpm -e mod_ssl`, `rpm -e openssl` und `rpm -e apache`.

11 Beantragen eines Zertifikats für Ihren sicheren Server

In diesem Kapitel wird erläutert, wie Sie ein Zertifikat beantragen und installieren, das Ihren Server vor unberechtigten Zugriffen schützt und seine Echtheit bestätigt.

Damit die Daten Ihrer Kunden beim Geschäftsverkehr über das Web sicher und geschützt sind, müssen Sie Ihren Web-Server vor unberechtigten Zugriffen schützen. Sichere Server verwenden das Protokoll **Secure Sockets Layer** (SSL), das die zwischen Browser und Server übertragenen Daten verschlüsselt. Wenn Ihr Browser mit SSL Daten überträgt, wird in der Navigationsleiste vor der URL (URL = Uniform Resource Locator) das Präfix https: angezeigt.

Ihre Kunden können beruhigt im Web einkaufen, wenn sie wissen, dass ihre Transaktionen nicht in die falschen Hände geraten. Sichere Server werden jedoch nicht nur für den elektronischen Handel verwendet, sondern übermitteln auch sicherheitsrelevante Daten wie Verkaufszahlen über das Internet an Verkäufer oder Geschäftspartner.

Sichere Server weisen sich mit einem Zertifikat bei den Web-Browsern aus. Sie können entweder ein eigenes Zertifikat generieren (mit eigener Signatur) oder eines von einer anerkannten Zertifizierungsstelle (ZS) erwerben. Sie haben dann die Garantie, dass die betreffende Website tatsächlich mit dem angegebenen Unternehmen oder der Organisation verbunden ist.

Wenn Sie Ihren Server für den elektronischen Handel (E-Commerce) einsetzen, sollten Sie ein Zertifikat von einer ZS erwerben. Dies hat die folgenden Vorteile: die Browser erkennen ein solches Zertifikat in der Regel automatisch an und die ZS garantiert, dass die für die Website verantwortliche Organisation tatsächlich die ausgewiesene ist. Selbstgenerierte Zertifikate mit eigener Signatur werden nicht automatisch von den Browsern akzeptiert. Statt dessen wird der betreffende Benutzer gefragt, ob das Zertifikat akzeptiert und die Verbindung hergestellt werden soll.

Wenn Sie das Zertifikat einer Zertifizierungsstelle verwenden, ist die Identität der Organisation, die den Server betreibt, garantiert. Beispiel: das Zertifikat weist Red Hat als Eigentümer der Website aus, und die ZS ist vertrauenswürdig. Sie können dann sicher sein, dass alle Dateien und Programme, die Sie von dieser Site herunterladen, tatsächlich von Red Hat stammen.

Als ersten Schritt erstellen Sie einen öffentlichen und einen privaten Schlüssel. Anschließend senden Sie entweder einen Zertifikatsantrag an die Zertifizierungsstelle oder Sie erstellen ein Zertifikat mit eigener Signatur. In diesem Kapitel wird erläutert, wie Sie signierte Zertifikate bei VeriSign (http://www.verisign.com, Informationen zu Preisnachlässen für Red Hat Kunden unter http://www.verisign.com/offer/redhat/) und Thawte (http://www.thawte.com) beantragen und wie Sie ein eigenes Zertifikat erstellen.

Bitte beachten

Sie können signierte Zertifikate bei beliebigen Zertifizierungsstellen Ihrer Wahl beantragen und sind nicht auf die in diesem Handbuch angegebenen festgelegt. VeriSign bietet jedoch Kunden von Red Hat einen Preisnachlass an. Weitere Informationen zum Preisnachlass von VeriSign finden Sie unter http://www.verisign.com/offer/redhat.

In diesem Kapitel wird darüber hinaus erläutert, wie Sie ein eigenes Zertifikat oder ein Zertifikat einer ZS auf Ihrem Red Hat Linux Secure Web Server installieren.

11.1 Verwenden vorhandener Schlüssel und Zertifikate

Wenn Sie bereits über einen Schlüssel und ein Zertifikat verfügen (z.B., wenn Sie Red Hat Linux Secure Web Server installieren, um den sicheren Web-Server eines anderen Herstellers zu ersetzen), ist es mit großer Wahrscheinlichkeit möglich, den vorhandenen Schlüssel und das Zertifikat auch mit Red Hat Linux Secure Web Server zu verwenden. In den folgenden Situationen können Sie bereits vorhandene Schlüssel und Zertifikate jedoch nicht wieder verwenden:

- Sie ändern die IP-Adresse oder den Domänennamen.

- Sie besitzen ein Zertifikat von VeriSign und verwenden eine neue Server-Software.

Alte Schlüssel und Zertifikate können nicht wiederverwendet werden, wenn Sie die IP-Adresse oder den Domänennamen ändern. Zertifikate werden für eine bestimmte Kombination aus IP-Adresse und Domänenname vergeben. Wenn Sie entweder IP-Adresse oder Domänennamen ändern, müssen Sie ein neues Zertifikat beantragen.

VeriSign ist eine renommierte Zertifizierungsstelle. Wenn Sie bereits ein Zertifikat von VeriSign für einen anderen Zweck besitzen, würde es sich anbieten, dieses mit dem neuen Red Hat Linux Secure Web Server zu verwenden. Die Zertifikate von VeriSign sind jedoch nicht übertragbar, da sie nur für eine bestimmte Server-Software und eine bestimmte Kombination aus IP-Adresse und Domänenname ausgestellt werden.

Sobald Sie einen dieser Parameter ändern (Sie ersetzen beispielsweise Ihr bisheriges sicheres Web-Server-Produkt durch Red Hat Linux Secure Web Server), können Sie das vorhandene VeriSign-Zertifikat nicht mehr verwenden, sondern müssen ein neues beantragen.

Wenn Sie über einen gültigen Schlüssel und ein gültiges Zertifikat verfügen, müssen Sie die Anleitungen in Kapitel 11, *Beantragen eines Zertifikats für Ihren sicheren Server* nicht befolgen. Statt dessen müssen Sie die Dateien, die Schlüssel und Zertifikat enthalten, verschieben oder umbenennen.

Verschieben Sie die vorhandene Schlüsseldatei in das Verzeichnis:

```
/etc/httpd/conf/ssl.key/server.key
```

Verschieben Sie die vorhandene Zertifikatsdatei in das Verzeichnis:

```
/etc/httpd/conf/ssl.crt/server.crt
```

Fahren Sie dann bei Abschnitt 11.10, *Testen Ihres Zertifikats* fort.

Wenn Sie von den Versionen 1.0 und 2.0 des Red Hat Secure Web Server upgraden, werden Schlüssel (`httpsd.key`) und Zertifikat (`httpsd.crt`) im Verzeichnis `/etc/httpd/conf/` abgelegt. Sie müssen Schlüssel und Zertifikat verschieben und umbenennen, damit der Red Hat Linux Secure Web Server sie verwenden kann.

Mit den folgenden Befehlen können Sie Schlüssel- und Zertifikatsdateien verschieben und umbenennen:

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

Starten Sie den Red Hat Linux Secure Web Server dann, wie in Abschnitt 11.11, *Starten und Beenden von Apache* beschrieben. Sie müssen kein neues Zertifikat erwerben, wenn Sie von einer vorherigen Version des Red Hat Linux Secure Web Server upgraden.

11.2 Sicherheit der Web Server im Überblick

Zur gesicherten Datenübertragung verwendet der Red Hat Linux Secure Web Server das Protokoll Secure Sockets Layer (SSL) und (in den meisten Fällen) digitale Zertifikate von offiziellen Zertifizierungsstellen. SSL verschlüsselt die Daten bei der Übertragung und regelt die Authentifzierung zwischen Browsern und dem Red Hat Linux Secure Web Server. Das zugelassene digitale Zertifikat liefert die Authentifizierung für Ihren Red Hat Linux Secure Web Server (die Zertifizierungsstelle steht mit ihrem Namen für die Echtheit der Identität Ihrer Organisation).

Die Art der Verschlüsselung hängt von den verwendeten Schlüsseln ab. (Die Schlüssel sind eine Art geheimer Ringe in Datenformat zur Kodierung und Dekodierung). Bei der konventionellen oder symmetrischen Verschlüsselung verfügen beide Seiten der Transaktion über denselben Schlüssel, mit dem sie die jeweiligen Übertragungen dekodieren. Bei der öffentlichen oder asymmetrischen Verschlüsselung gibt es zwei Schlüssel: einen öffentlichen und einen privaten Schlüssel. Personen oder Organisationen halten ihren privaten Schlüssel geheim, der öffentliche Schlüssel wird jedoch bekannt gegeben. Daten, die mit dem öffentlichen Schlüssel kodiert wurden, können nur mit dem privaten dekodiert werden. Umgekehrt können Daten, die mit dem privaten Schlüssel kodiert wurden, nur mit dem öffentlichen dekodiert werden.

Bei der Verschlüsselung unter Verwendung öffentlicher Schlüssel wird ein Paar aus öffentlichem und privatem Schlüssel erstellt. In den meisten Fällen senden Sie Ihren

Zertifikatsantrag (einschließlich öffentlichem Schlüssel), einen Nachweis der Identität Ihres Unternehmens und die Zahlung an die Zertifizierungsstelle. Die ZS überprüft den Antrag und die Identität Ihres Unternehmens und sendet ein Zertifikat für Ihren Red Hat Linux Secure Web Server zurück.

Als Alternative haben Sie die Möglichkeit, ein eigensigniertes Zertifikat zu erstellen. Diese Zertifikate sollen jedoch nicht in Produktionsumgebungen verwendet werden. Weitere Informationen zu den Unterschieden zwischen Zertifikaten mit eigener und offizieller Signatur finden Sie in Abschnitt 11.3, *Verschiedene Arten von Zertifikaten*.

11.3 Verschiedene Arten von Zertifikaten

Wenn Sie den Red Hat Linux Secure Web Server über das Red Hat Linux Installationsprogramm installiert haben, werden ein zufälliger Schlüssel und ein Test-Zertifikat erzeugt und in den entsprechenden Verzeichnissen gespeichert. Bevor Sie mit dem sicheren Server arbeiten können, müssen Sie jedoch Ihren eigenen Schlüssel generieren und ein Zertifikat beantragen, das Ihren Server korrekt identifiziert.

Sie benötigen einen Schlüssel und ein Zertifikat, um den Red Hat Linux Secure Web Server betreiben zu können und haben die Auswahl zwischen einem eigensigniertem und einem ZS-signierten Zertifikat. Wo liegen die Unterschiede?

Ein Zertifikat mit offizieller Signatur von der ZS hat zwei Vorteile:

- Browser erkennen das Zertifikat in der Regel automatisch an. Die gesicherte Verbindung wird ohne zusätzliche Bestätigung durch den Benutzer hergestellt.
- Mit dem signierten Zertifikat gewährleistet die Zertifizierungsstelle die Echtheit und Identität der Organisation, die dem Browser die Web-Seiten zur Verfügung stellt.

Sie können für Ihren Red Hat Linux Secure Web Server ein eigenes Zertifikat generieren. Bedenken Sie jedoch, dass es nicht dieselben Vorteile bietet wie ein Zertifikat von offizieller Stelle. Von den Browsern der Benutzer wird es nicht automatisch anerkannt, und es liefert keine Garantie bezüglich der Echtheit und Identität der Organisation, die die Website bereitstellt. Diese wichtigen Voraussetzungen für die Sicherheit Ihres Servers werden von einem Zertifikat mit ZS-Signatur erfüllt. Wenn Ihr

Server in eine Produktionsumgebung eingebunden ist, benötigen Sie wahrscheinlich ein Zertifikat mit ZS-Signatur.

Wenn Ihr Red Hat Linux Secure Web Server durch viele Benutzer verwendet werden soll, ist ein Zertifikat mit ZS-Signatur erforderlich. Nur so können Besucher Ihrer Website auch wirklich sichergehen, dass die Website tatsächlich der angegebenen Organisation gehört. Die ZS überprüft zunächst die Identität der Organisation, die das Zertifikat beantragt.

Die meisten Web-Browser, die SSL unterstützen, verfügen über eine Liste von Zertifizierungsstellen, deren Zertifikate sie automatisch akzeptieren. Falls ein Browser auf ein Zertifikat trifft, das nicht von einer in der Liste befindlichen ZS ausgestellt wurde, wird der Benutzer aufgefordert, sich zu entscheiden, ob die Verbindung angenommen oder abgelehnt werden soll.

Die Beantragung eines Zertifikats von einer Zertifizierungsstelle ist denkbar einfach. Es folgt ein kurzer Überblick:

- Erstellen Sie einen privaten und einen öffentlichen Schlüssel.
- Erstellen Sie einen Zertifikatsantrag auf Basis des öffentlichen Schlüssels. Der Antrag enthält Informationen über Ihren Server und Ihr Unternehmen.
- Senden Sie den Zertifikatsantrag zusammen mit den Dokumenten, die Ihre Identität belegen, an eine ZS.
- Nach Überprüfung der Identität und Echtheit Ihres Unternehmens sendet die Zertifizierungsstelle Ihnen ein digitales Zertifikat.
- Installieren Sie dieses auf Ihrem Web-Server, und Ihre Transaktionen sind nun gegen unerlaubten Zugriff geschützt.

11.4 Auswählen einer Zertifizierungsstelle

Wir können Ihnen die Entscheidung bei der Auswahl einer Zertifizierungsstelle nicht abnehmen. Sie werden sich von eigenen Erfahrungen, Erfahrungen von Freunden oder Kollegen oder von Kostenfaktoren leiten lassen. Im Folgenden wird erläutert, wie Sie ein digitales Zertifikat von VeriSign oder von Thawte erwerben. Sie können jedoch auch eine andere Zertifizierungsstelle wählen.

Es gibt noch viele weitere Zertifizierungsstellen. Klicken Sie auf den Button **Security** in der Symbolleiste von Navigator oder auf das Vorhängeschlosssymbol links unten auf dem Bildschirm. Klicken Sie dann auf **Signers**, um eine Liste der Zertifizierungsstellen anzuzeigen, deren Zertifikate Ihr Browser akzeptiert. Sie können auch im Web nach Zertifizierungsstellen suchen. Die Beantragung eines Zertifikats wird auch bei anderen Zertifizierungsstellen im Wesentlichen so ablaufen wie in diesem Handbuch beschrieben.

11.4.1 Zertifikatspaket von VeriSign

VeriSign bietet für Kunden von Red Hat Rabatte auf seine Zertifikatsangebote. Informationen hierzu finden Sie unter http://www.verisign.com/offer/redhat/.

VeriSign und Thawte bieten verschiedene Optionen für die angebotenen Server-Zertifikate. Sie sind im Folgenden aufgeführt. Vollständige und aktuelle Informationen erhalten Sie auf der entsprechenden Website.

Commerce Site Services

Commerce Site (mit 40-Bit-Verschlüsselung und dem Online-Zahlungsverwaltungsservice Payflow Pro)

Commerce Site Pro (mit 128-Bit-Verschlüsselung und dem Online-Zahlungsverwaltungsservice Payflow Pro)

Secure Site Services

Secure Site (mit 40-Bit-Verschlüsselung)

Secure Site Pro (mit 128-Bit-Verschlüsselung)

Die 128-Bit SSL IDs von VeriSign ermöglichen die weltweit stärkste Verschlüsselungstechnologie für Web-Server in Verbindung mit den verschiedenen Versionen der Microsoft- und Netscape-Browser für die USA und den internationalen Markt.

Die Lösungen von VeriSign umfassen ein SSL-Server-Zertifikat (oder "Server ID") und andere Funktionen, wie z.B.:

- NetSure Protection Plan, ein erweitertes Gewährleistungsprogramm, das VeriSign-Kunden vor einem finanziellen Verlust von bis zu $250.000 schützt, der durch Diebstahl, Beschädigung, unrechtmäßige Benutzung oder Verlust eines Zertifikats entsteht.

- VeriSign Secure Site Seal ermöglicht Besuchern die Überprüfung von ID und Status Ihres Servers in Echtzeit.
- Commerce Site Services und Secure Site Services umfassen außerdem Site Performance Measurement Services (Dienste zur Überwachung wichtiger Leistungsdaten Ihrer Site), Netcraft E-Commerce Security Analysis (Sicherheitsanalyse für E-Commerce) und Netzwerk-Scanning von Qualys zur Ermittlung der potentiellen Angriffsflächen Ihrer Site.
- Schulungsrabatte für den von VeriSign angebotenen Kurs ‘‘Building Secure Web Servers.’’
- Ein geprüfter Authentifizierungsprozess, der sicherstellt, dass VeriSign die Echtheit der Identität aller mit einer Server ID ausgestatteten Sites bestätigt.

Weitere Informationen zu den Server-ID-Lösungen von VeriSign finden Sie unter http://www.verisign.com/server/index.html. Weitere Informationen zu den SSL-Server-Zertifikaten von Thawte finden Sie unter http://www.thawte.com/certs/server/contents.html.

11.5 Nachweisen der Identität Ihrer Organisation gegenüber einer Zertifizierungsstelle

Wenn Sie ein signiertes Zertifikat beantragen, müssen Sie der Zertifizierungsstelle beweisen, dass Ihre Organisation das Recht hat, unter dem angegebenen Namen Geschäfte zu tätigen. Welche Daten und Dokumente die Zertifizierungsstellen im Einzelnen verlangen, ist unterschiedlich. Fragen Sie daher bei der Zertifizierungsstelle Ihrer Wahl an, welche Anforderungen Sie erfüllen müssen.

In einigen Fällen müssen Kopien der folgenden Dokumente per Mail oder Fax an die ZS gesendet werden. Das Zertifikat wird erst ausgestellt, wenn diese Dokumente bei der ZS eingegangen sind und überprüft wurden.

11.5.1 Nachweis der Organisations-Identität bei VeriSign

Die einfachste Möglichkeit, die Geschäftsberechtigung Ihrer Organisation zu beweisen, ist die Angabe Ihrer D-U-N-S-Nummer (DUNS = Dun & Bradstreet). Wenn Sie diese Nummer nicht besitzen, können Sie sie auf der Website von Dun & Bradstreet unter http://www.dnb.com/dunsno/whereduns.htm anfordern.

Wenn Sie nicht wissen, ob Sie eine D-U-N-S-Nummer besitzen, können Sie bei VeriSign unter https://digitalid.verisign.com/dnb_query.htm nachforschen.

Wenn Sie keine D-U-N-S-Nummer besitzen und auch keine anfordern möchten, lesen Sie unter http://www.verisign.com/server/enroll/globalpreparing.html#proof nach, welche Dokumente Sie VeriSign überlassen müssen.

11.5.2 Identitätsnachweise für Thawte

Unter http://www.thawte.com/certs/server/docs.html finden Sie eine Liste der Nachweise, die Thawte zur Anerkennung der Identität Ihrer Organisation benötigt. Zum Zeitpunkt der Erstellung dieser Dokumentation mussten die folgenden Nachweise geliefert werden:

1. Nachweis über den Namen der Organisation
2. Nachweis über das Recht an einem Domänennamen

Sie müssen nachweisen können, dass Sie das Recht haben, die Organisation oder das Unternehmen unter diesem Namen zu führen. Hierzu wird beispielsweise eine Kopie der offiziellen Registrierung des Unternehmens oder der Gründungsurkunde für Ihren Bundesstaat oder Ihr Land benötigt. Weitere mögliche Dokumente zum Nachweis des Organisationsnamens finden Sie unter http://www.thawte.com/certs/server/right_name.html.

Den Domänennamen müssen Sie nicht nachweisen, wenn der registrierte Domänenname dem Namen des Unternehmens entspricht, den Sie in Ihren (noch nicht erstellten) Zertifikatsantrag aufnehmen werden. Dies wird in den meisten Fällen zutreffen. Führen Sie auf Ihrer Domäne ein `whois` aus, um die Registrierungsinformationen Ihrer Domäne anzuzeigen. Unter http://www.thawte.com/certs/server/right_domain.html finden Sie weitere Informationen darüber, wie Sie Ihr Recht auf eine Domäne belegen, wenn die Informationen in Ihrem Zertifikatsantrag nicht genau mit denen übereinstimmen, die von einem `whois` zurückgegeben werden.

Sobald Sie alle benötigten Informationen zum Nachweis der Identität Ihrer Organisation zusammengetragen haben, können Sie einen Schlüssel und einen Zertifikatsantrag erstellen.

11.6 Generieren von Schlüsseln

Zunächst müssen Sie den Schlüssel und das Zertifikat entfernen, die während der Installation generiert wurden. `cd` in das Verzeichnis `/etc/httpd/conf`.

Entfernen Sie die zwei Dateien mit den folgenden Befehlen:

```
rm ssl.key/server.key
```

und

```
rm ssl.crt/server.crt
```

Als ersten Schritt zur Erstellung eines Zertifikats erstellen Sie einen eigenen zufallsgenerierten Schlüssel mit dem folgenden Befehl:

```
make genkey
```

Ihr System zeigt eine Meldung ähnlich der folgenden an:

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
................................................................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

Geben Sie nun ein Passwort ein. Ein sicheres Passwort sollte mindestens acht Zeichen umfassen, Zahlen und Satzzeichen enthalten und nicht einem Wörterbuch entnommen sein. Denken Sie außerdem daran, dass Klein- und Großschreibung beachtet werden.

Bitte beachten

Sie müssen das Passwort bei jedem Start von Red Hat Linux Secure Web Server eingeben. Vergessen Sie es nicht.

Sie werden aufgefordert, das Passwort zur Bestätigung ein zweites Mal einzugeben. Wenn es korrekt eingegeben wurde, wird die Datei `server.key` mit Ihrem Schlüssel erstellt.

Wenn Sie das Passwort nicht bei jedem Start des Red Hat Linux Secure Web Server eingeben möchten, verwenden Sie anstelle von `make genkey` die folgenden beiden Befehle, um den Schlüssel zu generieren. Beide Befehle sollten in einer Zeile eingegeben werden.

Mit dem Befehl:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

erzeugen Sie Ihren Schlüssel. Verwenden Sie dann den folgenden Befehl:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

um sicherzustellen, dass die Berechtigungen im Schlüssel korrekt gesetzt sind.

Wenn Sie diese Befehle zur Generierung des Schlüssels verwenden, müssen Sie Ihren Red Hat Linux Secure Web Server nicht mit einem Passwort starten.

ACHTUNG

Der Zugriffsschutz auf Ihren Web-Server ist gefährdet, wenn Sie die Passwort-Funktion deaktivieren. Aus diesem Grund wird davon abgeraten, die Passwort-Funktion für Ihren Red Hat Linux Secure Web Server zu deaktivieren.

Die Probleme, die mit der Deaktivierung des Passworts verbunden sind, stehen in direktem Zusammenhang mit der Sicherheit des Host-Systems. Personen mit krimineller Energie, die die regulären UNIX-Sicherheitsfunktionen auf dem Host-Rechner außer Kraft setzen, könnten Ihren privaten Schlüssel (den Inhalt Ihrer Datei `server.key`) abrufen. Mit diesem Schlüssel können falsche Web-Seiten erstellt werden, die scheinbar von Ihrer Site kommen.

Wenn alle von UNIX vorgesehenen Sicherheitsvorkehrungen für den Host-Computer genau eingehalten werden (d.h. alle Betriebssystem-Patches und -aktualisierungen werden bei Verfügbarkeit installiert, es werden keine unnötigen oder risikoreichen Services in Anspruch genommen usw.) mag das Red Hat Linux Secure Web Server Passwort nicht notwendig erscheinen. Da der Red Hat Linux Secure Web Server jedoch selten neu gestartet werden muss, lohnt es sich in den meisten Fällen, die Sicherheit durch ein Passwort noch zu erhöhen.

Die Datei `server.key` sollte Eigentum des Root-Benutzers Ihres Systems und für andere Benutzer nicht zugänglich sein. Erstellen Sie eine Sicherungskopie dieser Datei, und bewahren Sie die Kopie an einem sicheren Ort auf. Die Sicherungskopie ist wichtig für den Fall, dass die Datei `server.key` nach der Erstellung des Zertifikatsantrags verloren gehen sollte. In diesem Fall ist das Zertifikat ungültig, und die Zertifizierungsstelle wird Ihnen nicht helfen können. Die einzige Möglichkeit wäre dann das Beantragen (und Bezahlen) eines neuen Zertifikats.

Wenn Sie ein Zertifikat von einer Zertifizierungsstelle erwerben, fahren Sie bei Abschnitt 11.7, *Erzeugen von Zertifikatsanträgen für die Zertifizierungsstelle* fort. Wenn Sie ein eigenes Zertifikat erstellen, fahren Sie bei Abschnitt 11.9, *Erstellen eines Zertifikats mit eigener Signatur* fort.

11.7 Erzeugen von Zertifikatsanträgen für die Zertifizierungsstelle

Nach dem Schlüssel wird nun ein Zertifikatsantrag erstellt, den Sie an die Zertifizierungsstelle Ihrer Wahl senden. Geben Sie den folgenden Befehl ein:

```
make certreq
```

Das System zeigt die folgende Ausgabe an und fordert Sie auf, ein Passwort einzugeben (bei aktivierter Passwortoption):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Geben Sie das Passwort ein, das Sie bei der Generierung des Schlüssels ausgewählt haben. Es werden einige Anweisungen angezeigt, und Sie werden aufgefordert, eine Reihe von Fragen zu beantworten. Ihre Eingaben werden in den Zertifikatsantrag aufgenommen. Die folgende Abbildung zeigt einen Antrag mit möglichen Antworten:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter ’.’, the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Baden Württemberg
Locality Name (eg, city) []:Heidelberg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Testunternehmen
Organizational Unit Name (eg, section) []:Test
Common Name (eg, your name or your server’s hostname) []:test.meinedomäne.com
Email Address []:admin@meinedomäne.com
Please enter the following ’extra’ attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Die Standardantworten werden in eckigen Klammern `[]` angezeigt, unmittelbar nach den jeweiligen Eingabeaufforderungen. Die erste Angabe ist beispielsweise das Land, in dem das Zertifikat verwendet werden soll:

```
Country Name (2 letter code) [AU]:
```

Die vordefinierte Eingabe in eckigen Klammern ist **AU**. Wenn Sie den Standardwert akzeptieren möchten, drücken Sie die [Eingabetaste]. Anderenfalls geben Sie den zweistelligen Code für Ihr Land ein.

Geben Sie dann die restlichen Daten ein (`State or Province Name`, `Locality Name`, `Organization Name`, `Organizational Unit Name`, `Common Name` und `Email address`). Befolgen Sie beim Eingeben der Informationen die folgenden Richtlinien:

- Kürzen Sie Ort oder Bundesstaat nicht ab. Schreiben Sie alle Namen aus.
- Wenn Sie den Antrag an eine Zertifizierungsstelle senden, sollten die Informationen in allen Feldern, besonders jedoch in den Feldern `Organization Name` und `Common Name` korrekt sein. Die Zertifizierungsstelle überprüft anhand der Informationen im Antrag, ob Ihre Organisation tatsächlich für den allgemeinen Namen, den Sie unter `Common Name` angegeben haben, verantwortlich ist. Alle Anträge, die ungültige Informationen enthalten, werden abgelehnt.
- Geben Sie für `Common Name` die *richtige* Bezeichnung Ihres Red Hat Linux Secure Web Server ein (eine gültige DNS-Bezeichnung), keine eventuell vorhandenen Aliasnamen.
- Geben Sie unter `Email Address` die E-Mail-Adresse des Webmasters oder Systemadministrators ein.
- Vermeiden Sie Sonderzeichen wie @, #, &, ! usw. Einige Zertifizierungsstellen lehnen Anträge ab, die Sonderzeichen enthalten. Falls der Name Ihres Unternehmens also das Zeichen & enthält, schreiben Sie dieses als "und" statt als "."
- Die zusätzlichen Attribute (`A challenge password` und `An optional company name`) müssen Sie nicht ausfüllen. Drücken Sie einfach die [Eingabetaste], um die in der Voreinstellung leeren Felder zu akzeptieren.

Wenn Sie alle Informationen eingegeben haben, wird die Datei `server.csr` erstellt. `server.csr` ist Ihre Zertifikatsanfrage, die an die Zertifizierungsstelle gesendet werden kann.

11.8 Erwerben eines Zertifikats

Den erstellten Antrag müssen Sie nun zu einer ZS senden.

11.8.1 Erwerben eines Zertifikats von VeriSign

Zunächst müssen Sie entscheiden, was für ein Zertifikat Sie erwerben möchten. Eine Beschreibung der Zertifizierungsprodukte von VeriSign finden Sie in Abschnitt 11.4.1, *Zertifikatspaket von VeriSign*.

Rufen Sie dann die Website /www.verisign.com/server/ auf. Wählen Sie das Zertifikat aus, das Sie kaufen möchten.

Der Kaufvorgang ist bis zu einem gewissen Grad standardisiert. Sie erhalten im Folgenden schrittweise Anleitungen zum Erwerb des Zertifikats "Secure Site". Sie sollten anhand dieser Anleitungen auch ein anderes Zertifikat erwerben können.

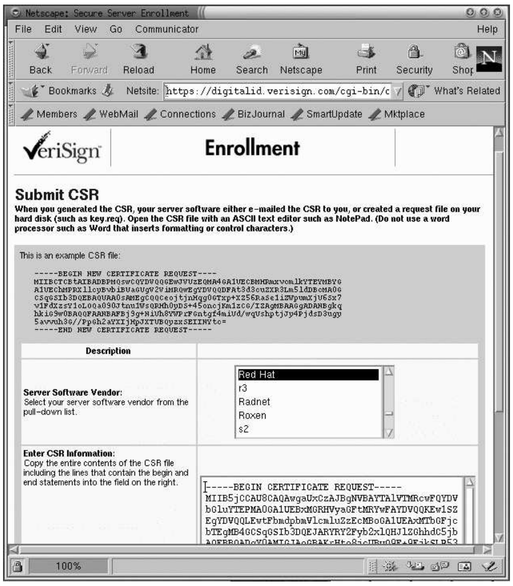
1. Für Zertifikate des Typs "Secure Site" können Sie, wenn gewünscht, eine Zweijahres-Option (**Two Year Option**) auswählen und den Standort Ihres Secure Servers bestätigen. Klicken Sie auf **Continue**, sobald Sie die Auswahl abgeschlossen haben.

2. Die nächste Seite **Preparing for Enrollment** wird aufgerufen. Hier erhalten Sie eine Zusammenfassung der Informationen, die Sie VeriSign zur Verfügung stellen müssen. Lesen Sie diese Seite, und stellen Sie sicher, dass alle nötigen Informationen bereitstehen, bevor Sie mit dem Antrag fortfahren. Klicken Sie dann auf den Button **Continue** am unteren Rand der Seite.

3. Die nächste Seite **CSR: Wizard: Verify Distinguished Name** wird angezeigt. Wenn Sie noch keinen Schlüssel und Antrag gemäß den in Abschnitt 11.6, *Generieren von Schlüsseln* und Abschnitt 11.7, *Erzeugen von Zertifikatsanträgen für die Zertifizierungsstelle* gegebenen Anweisungen erstellt haben, holen Sie dies jetzt nach. Wählen Sie dann das Kontrollkästchen **I have already prepared a CSR for this enrollment**, und klicken Sie auf **Continue**.

4. Der nächste Schritt, **Submit CSR**, wird in Abbildung 11–1, *Übergeben des Zertifikatsantrags an VeriSign* gezeigt. Wählen Sie aus der Liste **Server Software Vendor** die Option **Red Hat** aus.

Abbildung 11–1 Übergeben des Zertifikatsantrags an VeriSign



Fügen Sie den Inhalt Ihres Antrags in das Textfeld **Enter CSR Information** ein. Um den Inhalt der Datei auszuschneiden und einzufügen, wechseln Sie zunächst in das Verzeichnis `/etc/httpd/conf/ssl.csr` (wenn Sie mit X arbeiten). Zeigen Sie den Inhalt von `server.csr` mit dem Befehl `cat server.csr` an. Heben Sie den Inhalt der Datei hervor, indem Sie mit der linken Maustaste klicken und ziehen. Klicken Sie mit der linken Maustaste auf das Textfeld auf der Web-Seite. Klicken Sie mit der mittleren Maustaste, um den hervorgehobenen Text einzufügen.

Stellen Sie sicher, dass Sie beim Kopieren und Einfügen keine zusätzlichen Leerstellen vor oder nach dem Text einfügen (einschließlich der Zeilen

`-----BEGIN CERTIFICATE REQUEST-----` und `-----END CERTIFICATE REQUEST-----`). Einige Zertifizierungsstellen weisen Anträge zurück, die zusätzliche Leerstellen enthalten.

Wenn Sie die Daten in den Antrag eingefügt haben, klicken Sie auf **Continue**.

5. Als nächsten Schritt müssen Sie nun den Berechtigungsnachweis (**Proof of Right**) erbringen. Sie müssen also VeriSign nachweisen, dass Ihre Organisation ordnungsgemäß erfasst ist. Zunächst versucht VeriSign, den angegebenen Namen der Organisation in der Datenbank von Dun & Bradstreet zu finden. Wurde der Name Ihrer Organisation in der Datenbank gefunden, wählen Sie ihn aus. Wählen Sie anderenfalls **My company and/or my company's correct address is not displayed in this list.** Klicken Sie auf **Continue**.

   Die einfachste Möglichkeit, die Identität Ihres Unternehmens zu beweisen, ist die D-U-N-S-Nummer. Es gibt jedoch auch andere Möglichkeiten, wenn Sie über keine solche Nummer verfügen oder diese Nummer nicht verwenden möchten. VeriSign gibt Anweisungen dazu, wie Sie die Identität Ihrer Organisation mit anderen Mitteln nachweisen können. Sie müssen den Nachweis bereithalten, bevor Sie ein Zertifikat beantragen. Sobald die erforderlichen Dokumente vorliegen, können Sie mit dem Vorgang fortfahren.

6. Nach Auswahl der korrekten Organisation aus der Datenbank von Dun & Bradstreet und nach Klicken auf **Continue** wird die nächste Seite **Confirm Domain Registration** aufgerufen. Auf dieser Seite überprüft VeriSign, ob die angegebene Domäne für Ihre Organisation registriert ist. Weitere Informationen zur Registrierung eines Domänennamens finden Sie im InterNIC FAQ unter http://www.internic.net/faq.html und/oder kann bei Ihrem Netzwerkadministrator erfragt werden.

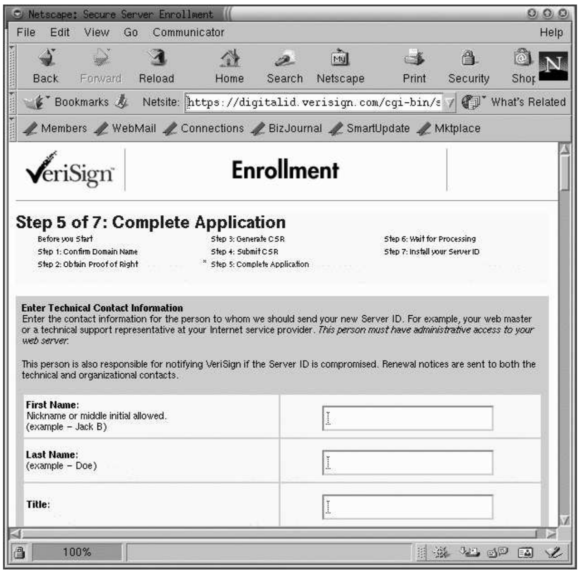
   Der verwendete Domänennamen muss für Ihre Organisation registriert sein. Der Name der in der **Domänenregistrierung aufgelisteten Organisation** sollte also dem Namen entsprechen, den Sie für die **Organisation eingegeben** haben. Anderenfalls müssen Sie einen neuen Antrag mit den korrekten Informationen erstellen.

   In den meisten Fällen werden die Namen übereinstimmen. Sie können das Feld **These organization names match** auswählen und dann auf **Continue** klicken.

7. Auf der nächsten Seite wird Ihnen mitgeteilt, dass Sie die erste Gültigkeitsüberprüfung von VeriSign bestanden haben. Klicken Sie auf **Continue**.

8. Die nächste Seite, **Complete Application**, wird angezeigt (siehe Abbildung 11–2, *Antrag auf ein VeriSign-Zertifikat*).

Abbildung 11–2 Antrag auf ein VeriSign-Zertifikat



Tragen Sie in den Bereich **Enter Technical Contact Information** alle Daten zum Administrator oder Webmaster Ihres Red Hat Linux Secure Web Server ein.

Geben Sie die entsprechenden Informationen zur Kontaktperson in Ihrer Organisation in den Abschnitt **Enter Organizational Contact Information** ein. Befolgen Sie dabei die Anweisungen von VeriSign.

Geben Sie in das Feld **Enter Billing Contact Information** die Daten des Mitarbeiters ein, der für die Abrechnung zuständig ist.

Geben Sie einen Abfrageausdruck und eine Erinnerungsfrage in die dafür vorgesehenen Bereiche "challenge phrase" und "reminder question" ein. Sie müssen den Abfrageausdruck kennen, wenn Sie Support-Leistungen von VeriSign in Anspruch nehmen möchten. Sie sollten ihn deshalb notieren und an einem sicheren Ort aufbewahren.

Geben Sie an, wie Sie das Zertifikat zahlen möchten.

Lesen Sie die Vereinbarungen für Unterzeichner im unteren Teil der Seite. Klicken Sie dann auf den Button **Continue**. Ihr Antrag wird übermittelt.

Wenn Sie den Antrag ausgefüllt haben und Ihre Daten und Zahlung bei VeriSign eingegangen sind, wird die Identität Ihrer Organisation bestätigt, und Ihr Zertifikat wird ausgestellt. Das genehmigte Zertifikat wird über E-Mail an die Kontaktpersonen im Unternehmen gesendet, die Sie angegeben haben.

Speichern Sie das Zertifikat von VeriSign in der Datei `server.crt` unter `/etc/httpd/conf/ssl.crt/`. Befolgen Sie die in Abschnitt 11.10, *Testen Ihres Zertifikats* beschriebenen Schritte, um Ihr Zertifikat zu installieren.

11.8.2 Erwerben eines Zertifikats von Thawte

So erwerben Sie ein Zertifikat von Thawte:

1. Rufen Sie in Ihrem Browser die Seite http://www.thawte.com/certs/server/request.html auf. Sie enthält einen Überblick über die notwendigen Schritte.

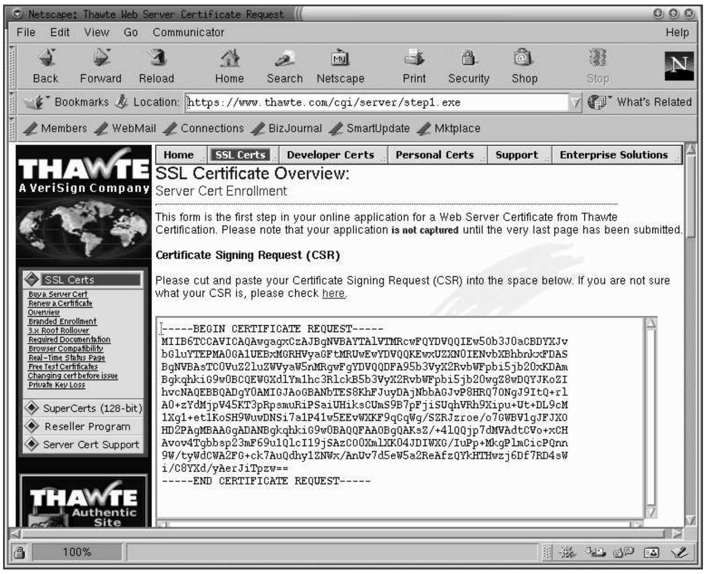
2. Zunächst einmal müssen Sie alle erforderlichen Dokumente zusammenstellen, wie unter Abschnitt 11.5.2, *Identitätsnachweise für Thawte* und auf der zuvor genannten Web-Seite beschrieben.

3. Generieren Sie dann einen Schlüssel und einen Signierungsantrag. Wenn Sie die Anweisungen unter Abschnitt 11.6, *Generieren von Schlüsseln* und Abschnitt 11.7, *Erzeugen von Zertifikatsanträgen für die Zertifizierungsstelle* befolgt haben, verfügen Sie bereits über einen Schlüssel (`/etc/httpd/conf/ssl.key/server.key`) und einen Antrag (`/etc/httpd/conf/ssl.csr/server.csr`). Wenn Sie Schlüssel und Zertifikatsantrag noch nicht erstellt haben, holen Sie dies nun nach, und befolgen Sie hierfür die in diesem Dokument aufgeführten Anweisungen.

4. Rufen Sie die Web-Seite von Thawte **Buy a Certificate** unter https://www.thawte.com/cgi/server/step1.exe auf. Wählen Sie **SSL Server Certificate** aus. Klicken Sie am unteren Rand der Seite auf den Button **Next**.

5. Die nächste Seite **Server Cert Enrollment** wird aufgerufen. Fügen Sie den Inhalt der Datei `/etc/httpd/conf/ssl.csr/server.csr` in das in Abbildung 11–3, *Antragsformular von Thawte* gezeigte Textfeld **Certificate Signing Request (CSR)** ein.

Abbildung 11–3 Antragsformular von Thawte

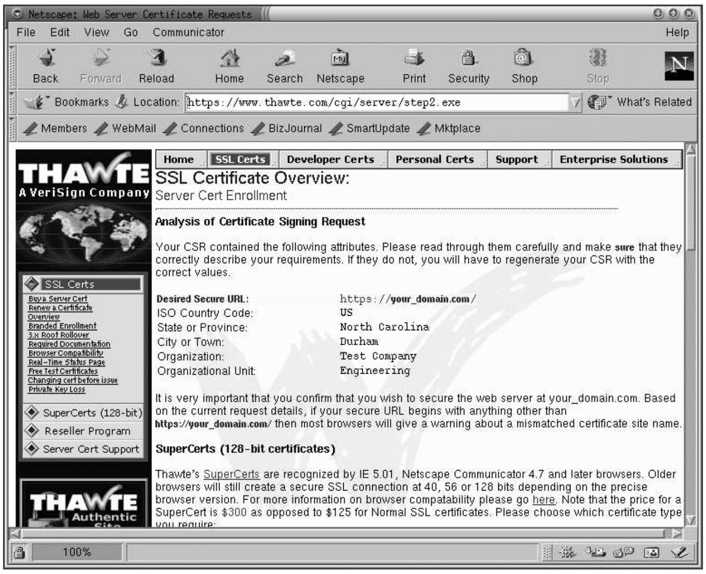


Um den Inhalt der Datei auszuschneiden und einzufügen, wechseln Sie zunächst mit dem Befehl `cd` in das Verzeichnis `/etc/httpd/conf/ssl.csr` (wenn Sie mit X arbeiten). Zeigen Sie den Inhalt von `server.csr` mit dem Befehl `cat server.csr` an. Markieren Sie den Inhalt der Datei, indem Sie mit der linken Maustaste klicken und ziehen. Klicken Sie mit der linken Maustaste auf das Textfeld auf der Web-Seite. Klicken Sie mit der mittleren Maustaste, um den hervorgehobenen Text einzufügen.

Stellen Sie sicher, dass Sie beim Kopieren und Einfügen keine zusätzlichen Leerstellen oder weißen Bereiche vor oder nach dem Text einfügen (einschließlich der Zeilen `-----BEGIN CERTIFICATE REQUEST-----` und `-----END CERTIFICATE REQUEST-----`). Einige Zertifizierungsstellen weisen Anträge zurück, die zusätzliche Leerstellen enthalten.

6. Wählen Sie aus dem Pulldown-Menü **Web Server Software** die Option **Red Hat Secure Server** aus.
7. Wählen Sie aus, in welcher Form die Zahlung für das Zertifikat erfolgen soll.
8. Klicken Sie am unteren Rand der Seite auf **Next.**
9. Auf der nächsten Seite wird eine Analyse des Zertifikatsantrags (**Analysis of Certificate Signing Request**) angezeigt (siehe Abbildung 11–4, *Analyse des Zertifikatsantrags*).

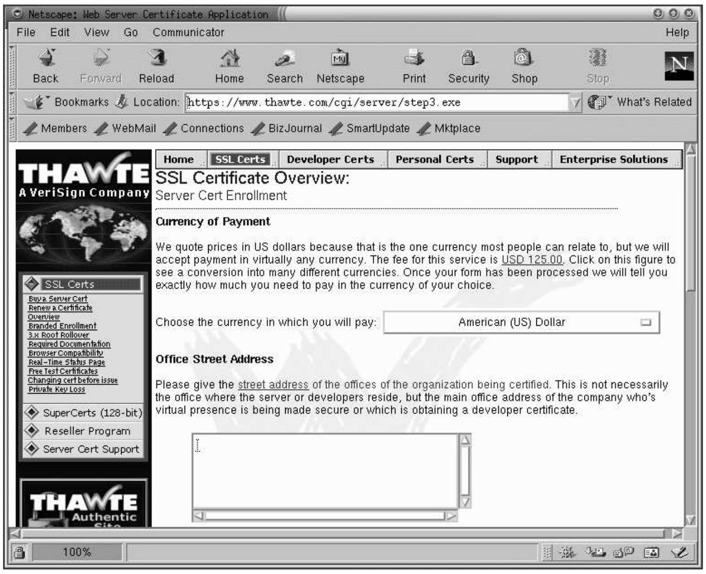
Abbildung 11–4 Analyse des Zertifikatsantrags



Weiter unten auf der Seite müssen Sie in **Background Information** eine Beschreibung Ihrer Organisation aus dem Pulldown-Menü auswählen oder eine eigene Beschreibung in das vorgesehene Textfeld eingeben.

10. Wenn Sie über eine D-U-N-S-Nummer verfügen, geben Sie diese in das dafür vorgesehene Textfeld **DUNS Number** ein.
11. Lesen Sie die Unterzeichnervereinbarungen von Thawte unter **Subscriber Agreement**. Tragen Sie die erforderlichen Daten zu den Personen Ihrer Organisation ein, die die Vereinbarungen autorisieren, wie unter Abschnitt 11.5.2, *Identitätsnachweise für Thawte* beschrieben.
12. Tragen Sie unter **Technical Contact/Webmaster** die Daten zum Administrator oder Webmaster Ihres Red Hat Linux Secure Web Server ein.
13. Klicken Sie am unteren Rand der Seite auf den Button **Next**.
14. Die nächste Seite, **Server Cert Enrollment**, ist die letzte Seite des Antragformulars (siehe Abbildung 11–5, *Zertifikatsantrag von Thawte*). Wählen Sie im ersten Pulldown-Menü die Währung aus, in der die Zahlung an Thawte erfolgt.

Abbildung 11–5 Zertifikatsantrag von Thawte



15. Geben Sie die Straße Ihrer Organisation in das Textfeld **Office Street Address** ein.
16. Geben Sie die Faxnummer in das Textfeld **Office Fax Number** ein.
17. Wählen Sie im Pulldown-Menü unter **Nearest Thawte Office** das Thawte-Büro aus, das Ihrer Organisation am nächsten liegt.
18. Geben Sie in das Textfeld unter **Privacy Protection Password** ein Passwort oder einen Abfrageausdruck ein. Nachdem Sie den Antrag ausgefüllt haben, können Sie seinen Status im Web überprüfen.
19. Klicken Sie am unteren Rand der Seite auf **Next**.
20. Auf der nächste Seite wird Ihnen mitgeteilt, dass der Antrag vollständig übermittelt wurde. Sie erhalten eine Referenznummer, unter der Sie den Status des Antrags im Web überwachen können.
21. Nach dem Erhalt der Dokumente und der Zahlung sendet Thawte das Zertifikat per E-Mail. Speichern Sie das erhaltene Zertifikat in die Datei

`/etc/httpd/conf/ssl.crt/server.crt`. Anweisungen zur Installation Ihres Zertifikats finden Sie unter Abschnitt 11.10, *Testen Ihres Zertifikats*.

11.9 Erstellen eines Zertifikats mit eigener Signatur

Sie können ein Zertifikat mit eigener Signatur erstellen. Bitte beachten Sie, dass dieses nicht dieselben Sicherheitsgarantien bietet wie ein Zertifikat, das von einer Zertifizierungsstelle gezeichnet ist. Weitere Informationen zu Zertifikaten finden Sie in Abschnitt 11.3, *Verschiedene Arten von Zertifikaten*.

Wenn Sie ein Zertifikat mit eigener Signatur erstellen möchten, erstellen Sie zunächst einen zufällig generierten Schlüssel. Befolgen Sie hierfür die Anweisungen unter Abschnitt 11.6, *Generieren von Schlüsseln*. Verwenden Sie dann den folgenden Befehl:

```
make testcert
```

Die folgende Ausgabe wird angezeigt, und Sie werden dazu aufgefordert, ein Passwort einzugeben (falls Sie keinen Schlüssel ohne Passwortschutz erstellen):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Nach Eingabe des Passworts (die entsprechende Eingabeaufforderung wird nicht ausgegeben, wenn die Passwortfunktion deaktiviert ist) müssen Sie weitere Informationen liefern. Die Ausgabe des Computers sowie die Eingaben entsprechen ungefähr der folgenden (Sie müssen die korrekten Daten zu Organisation und Host eingeben):

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter ’.’, the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Baden-Württemberg
Locality Name (eg, city) []:Heidelberg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Meine Firma GmbH
Organizational Unit Name (eg, section) []:Dokumentation
```

```
Common Name (eg, your name or your server’s hostname) []:Host.meineDomäne.com
Email Address []:meinemail@meineDomäne.de
```

Nach der korrekten Angabe aller Informationen wird ein Zertifikat mit eigener Signatur erstellt und in der Datei `/etc/httpd/conf/ssl.crt/server.crt` gespeichert. Sie müssen Ihren sicheren Server neu starten, nachdem das Zertifikat generiert wurde. Anweisungen zum Beenden und Starten des sicheren Web-Servers finden Sie in Abschnitt 11.11, *Starten und Beenden von Apache*.

11.10 Testen Ihres Zertifikats

Bei der Installation des sicheren Servers mit Red Hat Linux werden ein Zufallsschlüssel und ein allgemeines Zertifikat zu Testzwecken installiert. Mit diesem Zertifikat können Sie eine Verbindung zu Ihrem sicheren Server aufbauen. Das Zertifikat ist nur für Testzwecke geeignet. Für alle anderen Aufgaben müssen Sie ein Zertifikat von einer entsprechenden Stelle beantragen oder ein Zertifikat mit eigener Signatur generieren. Weitere Informationen zur den verschiedenen verfügbaren Zertifikaten finden Sie in Abschnitt 11.3, *Verschiedene Arten von Zertifikaten*.

Wenn Sie die Anweisungen in diesem Handbuch zur Erstellung oder zum Erwerb eines Zertifikats ausgeführt haben, verfügen Sie über die Datei `/etc/httpd/conf/ssl.key/server.key`, die Ihren Schlüssel enthält sowie über die Datei `/etc/httpd/conf/ssl.crt/server.crt` mit dem Test-Zertifikat. Wenn Schlüssel und Zertifikat in einem anderen Verzeichnis abgelegt sind, verschieben Sie diese in dieses Verzeichnis. Wenn Sie die Standardverzeichnisse oder Dateinamen für den Red Hat Linux Secure Web Server in den Konfigurationsdateien von Apache geändert haben, sollten Sie die beiden Dateien in das entsprechende geänderte Verzeichnis stellen.

Beenden und starten Sie Ihren Server wie in Abschnitt 11.11, *Starten und Beenden von Apache* beschrieben. Wenn Ihre Schlüsseldatei verschlüsselt ist, werden Sie aufgefordert, ein Passwort einzugeben. Geben Sie das Passwort ein. Ihr Server sollte jetzt hochfahren.

Rufen Sie mit Ihrem Web-Browser die Home Page Ihres Servers auf. Die URL zum Zugriff auf den Red Hat Linux Secure Web Server entspricht der folgenden:

```
https://Ihre_Domäne
```

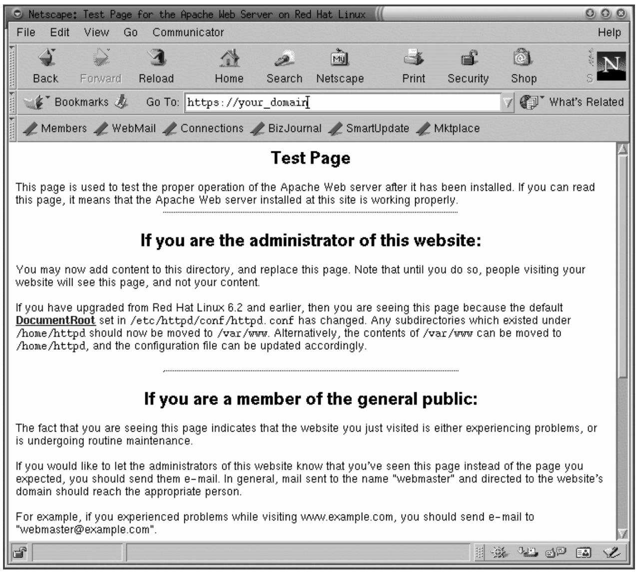
Bitte beachten

Beachten Sie, dass auf "http" ein "s" folgt. https: wird für sichere HTTP-Transaktionen verwendet. Sobald die Verbindung hergestellt ist, wird ein Dialogfeld eingeblendet. Es weist Sie an, Ihren Browser so zu konfigurieren, dass er das Test-Zertifikat akzeptiert.

Wenn Sie ein Zertifikat mit der Signatur einer bekannten Zertifizierungsstelle verwenden, akzeptiert der Browser das Zertifikat wahrscheinlich automatisch, ohne Sie um eine Bestätigung zu bitten und stellt die sichere Verbindung her. Ihr Browser erkennt ein Test-Zertifikat oder ein Zertifikat mit eigener Signatur nicht automatisch. Wenn Sie kein offiziell signiertes Zertifikat verwenden, befolgen Sie die Anweisungen Ihres Browsers, um sicherzustellen, dass das Zertifikat anerkannt wird. Akzeptieren Sie die Standardwerte, indem Sie auf **Next** klicken, bis alle Dialogfelder nacheinander geschlossen werden.

Wenn der Browser das Zertifikat anerkannt hat, zeigt der Red Hat Linux Secure Web Server eine Standard-Home-Page, die der in Abbildung 11–6, *Die Standard-Home-Page* entspricht.

Abbildung 11–6 Die Standard-Home-Page



11.11 Starten und Beenden von Apache

Während des Installationsvorgangs wurde ein Bourne-Shell-Skript namens `httpd` in das Verzeichnis `/etc/rc.d/init.d` installiert. Wenn Sie den Server manuell beenden oder starten möchten, führen Sie `httpd` aus, und geben Sie hierzu `stop` bzw. `start` als Argument ein.

Geben Sie den folgenden Befehl ein, um den Server zu starten:

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

Sie werden aufgefordert, Ihr Passwort einzugeben. Sobald Sie das Passwort eingegeben haben, startet der Server.

Geben Sie den folgenden Befehl ein, um den Server zu beenden:

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

Der Befehl `restart` bietet eine schnelle und einfache Möglichkeit, den Server zu beenden und neu zu starten. `restart` beendet den Server explizit und startet ihn dann erneut. Sie werden also aufgefordert, ein Passwort einzugeben. `restart` wird folgendermaßen eingegeben:

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

Wenn Sie die Datei `httpd.conf` bearbeitet haben, müssen Sie nicht unbedingt einen vollständigen Neustart durchführen. Sie können stattdessen auch den Befehl `reload` verwenden. Der Vorteil von `reload` liegt darin, dass Sie kein Passwort eingeben müssen. Anders als beim Neustart bleibt Ihr Passwort beim erneuten Laden im Cache gespeichert. `reload` wird folgendermaßen eingegeben:

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

Ihr Server (der Vorgang `httpd`) startet automatisch, wenn Ihr Rechner startet. Beachten Sie, dass Sie nach dem Start des Rechners aufgefordert werden, das Passwort für den sicheren Server einzugeben, wenn Sie Ihren Schlüssel mit Passwortschutz generiert haben.

11.12 Zugriff auf den sicheren Server

Um auf Ihren sicheren Server zuzugreifen, verwenden Sie die folgende URL:

https://Ihre_Domäne

Beachten Sie, dass die URLs, die auf den Red Hat Linux Secure Web Server zugreifen sollen, mit dem Protokollkennzeichner https: und nicht dem gängigeren Kennzeichner http: beginnen müssen. https: ist der Kennzeichner für gesicherte HTTP-Dateiübertragungen.

Auf einen ungesicherten Server kann mit der folgenden URL zugegriffen werden:

http://your_domain

Der Standardanschluss für gesicherte Web-Übertragungen ist Port 443. Der Standardanschluss für ungesicherte Web-Übertragungen ist Port 80. Der Red Hat Linux

Secure Web Server ist standardmäßig so konfiguriert, dass über beide Standardanschlüsse Verbindungen hergestellt werden können. Sie müssen daher die Port-Nummer in der URL nicht angegeben (sie wird automatisch angenommen).

Wenn Sie Ihren Server so konfigurieren, dass er einen nicht voreingestellten Port überwacht (d.h. nicht 80 oder 443) müssen Sie die Port-Nummer in allen URLs angeben, die auf den Server über diesen Port zugreifen.

Beispiel: Ein virtueller Host wird in einer nicht gesicherten Verbindung auf Port 12331 ausgeführt. Alle URLs, die auf diesen virtuellen Host zugreifen möchten, müssen diese Port-Nummer enthalten. Die folgende URL stellt eine Verbindung zu einem nicht gesicherten Web Server her, der Port 12331 überwacht:

```
http://your_domain:12331
```

Einige der in diesem Handbuch verwendeten Beispiel-URLs müssen eventuell geändert werden, je nachdem, ob Sie auf den Red Hat Linux Secure Web Server oder auf einen nicht gesicherten Web Server zugreifen. Die URLs in diesem Handbuch sind als allgemeine Beispiele gedacht, nicht als Anweisungen, die in allen Situationen verwendet werden können.

12 Konfigurieren des sicheren Servers

Die Standardkonfiguration von Red Hat Linux Secure Web Server ist normalerweise für die meisten Benutzer geeignet. Es kann sein, dass Sie nie auch nur eine einzige Konfigurationsanweisung von Apache ändern müssen. Wenn Sie jedoch an den Standardkonfigurationsoptionen Änderungen vornehmen möchten, müssen Sie einige der Optionen kennen und wissen, wo diese zu finden sind. In diesem Kapitel werden die Konfigurationsoptionen besprochen, die von Ihnen verwendet werden können.

Nach der Installation von Red Hat Linux Secure Web Server finden Sie die Dokumentation zum Apache Web-Server unter http://*ihre_domäne*/manual/, oder Sie können die Apache Dokumentation im Web einsehen unter http://www.apache.org/docs/. Die Apache Web-Server-Dokumentation enthält eine vollständige Liste und komplette Beschreibungen aller Konfigurationsoptionen von Apache. Um Ihnen die Übersicht zu erleichtern, enthält dieses Handbuch kurze Beschreibungen der Konfigurationsanleitungen für den Red Hat Linux Secure Web Server.

Beachten Sie bitte, dass die Standardkonfigurationsdatei Ihres Web-Servers sowohl Einträge für einen Web-Server ohne Verschlüsselung als auch für einen Web-Server mit Verschlüsselung (sicherer Web-Server) enthält. Der sichere Web-Server wird als virtueller Rechner ausgeführt, der in der Konfigurationsdatei `httpd.conf` konfiguriert wird. Weitere Informationen über virtuelle Rechner finden Sie unter Abschnitt 12.3, *Virtuelle Rechner verwenden*.

Bitte beachten

Es sind keine FrontPage-Erweiterungen enthalten, weil die Lizenz von Microsoft(TM) deren Lieferung in einem Produkt eines Drittanbieters verbietet.

12.1 Konfigurationsanweisungen in `httpd.conf`

Die Konfigurationsdatei für den Apache Web-Server ist `/etc/httpd/conf/httpd.conf`. Die Datei `httpd.conf` enthält ausführliche Kommentare und ist bis zu einem gewissen Grad selbsterklärend. Die Standardkonfiguration von Red Hat Linux Secure Web Server ist für die meisten Benutzer geeignet, und daher werden Sie wahrscheinlich keine Änderungen an den Anweisungen in `httpd.conf` vornehmen müssen. Vielleicht interessieren Sie sich aber für die wichtigsten Konfigurationsoptionen.

Die leeren Dateien `srm.conf` und `access.conf` befinden sich ebenfalls im Verzeichnis `/etc/httpd/conf`. `srm.conf` und `access.conf` wurden früher zusammen mit `httpd.conf` als Konfigurationsdateien für Apache verwendet.

Wenn Sie Ihren Red Hat Linux Secure Web Server konfigurieren müssen, ist lediglich die Datei `httpd.conf` zu editieren und anschließend der Red Hat Linux Secure Web Server neu zu laden oder anzuhalten und neu zu starten. Das Neuladen, Anhalten und Starten des Servers wird in Abschnitt 11.11, *Starten und Beenden von Apache* besprochen.

Vor dem Editieren von `httpd.conf` sollten Sie zuerst die Originaldatei kopieren und in `httpd.confold` (oder einen anderen von Ihnen gewählten Namen) umbenennen. Falls Sie beim Editieren der Konfigurationsdatei einen Fehler machen, steht Ihnen auf diese Weise eine Sicherheitskopie zur Verfügung, mit der Sie von vorn beginnen können.

Falls Sie einen Fehler machen und Ihr Red Hat Linux Secure Web Server nicht richtig funktioniert, sollten Sie zuerst die gerade editierte Datei `httpd.conf` auf Tippfehler überprüfen. Als Nächstes sollten Sie einen Blick auf die Fehlerprotokolldatei von Red Hat Linux Secure Web Server werfen (`/var/log/httpd/error_log`). Die Auswertung der Fehlerprotokolldatei ist, je nachdem, wie viel Erfahrung Sie damit haben, möglicherweise nicht ganz einfach. Wenn gerade ein Problem aufgetreten ist, sollten die letzten Einträge jedoch einige Hinweise liefern, was passiert ist.

Der nächste Abschnitt enthält kurze Beschreibungen der Anweisungen in `httpd.conf` in der Reihenfolge, wie sie in der Datei eingetragen sind. Diese Beschreibungen gehen nicht bis ins letzte Detail. Weitere Informationen finden Sie in der Apache Dokumentation im HTML-Format unter http://*ihre_domäne*/manual/ oder in der Apache Group Dokumentation unter http://www.apache.org/docs/. Weitere Informationen zu mod_ssl-Anweisungen finden Sie in der mitgelieferten Dokumentation im HTML-Format unter http://

ihre_domäne/manual/mod/mod_ssl/ bzw. im mod_ssl-*User Manual* (Benutzerhandbuch) unter http://www.modssl.org/docs/2.6/.

12.1.1 ServerType

Die Einstellung für `ServerType` kann entweder `inetd` oder `standalone` sein. Die Standardeinstellung für den Red Hat Linux Secure Web Server ist `ServerType standalone`.

`ServerType standalone` bedeutet, dass der Server einmal gestartet wird und dieser Server dann alle Verbindungen bearbeitet. `ServerType inetd` bedeutet, dass für jede HTTP-Verbindung eine neue Instanz des Servers gestartet wird. Jede Serverinstanz bearbeitet die Verbindung und wird beendet, wenn die Verbindung beendet wird. Wie Sie sich wahrscheinlich vorstellen können, ist die Verwendung von `inetd` sehr uneffektiv. Ein weiteres Problem ist, dass laut Informationen der Apache Group `inetd` möglicherweise nicht korrekt funktioniert. Da schließlich Red Hat Linux 7.0 `xinetd` verwendet, sind zusätzliche Konfigurationsarbeiten erforderlich, um über `xinetd` den Server zu starten. Aus diesen Gründen sollten Sie die Einstellung von `ServerType` von Red Hat Linux Secure Web Server auf `standalone` belassen.

12.1.2 ServerRoot

`ServerRoot` ist das oberste Verzeichnis, das die Serverdateien enthält. Sowohl der Server mit Verschlüsselung (sicherer Server) als auch der Server ohne Verschlüsselung sind auf die Verwendung von `/etc/httpd` als `ServerRoot` eingestellt.

12.1.3 LockFile

`LockFile` stellt den Pfad zur Sperrdatei ein, die verwendet wird, wenn der Apache Server entweder mit `USE_FCNTL_SERIALIZED_ACCEPT` oder mit `USE_FLOCK_SERIALIZED_ACCEPT` kompiliert wird. `LockFile` sollte normalerweise auf seinem Standardwert belassen werden.

12.1.4 PidFile

PidFile gibt die Datei an, in der der Server seine Prozess-ID (pid) ablegt. Der Red Hat Linux Secure Web Server ist so konfiguriert, dass er seine pid in /var/run/httpd.pid ablegt.

12.1.5 ScoreBoardFile

Im ScoreBoardFile werden interne Serverprozessinformationen gespeichert, die für die Kommunikation zwischen dem Eltern-Serverprozess und seinen Kind-Prozessen verwendet wird. Das ScoreBoardFile von Red Hat Linux Secure Web Server ist auf /var/run/httpd.scoreboard eingestellt.

12.1.6 ResourceConfig

Die Anweisung ResourceConfig veranlasst den Server, die nach ResourceConfig angegebene Datei nach weiteren Informationen zu durchsuchen. Die Anweisung ResourceConfig ist auskommentiert, weil Ihr Web-Server nur die Datei httpd.conf für Konfigurationsanweisungen verwendet.

12.1.7 AccessConfig

Die Anweisung AccessConfig veranlasst den Server, die nach AccessConfig angegebene Datei nach weiteren Anweisungen zu durchsuchen, nachdem die durch ResourceConfig angegebene Datei gelesen wurde. Die Anweisung AccessConfig ist auskommentiert, weil Ihr Web-Server nur die Datei httpd.conf für Konfigurationsanweisungen verwendet.

12.1.8 Timeout

Timeout gibt die Zeit in Sekunden an, die der Server während Kommunikationsverbindungen auf den Empfang und auf Übertragungen wartet. Insbesondere gibt Timeout an, wie lange der Server auf den Empfang einer GET-Anforderung wartet, wie lange er auf den Empfang von TCP-Paketen bei einer POST- oder GET-Anforderung wartet und wie lange er zwischen ACKs wartet, die als Antwort auf TCP-Pakete gesendet werden. Timeout ist auf 300 Sekunden eingestellt, eine für die meisten Situationen geeignete Einstellung.

12.1.9 KeepAlive

`KeepAlive` bestimmt, ob der Server wiederholte Verbindungen (d.h. mehr als eine Anforderung pro Verbindung) erlaubt. `KeepAlive` kann verwendet werden, um zu verhindern, dass ein einzelner Client zu viele der Serverressourcen verbraucht. Die Standardeinstellung für `KeepAlive` ist `on`, das heißt der Server erlaubt wiederholte Verbindungen. Sie können die Einstellung auf `off` ändern. Dadurch werden wiederholte Verbindungen deaktiviert. Eine ähnliche Möglichkeit, die Anfragen pro Verbindung zu begrenzen, finden Sie in Abschnitt 12.1.10, *MaxKeepAliveRequests* .

12.1.10 MaxKeepAliveRequests

Diese Anweisung gibt an, wie viele Anforderungen pro wiederholter Verbindung maximal erlaubt sind. Die Apache Group empfiehlt einen hohen Wert. Dadurch wird die Leistung des Servers verbessert. Die Standardeinstellung für `MaxKeepAliveRequests` ist `100`, eine für die meisten Situationen geeignete Einstellung.

12.1.11 KeepAliveTimeout

`KeepAliveTimeout` gibt die Anzahl der Sekunden an, die der Server auf eine nachfolgende Anforderung wartet, nachdem eine Anforderung bearbeitet wurde. Danach wird die Verbindung geschlossen. Nach dem Empfang einer Anforderung gilt stattdessen die Anweisung `Timeout`.

12.1.12 MinSpareServers und MaxSpareServers

Der Apache Web-Server passt sich dynamisch an die erkannte Last an, indem je nach Datenverkehr eine geeignete Anzahl von Reserve-Serverprozessen aufrechterhalten werden. Der Server prüft die Anzahl von Servern, die auf eine Anforderung warten, und beendet einige davon, wenn mehr als von `MaxSpareServers` angegeben vorhanden sind bzw. erzeugt einige neue, wenn weniger als in `MinSpareServers` angegeben vorhanden sind.

Die Standardeinstellung des Servers für `MinSpareServers` ist `5`. Die Standardeinstellung des Servers für `MaxSpareServers` ist `20`. Diese Standardeinstellungen sind für die meisten Situationen geeignet. `MinSpareServers` sollte nicht auf eine zu große Zahl eingestellt werden, weil dadurch selbst bei geringem Datenverkehr die Belastung des Servers hoch ist.

12.1.13 `StartServers`

`StartServers` bestimmt, wie viele Serverprozesse beim Start erzeugt werden. Da der Web-Server je nach Datenverkehrsaufkommen Serverprozesse dynamisch beendet bzw. erzeugt, muss dieser Parameter nicht verändert werden. Der Web-Server ist so konfiguriert, dass beim Start acht Serverprozesse erzeugt werden.

12.1.14 `MaxClients`

`MaxClients` gibt eine Obergrenze für die Gesamtzahl von Serverprozessen an (d.h. gleichzeitig verbundene Clients), die gleichzeitig ausgeführt werden können. Sie sollten `MaxClients` auf einer hohen Anzahl belassen (die Standardeinstellung des Servers ist 150), weil kein anderer Client eine Verbindung aufbauen darf, sobald diese Anzahl von gleichzeitig verbundenen Clients erreicht ist. Wenn `MaxClients` auf eine Anzahl eingestellt werden soll, die größer als 256 ist, muss Apache neu kompiliert werden. Der Hauptgrund für die Existenz von `MaxClients` ist, dass damit verhindert werden soll, dass Ihr Betriebssystem durch einen überlasteten Web-Server zum Absturz gebracht wird.

12.1.15 `MaxRequestsPerChild`

`MaxRequestsPerChild` bestimmt die Gesamtanzahl der Anforderungen, die ein Kind-Serverprozess bearbeitet, bevor er beendet wird. Der Hauptgrund für die Einstellung von `MaxRequestsPerChild` ist, dass lang andauernde, durch Prozesse verursachte Speicherlecks vermieden werden sollen. Die Standardeinstellung für `MaxRequestsPerChild` für den Server ist `100`.

12.1.16 `Listen`

Der Befehl `Listen` kennzeichnet den Port, an dem der Red Hat Linux Secure Web Server ankommende Anforderungen annimmt. Der Red Hat Linux Secure Web Server ist so konfiguriert, dass auf Port 80 auf unverschlüsselte Web-Kommunikation und (in Virtual Host-Tags, die den sicheren Server definieren) auf Port 443 auf sichere Web-Kommunikation gewartet wird.

Wenn Sie Apache so konfigurieren, dass an einem Port kleiner als 1024 gewartet wird, muss der Prozess `httpd` als Root starten. Für Port 1024 und darüber kann `httpd` als normaler Benutzer starten.

`Listen` kann auch zur Angabe spezieller IP-Adressen verwendet werden, über die der Server Verbindungen annimmt.

12.1.17 BindAddress

`BindAddress` ist eine Möglichkeit, um anzugeben, an welcher IP-Adresse der Server Verbindungen annimmt. Wenn Sie diese Funktion benötigen, sollten Sie stattdessen `Listen` verwenden. `BindAddress` wird vom Web-Server nicht verwendet. In der Datei `httpd.conf` ist es standardmäßig auskommentiert.

12.1.18 LoadModule

`LoadModule` wird in Dynamic Shared Object (DSO)-Modulen zum Laden verwendet. Weitere Informationen zur DSO-Unterstützung von Red Hat Linux Secure Web Server einschließlich der genauen Verwendung der Anweisung `LoadModule` finden Sie in Abschnitt 12.2, *Hinzufügen von Modulen zu Ihrem Server*. Beachten Sie, dass die Reihenfolge der Module wichtig ist. Sie sollten daher die Reihenfolge nicht verändern.

12.1.19 IfDefine

Die Tags `<IfDefine>` und `</IfDefine>` umschließen Konfigurationsanweisungen, die ausgeführt werden, wenn sich für die Bedingung im Tag `<IfDefine>` die Aussage wahr ergibt. Die Anweisungen werden nicht ausgeführt, wenn sich die Aussage falsch ergibt.

Die Bedingung in den Tags `<IfDefine>` ist eine Parameterbezeichnung (z.B. `HAVE_PERL`). Wenn der Parameter definiert ist (d.h. er wurde beim Start des Servers als Argument des Startbefehls angegeben), ist die Aussage wahr. In diesem Fall ist die Bedingung wahr, wenn der Red Hat Linux Secure Web Server gestartet ist, und die Anweisungen in den Tags `IfDefine` werden ausgeführt.

Standardmäßig umschließen die Tags `<IfDefine HAVE_SSL>` die virtuellen Rechnertags für den sicheren Server. `<IfDefine HAVE_SSL>`-Tags umschließen außerdem auch die Anweisungen `LoadModule` und `AddModule` für das `ssl_module`.

12.1.20 ClearModuleList

Die Anweisung `ClearModuleList` steht direkt vor der langen Liste mit `AddModule` -Anweisungen. `ClearModuleList` löscht die in den Server integrierte Liste der aktiven Module. Die Liste von `AddModule`-Anweisungen erstellt dann direkt nach `ClearModuleList` die Liste neu.

12.1.21 AddModule

`AddModule` ist die Anweisung zur Erstellung einer vollständigen Liste mit allen verfügbaren Modulen. Sie müssen die Anweisung `AddModule` verwenden, wenn Sie Ihr eigenes Modul als DSO einfügen. Weitere Informationen zur Verwendung von `AddModule` für die DSO-Unterstützung finden Sie in Abschnitt 12.2, *Hinzufügen von Modulen zu Ihrem Server*.

12.1.22 ExtendedStatus

Die Anweisung `ExtendedStatus` bestimmt, ob Apache beim Aufruf des `server-status`-Handlers Statusinformationen in einer Kurzfassung (`off`) oder einer detaillierten Fassung (`on`) erstellt. `Server-status` wird über `Location`-Tags aufgerufen. Weitere Informationen zum Aufruf von `server-status` finden Sie in Abschnitt 12.1.30, *`Location`* .

12.1.23 Port

Normalerweise definiert `Port` den Port, an dem der Server auf Anforderungen wartet. Der Red Hat Linux Secure Web Server wartet jedoch standardmäßig an mehr als einem Port, da die Anweisung `Listen` ebenfalls verwendet wird. Wenn `Listen`-Anweisungen aktiv sind, wartet der Server an allen diesen Ports. Weitere Informationen zu `Listen` finden Sie in der Beschreibung der Anweisung `Listen`.

Der Befehl `Port` wird auch dazu verwendet, die Portnummer anzugeben, die zur Erstellung des kanonischen Namens für Ihren Server verwendet wird. Weitere Informationen über den kanonischen Namen Ihres Servers finden Sie in Abschnitt 12.1.40, *`UseCanonicalName`* .

12.1.24 `User`

Die Anweisung `User` definiert die Benutzer-ID, die vom Server zur Beantwortung von Anforderungen verwendet wird. Die `User`-Einstellung bestimmt die Zugriffsrechte des Servers. Alle Dateien, auf die dieser Benutzer nicht zugreifen darf, sind für die Besucher Ihrer Website ebenfalls nicht zugänglich. Die Standardeinstellung für `User` ist `apache`.

Der in `User` eingetragene Benutzer sollte nur Zugriffsrechte auf solche Dateien haben, die für die Außenwelt sichtbar sein sollen. Der in `User` eingetragene Benutzer ist auch der Eigentümer aller vom Server erzeugten CGI-Prozesse. Der in `User` eingetragene Benutzer sollte nur Code ausführen dürfen, der zur Beantwortung von HTTP-Anforderungen vorgesehen ist.

Bitte beachten

Geben Sie in `User` als Benutzer niemals root an, es sei denn, Sie wissen genau, was Sie tun. Root als Eintrag für `User` würde riesige Sicherheitslöcher für Ihren Red Hat Linux Secure Web Server bedeuten.

Der Eltern-Prozess `httpd` wird im Normalbetrieb zuerst als Root ausgeführt, wird dann aber sofort zum Benutzer apache weitergegeben. Der Server muss als Root starten, weil die Bindung an einen Port unter 1024 erforderlich ist (der Standardport für sichere Web-Kommunikation ist der Port 443, der Standardport für unverschlüsselte Web-Kommunikation ist der Port 80). Ports unter 1024 sind für die Verwendung durch das System reserviert und können daher nur von Root verwendet werden. Sobald sich der Server jedoch an den Port gebunden hat, wird der Prozess an den in `User` eingetragenen Benutzer weitergegeben, bevor er Verbindungsanforderungen annimmt.

12.1.25 Group

Die Anweisung `Group` ähnelt der Anweisung `User`. `Group` legt die Gruppe fest, unter der der Server Anforderungen beantwortet. Die Standardeinstellung für `Group` ist ebenfalls `apache`.

12.1.26 ServerAdmin

`ServerAdmin` sollte auf die E-Mail-Adresse des Red Hat Linux Secure Web Server - Administrators eingestellt sein. Diese E-Mail-Adresse wird in Fehlermeldungen auf vom Server erstellten Web-Seiten angezeigt, damit die Benutzer dem Serveradministrator ein Problem per E-Mail melden können. `ServerAdmin` ist standardmäßig auf `root@localhost` eingestellt.

Meistens ist es am günstigsten, bei `ServerAdmin webmaster@ihre_domäne.com` einzutragen. Richten Sie dann in `/etc/aliases` einen Alias `webmaster` ein, der auf den für den Web-Server Verantwortlichen zeigt. Führen Sie schließlich `/usr/bin/newaliases` aus, um die neuen Aliase hinzuzufügen.

12.1.27 ServerName

Mit `ServerName` können Sie einen Rechnernamen für Ihren Server angeben, der sich vom wirklichen Namen Ihres Rechners unterscheidet. Zum Beispiel können Sie so den Namen www.ihre_domäne.com einrichten, obwohl der wirkliche Name Ihres Servers foo.ihre_domäne.com ist. Beachten Sie, dass `ServerName` einen gültigen Domain Name Service (DNS)-Namen enthalten muss, den Sie auch tatsächlich verwenden dürfen (also nicht einfach etwas ausdenken).

Wenn Sie in `ServerName` einen Servernamen angeben, muss die entsprechende Zuordnung von IP-Adresse und Servername in Ihrer `/etc/hosts`-Datei enthalten sein.

12.1.28 DocumentRoot

`DocumentRoot` enthält das Verzeichnis, das die meisten HTML-Dateien enthält, die der Server auf Anforderung überträgt. Der Standardeintrag für `DocumentRoot` ist sowohl für den unverschlüsselten als auch für den sicheren Web-Server

`/var/www/html`. Zum Beispiel könnte der Server eine Anforderung für folgendes Dokument empfangen:

```
http://ihre_domäne/foo.html
```

Der Server sucht die folgende Datei im Standardverzeichnis:

```
/var/www/html/foo.html
```

Wenn Sie den Eintrag in `DocumentRoot` so ändern möchten, dass es nicht vom sicheren und vom unverschlüsselten Web-Server gemeinsam benutzt wird, finden Sie in Abschnitt 12.3, *Virtuelle Rechner verwenden* entsprechende Informationen.

12.1.29 Directory

Die Tags `<Directory /path/to/directory>` und `</Directory>` werden verwendet, um eine Gruppe von Konfigurationsanweisungen zu umschließen, die sich nur auf dieses Verzeichnis und alle seine Unterverzeichnisse beziehen sollen. Alle Anweisungen, die auf ein Verzeichnis anwendbar sind, können innerhalb der `<Directory>` -Tags verwendet werden. `<File>`-Tags können auf die gleiche Weise verwendet werden, allerdings für eine spezielle Datei.

In der Standardeinstellung werden für das Root-Verzeichnis mit den Anweisungen `Options` (siehe Abschnitt 12.1.31, *`Options`*) und `AllowOverride` (siehe Abschnitt 12.1.32, *`AllowOverride`*) sehr restriktive Parameter vorgegeben. Bei dieser Konfiguration müssen für jedes Verzeichnis die Einstellungen explizit vergeben werden, wenn weniger restriktive Einstellungen erforderlich sind.

Mit `Location`-Tags werden für `DocumentRoot` (auch mit `"/"` bezeichnet) weniger restriktive Parameter definiert, damit HTTP-Anforderungen in diesem Verzeichnis bearbeitet werden können.

Das Verzeichnis `cgi-bin` wird mit der Option `ExecCGI` für die Ausführung von CGI-Skripten eingerichtet. Wenn die Ausführung von CGI-Skripten in anderen Verzeichnissen erforderlich ist, müssen Sie `ExecCGI` entsprechend für dieses Verzeichnis einstellen. Wenn Ihr Verzeichnis `cgi-bin` zum Beispiel `/var/www/cgi-bin` ist, Sie aber CGI-Skripten im Verzeichnis `/home/mein_cgi_verzeichnis` ausführen möchten, können Sie in Ihrer

Datei httpd.conf eine ExecCGI-Anweisung mit einem Satz von Directory-Anweisungen hinzufügen:

```
<Directory /home/mein_cgi_verzeichnis>
    Options +ExecCGI
</Directory>
```

Um die Ausführung von CGI-Skripten in /home/my_cgi_directory zuzulassen, sind neben der Einstellung von ExecCGI noch einige zusätzliche Schritte nötig. Für die Anweisung AddHandler müssen die Kommentare entfernt werden, damit Dateien mit der Endung .cgi als CGI-Skripten erkannt werden können. Anleitungen zur Einstellung von AddHandler finden Sie in Abschnitt 12.1.66, *AddHandler* . Die Zugriffsberechtigungen für CGI-Skripten und den gesamten Pfad zu den Skripten müssen auf 0755 eingestellt sein. Schließlich müssen der Eigentümer des Skripts und der Eigentümer des Verzeichnisses derselbe Benutzer sein.

12.1.30 Location

<Location>- und </Location>-Tags ermöglichen die Angabe von Zugangsberechtigungen auf URL-Basis.

Eine Möglichkeit, Location-Tags zu verwenden, ist die Konfiguration von Options und die Bereitstellung weiterer Konfigurationsrichtlinien für DocumentRoot. Diese Konfigurationsanweisungen werden innerhalb der Tags <Location "/"> und </Location> angegeben und sind erforderlich, um den Zugriff auf die Dokumente in DocumentRoot zu ermöglichen.

Eine weitere Möglichkeit, Location-Tags zu verwenden, ist die Angabe in IfModule mod_perl.c-Tags. Diese Konfigurationsanweisungen sind aktiv, wenn das DSO mod_perl.so geladen ist. Weitere Informationen zum Hinzufügen von Modulen zu Apache finden Sie in Abschnitt 12.2, *Hinzufügen von Modulen zu Ihrem Server*.

In den Location-Tags wird das Verzeichnis /var/www/perl (ein Alias für /perl) als das Verzeichnis angegeben, von dem Perl-Skripten bereitgestellt werden. Wenn ein Dokument mit einer URL mit /perl im Pfad angefordert wird, sucht der Web-Server in /var/www/perl/ nach dem entsprechenden Perl-Skript.

Mehrere andere `<Location>`-Optionen in der Datei `httpd.conf` sind auskommentiert. Wenn Sie deren Funktionen nutzen wollen, müssen Sie für den entsprechenden Anweisungsabschnitt die Kommentare entfernen.

Direkt nach den gerade besprochenen Perl-Anweisungen folgt in der Datei `httpd.conf` ein Abschnitt mit Anweisungen zur Aktivierung von HTTP PUT (z.B. für die Publizieren-Funktion von Netscape Gold, über die Web-Seiten auf einem Web-Server veröffentlicht werden können). Wenn Sie HTTP PUT zulassen möchten, müssen Sie für diesen gesamten Abschnitt die Kommentare entfernen:

```
#LoadModule put_module          modules/mod_put.so
#AddModule mod_put.c
#
#Alias /upload /tmp
#<Location /upload>
#    EnablePut On
#    AuthType Basic
#    AuthName Temporary
#    AuthUserFile /etc/httpd/conf/passwd
#    EnableDelete Off
#    umask 007
#    <Limit PUT>
#       require valid-user
#    </Limit>
#</Location>
```

Wenn Sie zulassen möchten, dass Benutzer von Ihrer Domäne aus Serverstatusberichte einsehen können, sollten Sie für den nächsten Abschnitt mit Anweisungen die Kommentare entfernen:

```
#<Location /server-status>
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .ihre_domäne.com
#</Location>
```

Dabei muss `.ihre_domäne.com` durch den Namen Ihrer Second Level-Domäne ersetzt werden.

Wenn Sie Serverkonfigurationsberichte (einschließlich installierter Module und Konfigurationsanweisungen) für Anforderungen aus Ihrer Domäne bereitstellen möchten, müssen für die folgenden Zeilen die Kommentare entfernt werden:

```
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>
```

Auch hier muss `.your_domain.com` entsprechend angegeben werden.

Im nächsten Abschnitt mit Anweisungen werden `Location`-Tags verwendet, um den Zugriff auf die Dokumentation in `/usr/share/doc` zu erlauben (z.B. mit einer URL wie http://*ihre_domäne*/doc/beliebig.html). Diese Anweisungen erlauben nur Anforderungen vom lokalen Rechner den Zugriff.

Eine weitere Möglichkeit, `Location`-Tags zu verwenden, ist ein auskommentierter Abschnitt, der Angriffe auf Ihren Web-Server aufspüren soll, die einen alten Bug aus der Zeit vor Apache 1.1 ausnutzen. Wenn Sie diese Anforderungen verfolgen wollen, entfernen Sie die Kommentare für die folgenden Zeilen:

```
#<Location /cgi-bin/phf*>
#    Deny from all
#    ErrorDocument 403 http://phf.apache.org/phf_abuse_log.cgi
#</Location>
```

Wenn für diese Zeilen die Kommentare entfernt werden, leitet Ihr Web-Server alle Anfragen, die mit `/cgi-bin/phf*` enden, zu einem CGI-Protokollierungsskript um, das von der Apache Group ausgeführt wird.

12.1.31 Options

Die Anweisung `Options` bestimmt, welche Serverfunktionen in einem bestimmten Verzeichnis verfügbar sind. Zum Beispiel ist für `Options` entsprechend den restriktiven Parametern für das Root-Verzeichnis lediglich `FollowSymLinks` angegeben. Es sind keine Funktionen aktiviert, außer dass der Server im Root-Verzeichnis symbolischen Links folgen darf.

In Ihrem Verzeichnis `DocumentRoot` ist `Options` so konfiguriert, dass `Indexes`, `Includes` und `FollowSymLinks` enthalten sind. `Indexes` erlaubt dem Server, eine Verzeichnisliste für ein Verzeichnis zu erstellen, wenn kein `DirectoryIndex` (d.h. `index.html usw.`) angegeben wird. `Includes` bedeutet, dass Server-Side Includes erlaubt sind. `FollowSymLinks` erlaubt dem Server, in diesem Verzeichnis symbolischen Links zu folgen.

Zusätzlich müssen innerhalb von Anweisungen für virtuelle Rechner `Options`-Anweisungen enthalten sein, damit Ihre virtuellen Rechner diese `Options` erkennen können.

Zum Beispiel sind serverseitige Includes innerhalb des Verzeichnisses `/var/www/html` bereits aktiviert, weil im Anweisungsabschnitt `Location "/"` die Zeile `Options Includes` enthalten ist. Wenn Sie jedoch erreichen möchten, dass ein virtueller Rechner erkennt, dass serverseitige Includes innerhalb von `/var/www/html` erlaubt sind, muss ein Abschnitt wie der folgende innerhalb der Tags für den virtuellen Rechner hinzugefügt werden:

```
<Directory /var/www/html>
Options Includes
</Directory>
```

12.1.32 `AllowOverride`

Die Anweisung `AllowOverride` bestimmt, ob `Options` durch Deklarationen in einer `.htaccess`-Datei überschrieben werden können. Standardmäßig sind sowohl das Root-Verzeichnis als auch `DocumentRoot` so konfiguriert, dass ein Überschreiben durch `.htaccess` nicht möglich ist.

12.1.33 `Order`

Die Anweisung `Order` bestimmt die Reihenfolge, in der die Anweisungen `allow` und `deny` ausgewertet werden. Der Server ist so konfiguriert, dass für Ihr `DocumentRoot`-Verzeichnis die `Allow`-Anweisungen vor den `deny`-Anweisungen ausgewertet werden.

12.1.34 `Allow`

`Allow` gibt an, welcher Anforderer auf ein bestimmtes Verzeichnis zugreifen darf. Der Anforderer kann sein: `all`, ein Domänenname, eine IP-Adresse, ein Teil einer IP-Adresse, ein Netzwerk/Netzmasken-Paar usw. Ihr `DocumentRoot`-Verzeichnis ist so konfiguriert, dass durch `Allow` Anforderungen von `all` (d.h. allen Anforderern) erlaubt sind.

12.1.35 `deny`

`Deny` funktioniert genauso wie `allow`, wobei angegeben wird, wem der Zugriff nicht erlaubt ist. In Ihrer `DocumentRoot` sind keine `deny`-Anweisungen enthalten.

12.1.36 `UserDir`

`UserDir` ist der Name des Unterverzeichnisses innerhalb eines Home-Verzeichnisses jedes Benutzers, wo private HTML-Seiten abgelegt werden können, die vom Web-Server bereitgestellt werden sollen. Die Standardeinstellung für das Unterverzeichnis ist `public_html`. Zum Beispiel könnte der Server die folgende Anforderung erhalten:

`http://`*`ihre_domäne/~benutzername/`*`foo.html`

Der Server sucht daraufhin die Datei:

```
/home/benutzername/public_html/foo.html
```

Im obigen Beispiel ist `/home/username` das Home-Verzeichnis des Benutzers. (Beachten Sie bitte, dass der Standardpfad zu den Home-Verzeichnissen von Benutzern auf Ihrem System abweichen kann.)

Überprüfen Sie, ob die Zugriffsberechtigungen für die Home-Verzeichnisse der Benutzer richtig eingestellt sind. Die richtige Einstellung ist 0755. Für die `public_html`-Verzeichnisse der Benutzer müssen die read (r)- und execute (x)-Bits eingestellt sein (0755 ist ausreichend). Dateien, die im `public_html`-Verzeichnis der Benutzer zum Abruf angeboten werden, müssen mindestens die Berechtigung 0644 haben.

12.1.37 `DirectoryIndex`

Der `DirectoryIndex` ist die Standardseite, die vom Server geliefert wird, wenn ein Benutzer durch Angabe von / am Ende eines Verzeichnisnamens einen Index eines Verzeichnisses anfordert.

Wenn ein Benutzer zum Beispiel die Seite http://*ihre_domäne*/*dieses_verzeichnis*/ anfordert, wird entweder die `DirectoryIndex` -Seite (falls vorhanden) oder eine vom Server erstellte Verzeichnisliste angezeigt. Die Standardeinstellung für den `DirectoryIndex` ist `index.html index.htm index.shtml index.cgi`. Der Server sucht nach diesen Dateien und gibt die Datei aus, die zuerst gefunden wird. Wenn keine dieser Dateien gefunden wird und `Options Indexes` für dieses Verzeichnis aktiviert ist, erstellt und überträgt der Server eine Liste im HTML-Format, die die Unterverzeichnisse und Dateien im Verzeichnis enthält.

12.1.38 `AccessFileName`

`AccessFileName` bestimmt die Datei, die vom Server zur Speicherung von Zugriffskontrollinformationen in jedem Verzeichnis verwendet werden soll. Standardmäßig ist Ihr Web-Server so konfiguriert, dass für die Speicherung von Zugriffskontrollinformationen die Datei `.htaccess` verwendet wird (falls vorhanden).

Unmittelbar nach der Anweisung `AccessFileName` wird durch eine Reihe von `Files`-Tags die Zugangskontrolle zu allen Dateien geregelt, die mit `.ht` beginnen. Diese Anweisungen verwehren aus Sicherheitsgründen den Zugriff auf alle `.htaccess`-Dateien (bzw. andere Dateien, die mit `.ht` beginnen).

12.1.39 `CacheNegotiatedDocs`

Standardmäßig fordert Ihr Red Hat Linux Secure Web Server Proxyserver auf, keine Dokumente im Cache zu halten, die auf der Grundlage des Inhalts übertragen wurden (d.h. sie können nach einer gewissen Zeit oder aufgrund der Eingabe des Anforderers geändert werden). Wenn die Kommentare für `CacheNegotiatedDocs` entfernt werden, wird diese Funktion deaktiviert, und Proxyserver können von diesem Zeitpunkt an Dokumente im Cache halten.

12.1.40 UseCanonicalName

UseCanonicalName ist standardmäßig auf on eingestellt. UseCanonicalName ermöglicht dem Server, mit ServerName und Port eine URL zu erstellen, die den Server selbst referenziert. Der Server verwendet diese URL, wenn er sich aufgrund von Anforderungen selbst referenziert. Wenn UseCanonicalName auf off eingestellt wird, verwendet der Server stattdessen den Wert, der in der Anforderung des Clients enthalten ist, um sich selbst zu referenzieren.

12.1.41 TypesConfig

TypesConfig gibt die Datei an, die die Standardliste der MIME Type-Zuordnungen definiert (Dateinamenerweiterungen für Inhaltstypen). Die Standarddatei für TypesConfig ist /etc/mime.types. Es wird empfohlen, zum Hinzufügen von MIME Type-Zuordnungen die Datei /etc/mime.types nicht zu editieren, sondern die Anweisung AddType zu verwenden.

12.1.42 DefaultType

DefaultType definiert einen Standardinhaltstyp, den der Web-Server für Dokumente verwendet, deren MIME Types nicht bestimmt werden können. Die Standardeinstellung für Ihren Web-Server ist, dass bei Dateien mit einem nicht genau zu bestimmenden Inhaltstyp ein Standardtext-Inhaltstyp angenommen wird.

12.1.43 IfModule

<IfModule> und </IfModule>-Tags umschließen Anweisungen, die Bedingungen enthalten. Die in den IfModule-Tags enthaltenen Anweisungen werden verarbeitet, wenn eine der zwei folgenden Bedingungen erfüllt ist. Die Anweisungen werden verarbeitet, wenn das im ersten <IfModule>-Tag enthaltene Modul in den Apache Server einkompiliert ist. Wenn ein "!" (Ausrufezeichen) vor dem Modulnamen steht, werden sie nur verarbeitet, wenn das Modul im ersten <IfModule>-Tag *nicht* einkompiliert ist.

Die Datei mod_mime_magic.c ist in diesen IfModule-Tags enthalten. Das Modul mod_mime_magic ist mit dem file-Befehl in UNIX vergleichbar, der einige

Bytes des Inhalts einer Datei untersucht und "Magic Numbers" sowie weitere Hinweise verwendet, um den MIME Type der Datei zu bestimmen.

Wenn das Modul mod_mime_magic in Apache einkompiliert ist, wird dem Modul mod_mime_magic über diese `IfModule`-Tags mitgeteilt, wo sich die Hinweisdatei befindet: `share/magic` in diesem Fall.

Das Modul mod_mime_magic ist nicht standardmäßig einkompiliert. Wenn Sie das Modul verwenden möchten, finden Sie in Abschnitt 12.2, *Hinzufügen von Modulen zu Ihrem Server* Hinweise zum Hinzufügen von Modulen zu Ihrem Server.

12.1.44 `HostnameLookups`

`HostnameLookups` kann auf `on` oder `off` eingestellt werden. Wenn Sie `HostnameLookups` erlauben (durch Einstellung auf `on`), wird vom Server die IP-Adresse für jede Verbindung, die ein Dokument von Ihrem Web-Server anfordert, automatisch aufgelöst. Die Auflösung der IP-Adresse bedeutet, dass Ihr Server mindestens eine Verbindung zum DNS herstellt, um den zu einer IP-Adresse gehörenden Rechnernamen zu bestimmen.

Im Allgemeinen sollten Sie die Einstellung für `HostnameLookups` auf `off` belassen, da die DNS-Anforderungen Ihren Server zusätzlich belasten und ihn unter Umständen langsamer machen. Wenn Ihr Server ausgelastet ist, kann die Wirkung der Einstellung von `HostnameLookups` ziemlich deutlich spürbar sein.

`HostnameLookups` ist auch für das Internet insgesamt von Bedeutung. Die einzelnen Verbindungen für das Heraussuchen des Rechnernamens addieren sich. Deshalb ist es sowohl für Ihren Server als auch für das Internet insgesamt von Vorteil, die Einstellung von `HostnameLookups` auf `off` zu belassen.

12.1.45 `ErrorLog`

`ErrorLog` bestimmt die Datei, in der Serverfehler protokolliert werden. Wie durch den Namen der Anweisung angedeutet, ist die Fehlerprotokolldatei für Ihren Web-Server `/var/log/httpd/error_log`.

Wenn Ihr Web-Server fehlerhaft oder überhaupt nicht arbeitet und Sie sich nicht sicher sind, warum dies auftritt, sollten Sie zuerst das Fehlerprotokoll überprüfen.

12.1.46 LogLevel

`LogLevel` legt fest, wie ausführlich die Fehlermeldungen im Fehlerprotokoll dargestellt werden. `LogLevel` kann auf `emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` oder `debug` eingestellt werden (von der kürzesten bis zur ausführlichsten Darstellung). Das `LogLevel` für Ihren Red Hat Linux Secure Web Server ist auf `warn` eingestellt (eine gute Mitte).

12.1.47 LogFormat

Die `LogFormat`-Anweisungen in Ihrer `httpd.conf`-Datei legen ein Format für die Meldungen in Ihrem Zugriffsprotokoll fest. Dieses Format kann Ihr Zugriffsprotokoll hoffentlich besser lesbar machen.

12.1.48 CustomLog

`CustomLog` bestimmt die Protokolldatei und das Protokolldateiformat. In der Standardkonfiguration Ihres Red Hat Linux Secure Web Server bestimmt `CustomLog` die Protokolldatei, in der die Zugriffe auf Ihren Web-Server protokolliert werden: `/var/log/httpd/access_log`. Wenn Sie für Ihren Web-Server Server-Leistungsstatistiken auf der Basis der Zugriffe erstellen möchten, muss Ihnen bekannt sein, wo diese Datei abgelegt ist.

`CustomLog` stellt außerdem das Protokolldateiformat auf common ein. Das Protokolldateiformat common sieht folgendermaßen aus:

```
remotehost rfc931 authuser [date] "request" status bytes
```

remotehost

Enthält den Namen des Remote-Rechners. Wenn der Rechnername über DNS nicht verfügbar ist, oder wenn `HostnameLookups` auf `Off` eingestellt ist, ist *`remotehost`* die IP-Adresse des Remote-Rechners.

rfc931

Wird nicht verwendet. An dieser Stelle wird in der Protokolldatei `-` eingetragen.

authuser

Wenn eine Authentifizierung erforderlich war, hat der Benutzer diesen Namen angegeben. Normalerweise nicht verwendet. An dieser Stelle wird `-` eingetragen.

[date]

Das Datum und die Uhrzeit der Anforderung.

"request"

Die Request-Zeichenkette wie sie vom Browser oder Client gesendet wurde.

status

Der HTTP-Statuscode, der an den Browser oder Client zurückgegeben wurde.

bytes

Die Größe des Dokuments.

Der Befehl `CustomLog` kann dazu verwendet werden, spezielle Protokolldateien einzurichten, die Referer (die URL der Web-Seite, die auf eine Seite auf Ihrem Web-Server verzweigt hat) und/oder Agenten protokollieren (die Browser, die zum Abrufen der Webseiten von Ihrem Web-Server verwendet wurden). Die entsprechenden Zeilen in `CustomLog` sind auskommentiert, wie unten gezeigt. Sie sollten die Kommentare jedoch entfernen, wenn Sie diese zwei Protokolldateien aktivieren möchten:

```
#CustomLog /var/log/httpd/referer_log referer
#CustomLog /var/log/httpd/agent_log agent
```

Als Alternative können Sie die Anweisung `CommonLog` auch so konfigurieren, dass ein `kombiniertes` Protokoll erstellt wird, indem Sie den Kommentar für folgende Zeile entfernen:

```
#CustomLog /var/log/httpd/access_log combined
```

Bei einem `kombinierten` Protokoll werden die Felder für Referer und Agent an das Ende der gemeinsamen Protokollfelder angefügt. Wenn Sie ein `kombiniertes` Protokoll verwenden möchten, müssen Sie die Anweisung `CustomLog` auskommentieren, um Ihre Zugriffsprotokolldatei auf das gemeinsame Protokolldateiformat einzustellen.

12.1.49 ServerSignature

Die Anweisung `ServerSignature` fügt in alle vom Server erstellten Dokumente eine Zeile ein, die die Apache Serverversion und den `ServerName` des Rechners enthält, auf dem der Server ausgeführt wird (z.B. Fehlermeldungen, die an Clients zurückgesendet werden). `ServerSignature` ist standardmäßig auf `on` eingestellt. Sie können die Einstellung auf `off` (es wird keine Zeile eingefügt) oder auf `EMail` ändern. `EMail` fügt ein HTML-Tag `mailto:ServerAdmin` in die Signaturzeile ein.

12.1.50 Alias

Die `Alias`-Einstellung macht es möglich, dass Verzeichnisse außerhalb des `DocumentRoot`-Verzeichnisses liegen können und doch vom Web-Server darauf zugegriffen werden kann. Jede URL, die mit dem Alias endet, verzweigt automatisch zum Aliaspfad. Als Standardeinstellung ist bereits ein Alias eingerichtet. Auf das Verzeichnis `icons` kann vom Web-Server zugegriffen werden, liegt jedoch nicht in `DocumentRoot`. Das Verzeichnis `icons` ist ein Alias, es handelt sich dabei in Wirklichkeit um `/var/www/icons/` und nicht um `/var/www/html/icons/`.

12.1.51 ScriptAlias

Die `ScriptAlias`-Einstellung legt fest, wo CGI-Skripte (oder andere Skriptarten) abgelegt sind. Im Allgemeinen sollten CGI-Skripte nicht in `DocumentRoot` abgelegt werden. In `DocumentRoot` abgelegte CGI-Skripten könnten wie Textdokumente gelesen werden. Auch wenn Sie nichts dagegen haben, dass andere Ihre CGI-Skripten lesen (und weiterverwenden), könnte die Offenlegung ihrer Funktion von Benutzern mit krimineller Energie zur Ausnutzung von Sicherheitslücken im Skript genutzt werden. Dies kann somit ein Sicherheitsrisiko für Ihren Server darstellen. Standardmäßig ist das Verzeichnis `cgi-bin` ein `ScriptAlias` von `/cgi-bin/` und in Wirklichkeit das Verzeichnis `/var/www/cgi-bin/`.

Für Ihr Verzeichnis `/var/www/cgi-bin` ist `Options ExecCGI` aktiviert, d.h. die Ausführung von CGI-Skripten ist innerhalb dieses Verzeichnisses erlaubt.

Hinweise zum Ausführen von CGI-Skripten in anderen Verzeichnissen als `cgi-bin` finden Sie in Abschnitt 12.1.66, *`AddHandler`* und Abschnitt 12.1.29, *`Directory`* .

12.1.52 Redirect

Wenn eine Web-Seite verschoben wird, kann mit `Redirect` die Zuordnung der alten URL auf eine neue URL erfolgen. Hier das Format:

```
Redirect /pfad/foo.html http://neue_domäne/pfad/foo.html
```

Wenn also eine HTTP-Anforderung für eine Seite empfangen wird, die früher unter http://*ihre_domäne* /*path*/foo.html abgerufen werden konnte, sendet der Server die neue URL (http://*new_domain* /*path*/foo.html) an den Client, der dann im Normalfall versucht, das Dokument von der neuen URL abzurufen.

12.1.53 IndexOptions

`IndexOptions` bestimmt das Erscheinungsbild der vom Server erstellten Verzeichnislisten durch das Hinzufügen von Symbolen und Dateibeschreibungen usw. Wenn `Options Indexes` aktiviert ist (siehe Abschnitt 12.1.31, *`Options`*), kann Ihr Web-Server eine Verzeichnisliste erstellen, wenn er eine HTTP-Anforderung wie die Folgende empfängt:

http://*ihre_domäne*/*dieses_verzeichnis*/

Als Erstes sucht Ihr Web-Server in diesem Verzeichnis nach einer Datei aus der Liste, die nach der `DirectoryIndex`-Anweisung angegeben ist (z.B. `index.html`). Wenn er keine der Dateien finden kann, wird eine HTML-Verzeichnisliste der in dem Verzeichnis enthaltenen Unterverzeichnisse und Dateien erstellt. Mit bestimmten Anweisungen (z.B. mit `IndexOptions`) können Sie in `httpd.conf` das Erscheinungsbild dieser Verzeichnisliste anpassen.

In der Standardkonfiguration ist `FancyIndexing` aktiviert. Wenn `FancyIndexing` aktiviert ist, werden durch Klicken auf die Überschrift der Spalte in der Verzeichnisliste die Einträge entsprechend dieser Spalte sortiert. Ein weiterer Klick auf dieselbe Überschrift schaltet von aufsteigender zu absteigender Reihenfolge um und umgekehrt. `FancyIndexing` zeigt außerdem je nach Dateiendung verschiedene

Symbole für verschiedene Dateien an. Bei Verwendung der Anweisung `AddDescription` und aktiviertem `FancyIndexing` wird in der vom Server erstellten Verzeichnisliste eine kurze Dateibeschreibung angegeben.

`IndexOptions` hat eine Reihe von weiteren Parametern, die zur Festlegung des Erscheinungsbilds der vom Server erstellten Verzeichnisse verwendet werden können. Zu diesen Parametern gehören `IconHeight` und `IconWidth`, durch die der Server angewiesen wird, die HTML-Tags `HEIGHT` und `WIDTH` für die Symbole in vom Server erstellten Web-Seiten zu verwenden, sowie `IconsAreLinks`, durch die die Symbole zusammen mit dem Dateinamen als Teil des HTML-Ankers für den Link verwendet werden können.

12.1.54 AddIconByEncoding

Diese Anweisung bestimmt die Symbole, die in vom Server erstellten Verzeichnislisten für Dateien mit MIME-Encoding angezeigt werden. Zum Beispiel verwendet der Web-Server in vom Server erstellten Verzeichnislisten standardmäßig für MIME-codierte x-compress- und x-gzip-Dateien das Symbol `compressed.gif`.

12.1.55 AddIconByType

In dieser Anweisung werden Symbole angegeben, die in vom Server erstellten Verzeichnislisten für Dateien mit MIME-Types angezeigt werden. Ihr Server ist zum Beispiel so konfiguriert, dass in vom Server erstellten Verzeichnislisten für Dateien mit dem Mime-Type "text" das Symbol `text.gif` angezeigt wird.

12.1.56 AddIcon

`AddIcon` gibt an, welche Symbole in vom Server erstellten Verzeichnislisten für bestimmte Dateitypen bzw. für Dateien mit bestimmten Erweiterungen anzuzeigen sind. Zum Beispiel ist Ihr Web-Server so konfiguriert, dass das Symbol `binary.gif` für Dateien mit der Erweiterung `.bin` oder `.exe` verwendet wird.

12.1.57 DefaultIcon

`DefaultIcon` bestimmt das Symbol, das in vom Server erstellten Verzeichnislisten für Dateien angezeigt wird, für die kein anderes Symbol angegeben ist. `unknown.gif` ist für diese Dateien standardmäßig `DefaultIcon`.

12.1.58 AddDescription

Mit `AddDescription` können Sie in vom Server erstellten Listen für bestimmte Dateien von Ihnen eingegebenen Text anzeigen lassen (dazu muss außerdem `FancyIndexing` in `IndexOptions` aktiviert sein). Sie können bestimmte Dateien, Platzhalterausdrücke oder Dateiendungen für die Dateien angeben, auf die diese Anweisung angewendet werden soll. Sie könnten zum Beispiel die folgende Zeile angeben:

```
AddDescription "Eine Datei mit der Endung .ni" .ni
```

In vom Server erstellten Verzeichnislisten hätten dann alle Dateien mit der Endung `.ni` die Beschreibung `Eine Datei mit der Endung .ni` nach dem Dateinamen. Beachten Sie, dass zusätzlich `FancyIndexing` aktiviert sein muss.

12.1.59 ReadmeName

`ReadmeName` bestimmt die Datei, die an das Ende der vom Server erstellten Verzeichnisliste angehängt wird (falls die Datei im Verzeichnis vorhanden ist). Der Web-Server versucht zuerst, die Datei als HTML-Dokument anzuhängen, dann als Standardtextdatei. Standardmäßig ist `ReadmeName` auf `README` eingestellt.

12.1.60 HeaderName

`HeaderName` bestimmt die Datei, die am Beginn der vom Server erstellten Verzeichnislisten eingefügt wird (falls die Datei im Verzeichnis vorhanden ist). Wie bei `ReadmeName` versucht der Server, die Datei nach Möglichkeit als HTML-Datei anzuhängen, sonst als einfachen Text.

12.1.61 IndexIgnore

`IndexIgnore` kann Dateiendungen, Teile von Dateinamen, Platzhalterausdrücke oder vollständige Dateinamen enthalten. Der Web-Server nimmt Dateien, die diesen Parametern entsprechen, nicht mit in vom Server erstellte Verzeichnislisten auf.

12.1.62 AddEncoding

`AddEncoding` bestimmt, welche Dateinamenerweiterungen eine spezielle Codierungsart angeben sollen. `AddEncoding` kann auch bei manchen Browsern (nicht bei allen) dazu verwendet werden, bestimmte Dateien beim Download zu entpacken.

12.1.63 AddLanguage

`AddLanguage` verknüpft Dateinamenserweiterungen mit der speziellen Sprache, in der der Inhalt abgefasst ist. Diese Anweisung ist hauptsächlich für den Inhaltsabgleich nützlich, wenn der Server je nach Spracheinstellung im Browser des Clients eines von mehreren möglichen Dokumenten zurückliefert.

12.1.64 LanguagePriority

`LanguagePriority` ermöglicht die Einstellung, in welchen Sprachen Dateien geliefert werden sollen, falls vom Client keine Angabe zur Sprache vorliegt.

12.1.65 AddType

Mit der Anweisung `AddType` können Sie paarweise Zuordnungen aus MIME-Types und Dateierweiterungen definieren. Wenn Sie zum Beispiel PHP4 einsetzen, verwendet Ihr Web-Server die Anweisung `AddType`, um Dateien mit PHP-Endungen (`.php4`, `.php3` `.phtml` `.php`) als PHP MIME-Types erkennen zu können.

Die folgende `AddType`-Zeile weist Ihren Server an, die Dateierweiterung `.shtml` zu erkennen (für serverseitige Includes):

```
AddType text/html .shtml
```

Diese Zeile muss innerhalb der Virtual Host-Tags stehen, wenn bei Ihnen virtuelle Rechner serverseitige Includes erlauben.

12.1.66 AddHandler

`AddHandler` ordnet Dateierweiterungen speziellen Handlern zu. Der `cgi-script`-Handler kann zum Beispiel in Kombination mit der Erweiterung `.cgi` verwendet werden, um eine Datei mit der Endung `.cgi` als CGI-Skript zu behandeln. Das funktioniert auch für Dateien, die außerhalb des `ScriptAlias`-Verzeichnisses liegen, wenn Sie die hier angegebenen Hinweise beachten.

Ihre Datei `httpd.conf` enthält einen `AddHandler` für CGI:

```
AddHandler cgi-script .cgi
```

Die Kommentare für diese Zeile müssen entfernt werden. Apache führt dann CGI-Skripten für Dateien aus, die mit `.cgi` enden, auch wenn sie außerhalb von `ScriptAlias` liegen. Als Standardeinstellung wird Ihr Verzeichnis `/cgi-bin/` in `/var/www/cgi-bin/` gesucht.

Zusätzlich muss `ExecCGI` als `Options` für alle Verzeichnisse eingestellt werden, die ein CGI-Skript enthalten. Weitere Informationen zum Einstellen von `ExecCGI` für ein Verzeichnis finden Sie in Abschnitt 12.1.29, *`Directory`* . Überprüfen Sie außerdem, ob die Zugriffsberechtigungen für die CGI-Skripten und die Verzeichnisse, die CGI-Skripten enthalten, richtig gesetzt sind. CGI-Skripten und der gesamte Verzeichnispfad zu den Skripten müssen die Berechtigung 0755 haben. Schließlich müssen der Eigentümer des Verzeichnisses und der Eigentümer der Skriptdatei derselbe Benutzer sein.

Dieselbe `AddHandler`-Zeile muss in `VirtualHost` eingefügt werden, wenn Sie virtuelle Rechner verwenden und diese auch CGI-Skripten außerhalb von `ScriptAlias` erkennen können sollen.

`AddHandler` wird vom Server neben CGI-Skripten auch für die Verarbeitung der vom Server verarbeiteten HTML- und Imagemap-Dateien verwendet.

12.1.67 Action

`Action` ermöglicht die Angabe einer Paarung aus MIME-Inhaltstyp und CGI-Skript, damit ein spezielles CGI-Skript immer dann ausgeführt wird, wenn eine Datei dieses Medientyps angefordert wird.

12.1.68 MetaDir

`MetaDir` gibt den Namen eines Verzeichnisses an, in dem Ihr Web-Server nach Dateien suchen soll, die Metainformationen enthalten (zusätzliche HTTP-Header), die bei der Bereitstellung von Dokumenten mit einzubeziehen sind.

12.1.69 MetaSuffix

MetaSuffix gibt das Dateinamensuffix für die Datei an, die die Metainformationen enthält (zusätzliche HTTP-Header), die im Verzeichnis MetaDir abgelegt sein sollten.

12.1.70 ErrorDocument

Standardmäßig gibt Ihr Web-Server bei einem Problem oder Fehler eine einfache (und meist kryptische) Fehlermeldung an den anfordernden Client zurück. Statt der Standardeinstellung können Sie ErrorDocument zur Konfiguration Ihres Web-Servers verwenden, so dass der Server eine von Ihnen angepasste Meldung ausgibt oder den Client zu einer lokalen oder externen URL umleitet. ErrorDocument verknüpft einfach einen HTTP-Antwortcode mit einer Meldung oder einer URL, die zum Client zurückgesendet wird.

12.1.71 BrowserMatch

Die Anweisung BrowserMatch ermöglicht es Ihrem Server, Umgebungsvariablen zu definieren und/oder auf Grundlage des User-Agent HTTP-Header-Felds (gibt den Browser des Clients an) in geeigneter Weise zu reagieren. Standardmäßig verwendet Ihr Web-Server BrowserMatch, um keine Verbindungen mit Browsern zuzulassen, die Probleme bereiten, und zum Deaktivieren von Keepalives und HTTP-Header-Löschbefehlen für Browser, von denen bekannt ist, dass sie Probleme mit diesen Aktionen haben.

12.1.72 ProxyRequests

Wenn Sie die Kommentare für die IfModule-Tags entfernen, die ProxyRequests und andere Anweisungen einschließen, arbeitet Ihr Apache Server auch als Proxyserver. Zusätzlich müssen Sie das Modul mod_proxy laden. Hinweise zum Laden von Modulen finden Sie in Abschnitt 12.2, *Hinzufügen von Modulen zu Ihrem Server*.

12.1.73 ProxyVia

Der Befehl ProxyVia legt für eine HTTP Via:-Zeile fest, ob diese zusammen mit Anforderungen oder Antworten gesendet wird, die über den Apache Proxyserver laufen. Der Header Via: enthält den Rechnernamen, wenn ProxyVia auf On eingestellt ist, den Rechnernamen und die Apache Version bei Einstellung auf Full, alle Via:-Zeilen werden unverändert weitergegeben bei Einstellung auf Off und die Via:-Zeilen werden entfernt bei Einstellung auf Block.

12.1.74 Cache Directives

Eine Reihe von Cache-Anweisungen sind in den oben genannten Proxy- IfModule-Tags auskommentiert. Wenn Sie die Proxyserver-Funktion nutzen und auch den Proxy-Cache aktivieren möchten, sollten Sie wie beschrieben die Kommentare für die Cache-Anweisungen entfernen. Die Standardeinstellungen für Ihre Cache-Anweisungen sollten für die meisten Konfigurationen ausreichen.

CacheRoot bestimmt den Namen des Verzeichnisses, in dem die zwischengespeicherten Dateien abgelegt werden. Die Standard- CacheRoot ist /var/cache/httpd.

CacheSize bestimmt, wie viel Speicherplatz in KB für den Cache zur Verfügung gestellt wird. Der Standardwert für CacheSize ist 5 KB.

CacheGcInterval legt eine Anzahl von Stunden fest, nach der im Cache enthaltene Dateien gelöscht werden, wenn der Cache mehr Platz beansprucht als durch CacheSize erlaubt. Die Standardeinstellung für CacheGcInterval ist vier Stunden.

Im Cache gespeicherte HTML-Dokumente werden für eine maximale Anzahl von Stunden im Cache gehalten (ohne Neuladen vom Ursprungsserver), die durch CacheMaxExpire eingestellt wird. Der Standardwert ist 24 Stunden.

Der CacheLastModifiedFactor betrifft die Erzeugung eines Ablaufdatums (expiration) für ein Dokument, das vom Ursprungsserver nicht mit einem eigenen Ablaufdatum versehen wurde. Der Standard-CacheLastModifiedFactor ist auf 0.1 eingestellt, d.h. das Ablaufdatum für solche Dokumente entspricht einem Zehntel der Zeit, die vergangen ist, seitdem das Dokument zuletzt geändert wurde.

`CacheDefaultExpire` ist die Ablaufzeit in Stunden für ein Dokument, das über ein Protokoll empfangen wurde, das keine Ablaufzeiten unterstützt. Die Standardeinstellung ist eine Stunde.

Dokumente, die von einem Rechner und/oder einer Domäne abgerufen werden, die mit einem Eintrag in `NoCache` übereinstimmen, werden nicht im Cache gespeichert. Wenn Sie die Dokumente von bestimmten Rechnern oder Domänen nicht im Cache speichern möchten, können Sie die Kommentare für `NoCache` entfernen und die entsprechenden Domänen oder Rechnernamen hier angeben.

12.1.75 NameVirtualHost

Wenn Sie namensbasierte virtuelle Rechner einrichten, müssen Sie die Anweisung `NameVirtualHost` für die IP-Adresse verwenden (und die Portnummer, falls erforderlich). Die Konfiguration von namensbasierten virtuellen Rechnern wird verwendet, wenn Sie verschiedene virtuelle Rechner für verschiedene Domänen einrichten möchten, aber nicht genügend verschiedene IP-Adressen für die verschiedenen Domänennamen haben (oder verwenden möchten), für die Ihr Web-Server Dokumente bereitstellt.

Bitte beachten

Namensbasierte virtuelle Rechner können nicht gemeinsam mit dem sicheren Server verwendet werden. Alle eingerichteten namensbasierten virtuellen Rechner funktionieren nur für unverschlüsselte HTTP-Verbindungen, nicht für SSL-Verbindungen.

Namensbasierte virtuelle Rechner können nicht zusammen mit dem sicheren Server verwendet werden, weil der SSL-Handshake (der Zeitpunkt, wenn der Browser das Authentifizierungszertifikat des sicheren Web-Servers annimmt) vor der HTTP-Anforderung stattfindet, die den richtigen namensbasierten virtuellen Rechner identifiziert. Anders ausgedrückt, die Authentifizierung findet statt, bevor die Identifikation der verschiedenen namensbasierten virtuellen Rechner stattfindet. Virtuelle Rechner müssen IP-Adressen-basiert sein, um sie gemeinsam mit dem sicheren Server verwenden zu können.

Wenn Sie namensbasierte virtuelle Rechner verwenden, sind für die Konfigurationsanweisung `NameVirtualHoHallst` die Kommentare zu entfernen, und nach `NameVirtualHost` ist die richtige IP-Adresse für Ihren Server anzugeben. Anschließend sind mit `Virtual Host`-Tags weitere Informationen zu den verschiedenen Domänen hinzuzufügen, die `ServerName` für jeden virtuellen Rechner sowie weitere Konfigurationsanweisungen einschließen, die nur für diesen virtuellen Rechner gelten.

12.1.76 `VirtualHost`

`<VirtualHost>`- und `</VirtualHost>`-Tags umschließen alle Konfigurationsanweisungen, die für einen virtuellen Rechner gelten. Die meisten Konfigurationsanweisungen können innerhalb von VirtualHost-Tags verwendet werden und gelten dann für diesen virtuellen Rechner.

Eine Reihe von auskommentierten `VirtualHost`-Tags umschließen einige Beispielkonfigurationsanweisungen und Platzhalter für die Informationen, die für die Einrichtung eines virtuellen Rechners benötigt würden. Weitere Informationen über virtuelle Rechner finden Sie in Abschnitt 12.3, *Virtuelle Rechner verwenden*.

12.1.77 SetEnvIf

Die Apache Konfigurationsanweisung `SetEnvIf` wird zur Deaktivierung von HTTP-Keepalive verwendet und ermöglicht SSL das Schließen der Verbindung, ohne dass ein Close Notify-Alarm vom Client-Browser gesendet wird. Diese Einstellung ist für bestimmte Browser erforderlich, die die SSL-Verbindung nicht zuverlässig beenden.

12.1.78 SSL-Konfigurationsanweisungen

Die SSL-Anweisungen sind in der Datei `httpd.conf` Ihres Servers enthalten, um sichere Web-Kommunikationen mit SSL und TLS zu ermöglichen.

Weitere Informationen zu SSL-Anweisungen finden Sie unter http://*ihre_domäne*/manual/mod/mod_ssl/. Weitere Informationen zu SSL-Anweisungen finden Sie außerdem unter http://www.modssl.org/docs/2.6/ssl_reference.html/. Es handelt sich dabei um ein Kapitel in einem Webdokument über mod_ssl von Ralf Engelschall. Dasselbe Dokument, das mod_ssl *User Manual*, beginnt unter http://www.modssl.org/docs/2.6/ und ist (selbstverständlich) eine gute Referenzquelle für mod_ssl und für Web-Kryptographie im Allgemeinen. Informationen zum Thema Sicherheit für Ihren Web-Server finden Sie im vorliegenden Handbuch in Kapitel 11, *Beantragen eines Zertifikats für Ihren sicheren Server*.

Bitte beachten

Nehmen Sie keine Veränderungen an Ihren SSL-Anweisungen vor, es sei denn, Sie wissen genau, was Sie tun. Für die große Mehrheit der Red Hat Linux Secure Web Server sind die SSL-Anweisungen in der installierten Form völlig ausreichend.

12.2 Hinzufügen von Modulen zu Ihrem Server

Da Apache 1.3 DSOs unterstützt, können Sie Apache Module auf einfache Weise laden bzw. Ihre eigenen Module für den Red Hat Linux Secure Web Server einkompilieren. DSO-Unterstützung bedeutet, dass Module während der Laufzeit geladen werden können. Da die Module nur bei Bedarf geladen werden, belegen Sie keinen Speicherplatz, wenn sie nicht geladen sind. Dadurch sinkt der Speicherbedarf insgesamt.

Die Apache Group stellt eine vollständige DSO-Dokumentation unter http://www.apache.org/docs/dso.html zur Verfügung. Nach der Installation Ihres Servers können Sie auch unter http://*ihre_domäne*/manual/mod/ Dokumentationen im HTML-Format zu Apache Modulen finden (falls das Paket `apache-manual` installiert ist). Im Folgenden wird eine Kurzbeschreibung zum Laden von Modulen gegeben. Wenn Sie mehr Einzelheiten wissen möchten, sollten Sie jedoch die oben genannten URLs aufrufen.

Damit Ihr Red Hat Linux Secure Web Server ein dynamisch gemeinsam verwendetes Modul verwenden kann, muss für dieses Modul in der Datei `httpd.conf` eine `LoadModule`-Zeile und eine `AddModule`-Zeile enthalten sein. Viele Module enthalten diese zwei Zeilen bereits standardmäßig in `httpd.conf`, doch sind einige der weniger oft verwendeten Module auskommentiert. Die auskommentierten Module wurden während des Kompilierens eingefügt, werden jedoch standardmäßig nicht geladen.

Wenn Sie eines dieser nichtgeladenen Module verwenden müssen, finden Sie in der Datei `httpd.conf` alle verfügbaren Module. Alle verfügbaren Module haben eine entsprechende `LoadModule`-Zeile. Der Abschnitt `LoadModule` beginnt mit diesen sieben Zeilen:

```
#LoadModule mmap_static_module modules/mod_mmap_static.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule env_module         modules/mod_env.so
LoadModule config_log_module  modules/mod_log_config.so
LoadModule agent_log_module   modules/mod_log_agent.so
LoadModule referer_log_module modules/mod_log_referer.so
#LoadModule mime_magic_module  modules/mod_mime_magic.so
```

Die meisten der Zeilen sind nicht auskommentiert, was anzeigt, dass jedes verknüpfte Modul einkompiliert wurde und standardmäßig geladen wird. Die erste Zeile ist auskommentiert, d.h. das entsprechende Modul (`mmap_static_module`) wurde einkompiliert, aber nicht geladen.

Um Ihren Red Hat Linux Secure Web Server anzuweisen, ein nicht geladenes Modul zu laden, entfernen Sie zuerst die entsprechende `LoadModule`-Zeile. Wenn Sie zum Beispiel erreichen möchten, dass Ihr Red Hat Linux Secure Web Server das Modul `mime_magic_module` lädt, ändern Sie die `LoadModule`-Zeile:

```
#LoadModule mime_magic_module modules/mod_mime_magic.so
```

Entfernen Sie die Kommentare in dieser Zeile, damit die folgende Zeile entsteht:

```
LoadModule mime_magic_module modules/mod_mime_magic.so
```

Als Nächstes müssen Sie die Kommentare für die entsprechende Zeile im Abschnitt `AddModule` in der Datei `httpd.conf` entfernen. Wir fahren nun mit unserem Beispiel von vorhin fort. Entfernen Sie die Kommentare in der `mod_mime_magic`-Zeile. Die ursprüngliche (Standard-) Zeile sieht folgendermaßen aus:

```
#AddModule mod_mime_magic.c
```

Ohne die Kommentare sieht die Zeile dann so aus:

```
AddModule mod_mime_magic.c
```

Nachdem Sie für die `LoadModule`- und `AddModule`-Zeilen für die Module, die Sie laden möchten, die Kommentare entfernt haben, halten Sie den Web-Server an, und starten Sie ihn neu, wie in Abschnitt 11.11, *Starten und Beenden von Apache* beschrieben. Nach dem Start sollten die Module in Ihren Red Hat Linux Secure Web Server geladen werden.

Wenn Sie ein eigenes Modul haben, können Sie es zur Datei `httpd.conf` hinzufügen, damit es als ein DSO einkompiliert und geladen wird. Dazu müssen Sie das Paket `apache-devel` installieren, wie in Kapitel 10, *Installieren von Red Hat Linux Secure Web Server* beschrieben. Das Paket `apache-devel` wird benötigt, weil es die Include-Dateien, die Header-Dateien und das APache eXtenSion (APXS)-Unterstützungstool installiert. APXS verwendet die Include-Dateien und die Header-Dateien zum Kompilieren Ihres Moduls, damit es mit Apache zusammenarbeiten kann.

Wenn Sie ein eigenes Modul geschrieben haben oder eines von einem anderen Benutzer ausborgen, sollten Sie APXS für das Kompilieren Ihrer Modulquellen außerhalb des Apache Quellbaums anwenden können, ohne Compiler- und/oder Linkerflags anpassen zu müssen. Weitere Informationen über APXS finden Sie in der Apache Dokumentation unter http://www.apache.org/docs/dso.html.

Speichern Sie Ihr Modul nach dem Kompilieren mit APXS in `/usr/lib/apache`. Anschließend muss in der Datei `httpd.conf` wie oben für die eigenen Module von Apache beschrieben eine `LoadModule`- und eine `AddModule` -Zeile eingefügt werden. Fügen Sie nach der `LoadModule`-Liste in der Datei `httpd.conf` für die Shared Object-Datei für Ihr Modul eine Zeile wie die folgende ein:

```
LoadModule foo_module  modules/mod_foo.so
```

Beachten Sie, dass Sie den Modulnamen und den Namen Ihrer Shared Object-Datei in geeigneter Weise ändern müssen.

Fügen Sie am Ende der `AddModule`-Liste in der Datei `httpd.conf` für Ihr Modul eine Zeile für die Quellcodedatei wie die Folgende ein:

```
AddModule mod_foo.c
```

Beachten Sie, dass der Name der Quellcodedatei in geeigneter Weise geändert werden muss.

Halten Sie Ihren Web-Server an, und starten Sie ihn erneut wie in Abschnitt 11.11, *Starten und Beenden von Apache* beschrieben, nachdem Sie die oben beschriebenen Schritte ausgeführt haben. Wenn Sie keine Fehler gemacht haben und Ihr Modul richtig programmiert ist, sollte der Web-Server Ihr Modul beim Starten finden und laden.

12.2.1 Das mod_ssl-Sicherheitsmodul

Der mod_ssl-Sicherheitsteil von Red Hat Linux Secure Web Server liegt als Dynamic Shared Object (DSO) vor. Das bedeutet, der Apache Web-Server kann vom Benutzer neu kompiliert werden, wenn der EAPI-Erweiterungspatch aus dem mod_ssl-Sicherheitsmodul in Apache integriert wird. Folgen Sie der in der mod_ssl-Dokumentation enthaltenen Anleitung zum Integrieren von mod_ssl in Apache, fügen Sie jedoch das folgende Flag hinzu:

```
--with-eapi-only
```

Die vollständige Befehlszeile sollte dann so aussehen:

```
./configure [Benutzerflags] --with-eapi-only
```

Erstellen und installieren Sie dann Apache.

Bitte beachten

Red Hat kann für neukompilierte Versionen von Apache Web-Server keinen Support anbieten. Für die Installation der Ihnen bereitgestellten Version wird Support angeboten, wenn Sie jedoch Apache neu kompilieren, entfällt dieser. Bitte nehmen Sie keine Neukompilierung von Apache vor, es sei denn, Sie wissen genau, was Sie tun.

12.3 Virtuelle Rechner verwenden

Sie können mit Apache das Prinzip der virtuellen Rechner nutzen, um auf demselben Rechner verschiedene Server mit verschiedenen IP-Adressen, verschiedenen Rechnernamen oder verschiedenen Ports auszuführen. Wenn Sie sich dafür interessieren, können Sie in der Apache Dokumentation auf Ihrem Rechner und im Web unter http://www.apache.org/docs/vhosts/ weitere Informationen finden.

Bitte beachten

Namensbasierte virtuelle Rechner können nicht zusammen mit dem Red Hat Linux Secure Web Server verwendet werden, weil der SSL-Handshake (der Zeitpunkt, wenn der Browser das Authentifizierungszertifikat des sicheren Web-Servers annimmt) vor der HTTP-Anforderung stattfindet, die den richtigen namensbasierten virtuellen Rechner identifiziert. Wenn Sie namensbasierte virtuelle Rechner verwenden möchten, können Sie diese nur mit dem Web-Server verwenden, der ohne Verschlüsselung arbeitet.

Virtuelle Rechner werden in der Datei `httpd.conf` konfiguriert, wie in Abschnitt 12.1, *Konfigurationsanweisungen in `httpd.conf`* beschrieben. Bitte lesen Sie dort nach, bevor Sie die Konfiguration der virtuellen Rechner auf Ihrem Rechner ändern.

12.3.1 Die virtuellen Rechner von Red Hat Linux Secure Web Server

In der Standardkonfiguration Ihres Red Hat Linux Secure Web Server wird ein unverschlüsselter und sicherer Server ausgeführt. Beide Server verwenden dieselbe IP-Adresse und denselben Rechnernamen, warten jedoch an verschiedenen Ports auf Anforderungen. Außerdem ist der sichere Server ein virtueller Rechner. Mit dieser Konfiguration können Sie sowohl unverschlüsselte als auch sichere Dokumente auf effektivste Weise bereitstellen. Wie Ihnen wahrscheinlich bekannt ist, erfordern sichere HTTP-Übertragungen mehr Zeit als nicht verschlüsselte Übertragungen, da während der sicheren Transaktionen erheblich mehr Informationen ausgetauscht werden. Die Verwendung Ihres sicheren Servers für unverschlüsselten Web-Datenverkehr ist daher nicht zu empfehlen.

Die Konfigurationsanweisungen für Ihren sicheren Server sind innerhalb von Virtual Host-Tags in der Datei `httpd.conf` untergebracht. Wenn Sie die Konfiguration Ihres sicheren Servers ändern möchten, müssen Sie die Konfigurationsanweisungen innerhalb der Virtual Host-Tags in der Datei `httpd.conf` anpassen. Wenn Sie bestimmte Funktionen für Ihren sicheren Server aktivieren möchten (z.B. serverseitige Includes), müssen diese innerhalb der Virtual Host-Tags aktiviert werden, die Ihren sicheren Server definieren.

Der unverschlüsselte Web-Server wird wie der "nichtvirtuelle" Rechner in der Datei `httpd.conf` konfiguriert. Anders ausgedrückt, die Konfigurationsoptionen des unverschlüsselten Web-Servers befinden sich außerhalb der Virtual Host-Tags in der Datei `httpd.conf`. Wenn Sie an der Konfiguration Ihres unverschlüsselten Web-Servers Änderungen vornehmen möchten, müssen Sie die Konfigurationsanweisungen außerhalb der Virtual Host-Tags in der Datei `httpd.conf` ändern.

Standardmäßig verwenden sowohl der sichere als auch der unverschlüsselte Web-Server dieselbe `DocumentRoot`. Diese Konfigurationsanweisung wird in der Datei `httpd.conf` angegeben. Anders ausgedrückt, der sichere und der unverschlüsselte Web-Server verwenden dasselbe Verzeichnis für die HTML-Dateien, die für Anforderungen bereitgestellt werden. Standardmäßig ist `DocumentRoot` auf `/var/www/html` eingestellt.

Um `DocumentRoot` so zu ändern, dass es nicht mehr gemeinsam vom sicheren und vom unverschlüsselten Server verwendet wird, ist eine der `DocumentRoot`-Anweisungen in der Datei `httpd.conf` zu ändern. `DocumentRoot` außerhalb der Virtual Host-Tags definiert die `DocumentRoot` für Ihren unverschlüsselten Web-Server. Wenn `DocumentRoot` innerhalb der Virtual Host-Tags steht, die Ihren sicheren Server definieren, so definiert diese (offensichtlich) Ihren sicheren Server.

Sie können den unverschlüsselten Web-Server auf Ihrem Rechner deaktivieren. Der sichere Server wartet am Port 443, dem Standardport für sichere Web-Kommunikation, auf Anforderungen. Der unverschlüsselte Web-Server wartet am Port 80, dem Standardport für unverschlüsselte Web-Kommunikation, auf Anforderungen. Um für den unverschlüsselten Server die Annahme von Anforderungen zu deaktivieren, ist in der Datei `httpd.conf` folgende Zeile zu suchen:

```
Port 80
```

Ändern Sie diese Zeile folgendermaßen:

```
Port 443
```

Kommentieren Sie dann die Zeile `Listen 80` aus, so dass anstatt von

```
Listen 80
```

die Zeile so aussieht:

```
#Listen 80
```

Nachdem diese zwei Schritte ausgeführt sind, nimmt Ihr Red Hat Linux Secure Web Server Verbindungen an Port 443 an, dem Standardport für sichere Web-Kommunikation. An Port 80, dem Standardport für unverschlüsselte Verbindungen, werden vom Server jedoch keine Verbindungen angenommen. Der unverschlüsselte Web-Server ist damit praktisch deaktiviert.

12.3.2 Einrichten von virtuellen Rechnern

Die meisten Benutzer verwenden Red Hat Linux Secure Web Server wahrscheinlich in seiner Standardkonfiguration. Daher werden die integrierten Funktionen für virtuelle Rechner verwendet, eine Bearbeitung der Anweisungen für virtuelle Rechner in der Datei `httpd.conf` ist jedoch nicht erforderlich. Sie können virtuelle Rechner aber auch aus anderen Gründen verwenden.

Zum Erstellen eines virtuellen Rechners müssen entweder die in der Datei `httpd.conf` als Beispiel enthaltenen Virtual Host-Zeilen geändert werden, oder Sie erstellen Ihren eigenen Virtual Host-Abschnitt. (Beachten Sie bitte, dass namensbasierte virtuelle Rechner nicht mit dem sicheren Server zusammen funktionieren — wenn SSL-fähige virtuelle Rechner benötigt werden, müssen Sie IP-Adressen-basierte virtuelle Rechner verwenden. Der unverschlüsselte Server unterstützt jedoch sowohl IP-Adressen- als auch namensbasierte virtuelle Rechner.)

Hier die Beispielzeilen für den virtuellen Rechner:

```
#<VirtualHost ip.address.of.host.some_domain.com>
#    ServerAdmin webmaster@host.some_domain.com
#    DocumentRoot /www/docs/host.some_domain.com
#    ServerName host.some_domain.com
#    ErrorLog logs/host.some_domain.com-error_log
#    CustomLog logs/host.some_domain.com-access_log common
#</VirtualHost>
```

Entfernen Sie das Kommentarzeichen # vom Beginn jeder Zeile. Tragen Sie dann in jeder Zeile die für Ihren Rechner und/oder virtuellen Rechner zutreffenden Informationen ein.

In der ersten Zeile ist `ip.address.of.host.some_domain.com` in die IP-Adresse Ihres Servers zu ändern. Ändern Sie `ServerName` in einen *gültigen* DNS-Namen für den virtuellen Rechner. (Also nicht einfach etwas erfinden. Fragen Sie Ihren Systemadministrator, wenn Sie nicht wissen, wie Sie an einen gültigen Domänennamen gelangen können.)

Außerdem muss für eine der `NameVirtualHost`-Zeilen in der Datei `httpd.conf` das Kommentarzeichen entfernt werden:

```
#NameVirtualHost 12.34.56.78:80
#NameVirtualHost 12.34.56.78
```

Entfernen Sie in einer der Zeilen das Kommentarzeichen, und ändern Sie die IP-Adresse in die IP-Adresse (und den Port, falls erforderlich) des virtuellen Rechners.

Zwischen den Virtual Host-Tags können je nach dem Zweck des virtuellen Rechners viele andere Konfigurationsanweisungen angegeben werden.

Wenn Sie einen virtuellen Rechner einrichten und dieser an einem Port auf Anforderungen warten soll, der nicht der Standardport ist (80 ist der Standardport für unverschlüsselte Web-Kommunikation, 443 der Standardport für sichere Web-Kommunikation) müssen Sie für diesen Port einen virtuellen Rechner einrichten und eine `Listen`-Anweisung in die Datei `httpd.conf` einfügen, die diesem Port entspricht.

Um einen virtuellen Rechner speziell für diesen Port einzurichten, ist in der ersten Zeile der Konfiguration für den virtuellen Rechner die Portnummer anzugeben. Die erste Zeile sollte etwa folgendermaßen aussehen:

```
<VirtualHost ip_address_of_your_server:12331>
```

Diese Zeile würde einen virtuellen Rechner erzeugen, der an Port 12331 auf Anforderungen wartet. Geben Sie hier für `12331` die von Ihnen gewünschte Portnummer an.

Fügen Sie in der Datei `httpd.conf` unter den `Listen`-Zeilen eine Zeile wie die folgende ein, die Ihren Web-Server anweist, an Port 12331 auf Anforderungen zu warten:

```
Listen 12331
```

Zum Starten eines neuen virtuellen Rechners muss der Server neu gestartet werden.

Vollständigere Informationen zum Erstellen und Konfigurieren von namens-basierten und IP-Adressen-basierten virtuellen Rechnern finden Sie im Web unter http://www.apache.org/docs/vhosts/index.html. Weitere Einzelheiten zur Verwendung virtueller Rechner finden Sie in der Dokumentation der Apache Group zu virtuellen Rechnern.

Teil III Installationsbezogene Referenzinformationen

13 Eine Installation im Textmodus vorbereiten

13.1 Was Sie wissen sollten

Um unangenehme Überraschungen während der Installation zu vermeiden, sollten Sie einige Systeminformationen sammeln, bevor Sie mit der Installation von Red Hat Linux beginnen. Die meisten Angaben hierzu finden Sie in der Dokumentation, die mit dem System geliefert wurde, oder Sie erhalten sie bei Ihrem Fachhändler oder dem Hersteller Ihres Computers.

Eine aktuelle Liste der von Red Hat Linux unterstützten Hardware können Sie unter http://www.redhat.com/hardware abrufen. Es kann nicht schaden, Ihre Hardware mit den dort aufgelisteten Komponenten zu vergleichen, bevor Sie mit der Installation beginnen.

Bitte beachten

Wenn Sie den Anweisungen in diesem Kapitel und in Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm* folgen, können Sie Red Hat Linux 7.0 auch im Textmodus installieren. Wenn Sie jedoch die Installation über eine CD-ROM vornehmen, ist die Verwendung des benutzerfreundlichen grafischen Installationsmodus empfehlenswert, der Ihnen zugleich ein hohes Maß an Flexibilität ermöglicht. Weitere Informationen zu Installationen mit grafischer Benutzeroberfläche finden Sie im *Offiziellen Red Hat Linux Installationshandbuch*.

Tipp

Am Ende des Kapitels *Bevor Sie beginnen* im *Offiziellen Red Hat Linux Installationshandbuch* befindet sich eine Tabelle, in die Sie ihre speziellen Systemanforderungen eintragen können. Damit können Sie sich einen besseren Überblick über die während der Installation benötigten Informationen verschaffen.

13.1.1 Grundlegende Hardware-Konfiguration

Vor der Installation sollten Sie wissen, welche Hardware in Ihrem System vorhanden ist:

- Festplatte(n) - Insbesondere Anzahl, Größe und Typ. Wenn Ihr System mit mehr als einer Festplatte ausgerüstet ist, sollten Sie wissen, welche die erste, die zweite usw. ist. Wichtig ist außerdem, ob es sich um IDE- oder SCSI-Festplatten handelt. Wenn Sie IDE-Laufwerke haben, müssen Sie im BIOS Ihres Computers nachsehen, ob der Zugriff im **linearen Modus** erfolgt. Bitte lesen Sie in der Dokumentation Ihres Computers nach, mit welcher Tastenkombination Sie das BIOS aufrufen können. Beachten Sie bitte, dass im BIOS Ihres Computers für den linearen Modus möglicherweise eine andere Bezeichnung steht, z.B. "large disk mode". Informationen hierzu finden Sie ebenfalls in der Computer-Dokumentation.
- Speicher - Größe des in Ihrem Computer installierten RAM.
- CD-ROM - Besonders wichtig ist der Schnittstellentyp (IDE, SCSI oder eine andere Schnittstelle) sowie bei Nicht-IDE-, Nicht-SCSI-CD-ROM-Laufwerken Hersteller und Modellnummer. IDE-CD-ROM-Laufwerke (auch als ATAPI bekannt) sind bei neueren PC-kompatiblen Computern am weitesten verbreitet.
- SCSI-Adapter (falls vorhanden) - Hersteller und Modellnummer.
- Netzwerkkarte (falls vorhanden) - Hersteller und Modellnummer.

- Maus - Maustyp (seriell, PS/2 oder Busmaus), Protokoll (Microsoft, Logitech, MouseMan usw.) und die Anzahl der Tasten. Bei einer seriellen Maus außerdem die serielle Schnittstelle, an der die Maus angeschlossen ist.

Auf vielen neueren Systemen erkennt das Installationsprogramm die Hardware automatisch. Um sicher zu gehen, sollten Sie sich diese Informationen trotzdem beschaffen.

Herausfinden der Hardware-Konfiguration mit Windows

Wenn auf Ihrem Computer bereits Windows 9*x* installiert ist, können Sie folgendermaßen weitere Angaben zur Konfiguration abrufen:

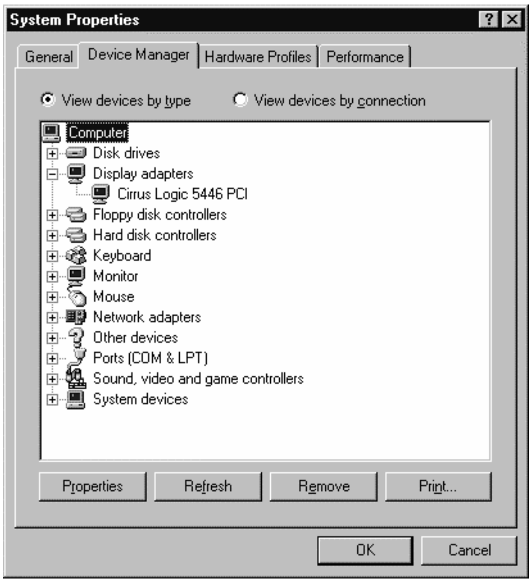
Abbildung 13–1 Windows Systemeigenschaften

- Klicken Sie unter Windows mit der zweiten (normalerweise der rechten) Maustaste auf das Symbol **Arbeitsplatz**. Ein Kontextmenü erscheint auf dem Bildschirm.

- Wählen Sie **Eigenschaften**. Das Fenster **Eigenschaften für System** wird geöffnet. Beachten Sie die unter **Computer** aufgeführten Angaben - insbesondere die Größe des RAM.
- Klicken Sie auf das Register **Gerätemanager**. Sie sehen eine grafische Darstellung der Hardware-Konfiguration Ihres Computers. Achten Sie darauf, dass das runde Optionsfeld **Modelle nach Typ anzeigen** ausgewählt ist.

Jetzt können Sie auf jedes Symbol doppelklicken (oder einmal auf das Pluszeichen **+**) um ausführlichere Informationen zum jeweiligen Eintrag zu erhalten. Suchen Sie unter den folgenden Symbolen nach ausführlicheren Informationen:

Abbildung 13–2 Gerätemanager unter Windows 95



- **Laufwerke** - Der Typ der Festplatte (IDE oder SCSI) wird angezeigt. (Bei IDE-Festplatten ist das Wort "IDE" normalerweise in der Angabe enthalten, bei SCSI-Festplatten jedoch nicht.)

- **Festplattenlaufwerk-Controller** - Hier erhalten Sie Angaben zu Ihrem Festplattenlaufwerk-Controller.
- **CD-ROM** - Hier finden Sie alle Informationen über die CD-ROM-Laufwerke in Ihrem Computer.

Bitte beachten

Manchmal wird kein CD-ROM-Symbol angezeigt, obwohl der Computer mit einem funktionierenden CD-ROM-Laufwerk ausgestattet ist. Je nach ursprünglicher Installation von Windows ist das normal. In diesem Fall erhalten Sie Informationen zu Ihrem CD-ROM-Laufwerk, wenn Sie sich den entsprechenden Treiber ansehen, der in der Datei `config.sys` Ihres Computers geladen wird.

- **Maus** - Der Typ der am Computer angeschlossenen Maus wird hier angezeigt.
- **Grafikkarten** - Wenn Sie mit dem X Window System arbeiten möchten, notieren Sie sich bitte die hier aufgeführten Angaben.
- **Audio-, Video- und Gamecontroller** - Wenn Ihr Computer über eine Soundkarte verfügt, finden Sie hier mehr Informationen dazu.
- **Netzwerkkarten** - Hier finden Sie weitere Informationen zur Netzwerkkarte des Computers (falls vorhanden).
- **SCSI-Controller** - Wenn Ihr Computer mit SCSI-Peripheriegeräten arbeitet, finden Sie hier Angaben zum SCSI-Controller.

Auch wenn diese Vorgehensweise das Öffnen des Computergehäuses nicht immer erspart, um einen Blick auf die vorhandenen Komponenten zu werfen, erhalten Sie damit in vielen Fällen genügend Informationen, um die Installation fortsetzen zu können.

Bitte beachten

Diese Informationen können durch Klicken auf die Schaltfläche **Drucken** auch gedruckt werden. Ein zweites Dialogfeld erscheint, in dem Sie den Drucker sowie den Reporttyp wählen können (der Reporttyp **Kombinierte Geräte- und Systemübersicht** enthält die meisten Informationen).

13.1.2 Grafikkonfiguration

Wenn Sie das X Window System installieren möchten, sollte Ihnen Folgendes bekannt sein:

- Grafikkarte - Hersteller und Modellnummer der Grafikkarte (oder der verwendete Grafikchipsatz) und die Größe des Grafikspeichers. Die meisten PCI-Karten werden vom Installationsprogramm automatisch erkannt.
- Bildschirm - Hersteller und Modellnummer sowie die zulässigen horizontalen und vertikalen Bildwiederholfrequenzen. (Neuere Modelle werden vom Installationsprogramm automatisch erkannt).

13.1.3 Informationen zum Netzwerk

Wenn Ihr Computer mit einem Netzwerk verbunden ist, sollte Ihnen Folgendes bekannt sein:

- IP-Adresse - Normalerweise dargestellt durch vier Zahlen, die durch Punkte getrennt sind, z.B. `10.0.2.15`.
- Netzmaske - Weitere vier durch Punkte getrennte Zahlen. Ein Beispiel für eine Netzmaske ist `255.255.248.0`.
- Gateway-IP-Adresse - Weitere vier durch Punkte getrennte Zahlen. Zum Beispiel `10.0.2.254`.
- Ein oder mehrere Nameserver-IP-Adressen - Eine oder mehrere Kombinationen von durch Punkte getrennten Zahlen. So könnte die Adresse Ihres Nameservers beispielsweise `10.0.2.1` lauten.

- Domänenname - Der Ihrer Organisation zugeteilte Name. Der Domänenname von Red Hat lautet zum Beispiel `redhat.com`.
- Rechnername - Der Name Ihres Computers. Ein Computer kann z.B. `Knecht` heißen.

Bitte beachten

Die oben aufgeführten Informationen sind lediglich Beispiele! Arbeiten Sie bitte *nicht* mit diesen Angaben, wenn Sie Red Hat Linux installieren! Wenn Sie die richtigen Angaben für Ihr Netzwerk nicht kennen, fragen Sie bitte Ihren Netzwerkadministrator.

14 Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm

Diese Version von Red Hat Linux bietet Ihnen ein grafisches, mausgestütztes Installationsprogramm, das im *Offiziellen Red Hat Linux Installationshandbuch* dokumentiert ist. Sie können Red Hat Linux jedoch auch mit einem textorientierten, tastaturbedienten Installationsprogramm installieren. Dieses Kapitel erläutert, wie Sie dabei vorgehen müssen. Hier einige Empfehlungen:

- Wenn Sie Linux noch niemals zuvor installiert haben, sollten Sie zunächst das *Offizielle Red Hat Linux Installationshandbuch* lesen. Auch wenn dort der Schwerpunkt auf dem Installationsvorgang mit grafischer Benutzeroberfläche liegt, gelten die meisten Konzepte auch für die Installation im Textmodus. Danach finden Sie in Kapitel 13, *Eine Installation im Textmodus vorbereiten* weiter gehende Informationen zu den Aspekten der Installation von Red Hat Linux, die nicht für den Installationsvorgang mit grafischer Benutzeroberfläche gelten.

  Des Weiteren kann Anhang B, *Eine Einführung in Festplattenpartitionen* für Sie interessant sein, da darin das Ändern der vorhandenen Festplattenpartitionen beschrieben wird (was sehr wichtig ist, wenn Sie Linux auf einer Festplatte installieren möchten, auf der Windows oder ein anderes Betriebssystem bereits installiert sind).

- Falls Sie für die Installation PCMCIA-Unterstützung benötigen (z.B. wenn Sie Linux auf einem Laptop installieren möchten, der mit einer PCMCIA-Karte ausgestattet ist), müssen Sie eine PCMCIA-Bootdiskette erstellen. Im *Offiziellen Red Hat Linux Installationshandbuch* ist das Erstellen einer solchen Diskette beschrieben.

- Wenn Sie Linux über ein Netzwerk (über NFS, FTP oder HTTP) installieren möchten, müssen Sie eine Bootdiskette für die Netzwerkinstallation erstellen. Im *Offiziellen Red Hat Linux Installationshandbuch* ist das Erstellen einer solchen Diskette beschrieben.

- Wenn Sie noch nie zuvor mit dem Installationsprogramm im Textmodus gearbeitet haben, oder wenn Sie Ihre Kenntnisse zu dessen Benutzeroberfläche auffrischen möchten, lesen Sie den nächsten Abschnitt.
- Wenn Sie gleich mit der Installation beginnen möchten, fahren Sie fort mit Abschnitt 14.2, *Starten des Installationsprogramms*.

14.1 Die Benutzeroberfläche des Installationsprogramms

Das Installationsprogramm für Red Hat Linux im Textmodus verfügt über eine bildschirmorientierte Oberfläche mit Widgets (also GUI-Elementen), die Sie zum größten Teil bereits von anderen grafischen Benutzeroberflächen kennen. Abbildung 14–1, *Widgets des Installationsprogramms in* **TCP/IP konfigurieren** und Abbildung 14–2, *Widgets des Installationsprogramms in* Disk Druid zeigen die Bildschirme, die angezeigt werden.

Abbildung 14–1 Widgets des Installationsprogramms in TCP/IP konfigurieren

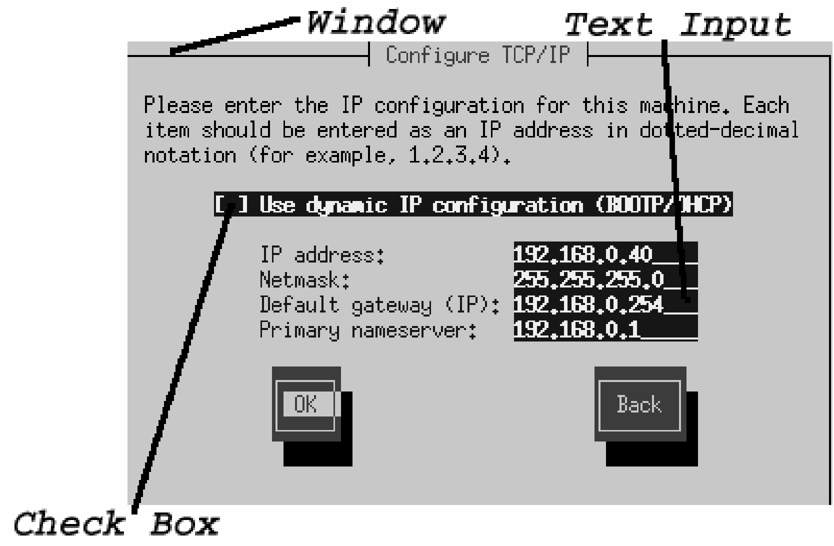
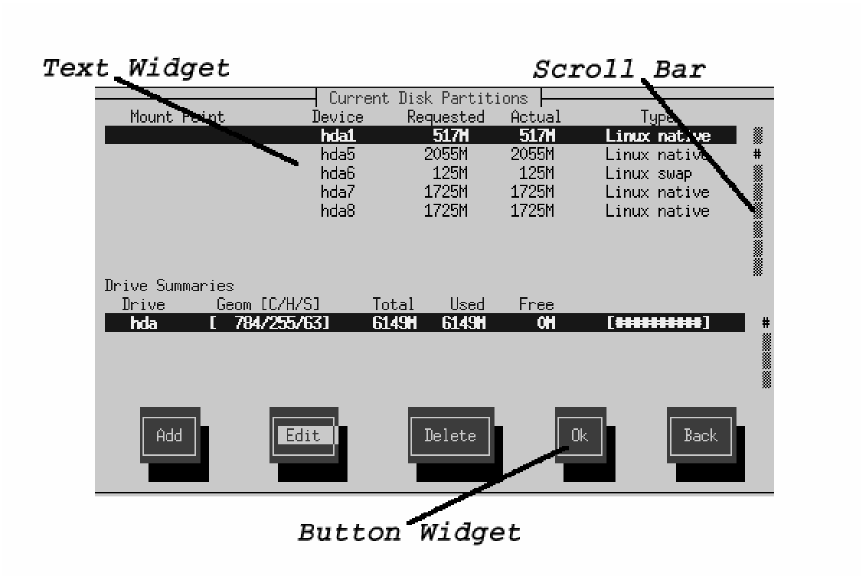


Abbildung 14–2 Widgets des Installationsprogramms in Disk Druid



Im Folgenden werden die wichtigsten der in Abbildung 14–1, *Widgets des Installationsprogramms in* **TCP/IP konfigurieren** und Abbildung 14–2, *Widgets des Installationsprogramms in* Disk Druid gezeigten Widgets vorgestellt:

- Fenster - Fenster (in diesem Handbuch meist als **Dialogfelder** bezeichnet) führen Sie durch den gesamten Installationsvorgang. Es kommt vor, dass sich zwei Fenster überlagern und Sie zunächst nur mit dem im Vordergrund angezeigten Fenster arbeiten können. Dieses "obere" Fenster wird geschlossen, und Sie können im anderen Fenster weiterarbeiten, sobald Sie die Eingaben für das obere Fenster abgeschlossen haben.
- Texteingabe - In die Texteingabezeilen geben Sie die für das Installationsprogramm relevanten Informationen ein. Zur Dateneingabe muss der Cursor in die Texteingabezeile gesetzt werden.
- Kontrollkästchen - Über die Kontrollkästchen können Sie einzelne Funktionen aktivieren oder deaktivieren. Im Kästchen erscheint ein Sternchen (aktiviert) oder

ein Leerzeichen (deaktiviert). Wenn sich der Cursor auf einem Kontrollkästchen befindet, können Sie dieses mit der [Leertaste] aktivieren bzw. deaktivieren.

- Text-Widget - Text-Widgets sind Bildschirmbereiche zur Anzeige von Text. Einige Text-Widgets enthalten selbst weitere Widgets, z.B. Kontrollkästchen. Eine Bildlaufleiste neben dem Text-Widget weist darauf hin, dass nicht alle Informationen auf einmal in das Textfenster passen. Wenn sich der Cursor innerhalb des Textfensters befindet, können Sie mit der [Nach-oben-Taste] und der [Nach-unten-Taste] alle verfügbaren Informationen anzeigen. Die aktuelle Position wird in der Bildlaufleiste mit dem Zeichen # gekennzeichnet. Je nachdem, wie Sie sich im Text bewegen, wird dieses Zeichen auf der Bildlaufleiste nach oben oder unten verschoben.

- Buttons - Buttons sind die wichtigsten Widgets zur Interaktion mit dem Installationsprogramm. Mit [Tabulatortaste] und [Eingabetaste] rufen Sie nach und nach alle Fenster des Installationsprogramms auf. Auf Buttons kann geklickt werden, wenn sie hervorgehoben dargestellt werden.

- Cursor - Der Cursor ist zwar selbst kein Widget, wird jedoch benötigt, um ein Widget auszuwählen bzw. mit einem Widget zu interagieren. Befindet er sich auf einem Widget, ändert sich möglicherweise die Farbe des entsprechenden Widgets, oder er wird einfach nur in oder neben dem Widget angezeigt. In Abbildung 14–1, *Widgets des Installationsprogramms in* **TCP/IP konfigurieren** befindet sich der Cursor auf dem Button **OK**. Abbildung 14–2, *Widgets des Installationsprogramms in* Disk Druid zeigt den Cursor auf dem Button **Edit**.

14.1.1 Navigieren mit der Tastatur

Sie können mit einigen einfachen Tastaturbefehlen in den Dialogfeldern des Installationsprogramms navigieren. Zum Bewegen des Cursors benutzen Sie die [Nach-links-Taste], die [Nach-rechts-Taste], die [Nach-oben-Taste] und die [Nach-unten-Taste]. Mit der [Tabulatortaste] und der Tastenkombination [Alt]-[Tabulatortaste] springen Sie zum jeweils nächsten oder vorigen Widget auf dem Bildschirm. In der Regel wird im unteren Bereich der einzelnen Bildschirme eine Übersicht der verfügbaren Tasten zum Positionieren des Cursors eingeblendet.

Um einen Button zu "drücken", positionieren Sie den Cursor auf dem Button (z.B. durch Verwenden der [Tabulatortaste]) und drücken die [Leertaste] oder die [Eingabetaste]. Um ein Element in einer Liste auszuwählen, bewegen Sie den Cursor auf das gewünschte Element und drücken die [Eingabetaste]. Sie aktivieren eine Funktion mit Hilfe der **Kontrollkästchen**, indem Sie den Cursor auf das entsprechende Kästchen bewegen und die [Leertaste] drücken. Drücken Sie die [Leertaste] erneut, um die Aktivierung rückgängig zu machen.

Durch Drücken von [F12] bestätigen Sie die aktuellen Werte und rufen das nächste Dialogfeld auf. Sie können hierfür auch auf den Button **OK** klicken.

ACHTUNG

Drücken Sie während des Installationsvorgangs keine Tasten, wenn Sie nicht dazu aufgefordert werden - es könnte unvorhersehbare Auswirkungen haben.

14.2 Starten des Installationsprogramms

Es gibt mehrere Möglichkeiten, um die Installation zu starten. Im Einzelnen stehen diese Methoden zur Verfügung:

- Legen Sie die Diskette, die in Ihrer Linux-Packung enthalten ist (oder eine von Ihnen erstellte PCMCIA- oder Netzwerk-Bootdiskette) in das erste Diskettenlaufwerk ein, und führen Sie einen Neustart durch.
- Wenn Ihr Computer von CD-ROM starten kann, legen Sie die Red Hat Linux CD-ROM in das Laufwerk ein und führen einen Neustart durch.
- Starten Sie MS-DOS, und führen Sie dann im Verzeichnis `dosutils` der Red Hat Linux CD-ROM das Programm `autoboot.bat` aus. (Diese Datei kann nur unter DOS ausgeführt werden. Die Ausführung in einem unter Windows gestarteten DOS-Fenster ist nicht möglich.)

Während das Installationsprogramm geladen wird, werden Meldungen auf dem Bildschirm angezeigt. Wenn das Installationsprogramm geladen ist, wird dieser Prompt angezeigt:

```
boot:
```

14.2.1 Anzeigen der Online-Hilfe

Sobald das Installationsprogramm in den Speicher geladen wurde, erhalten Sie Informationen zum Installationsvorgang und den entsprechenden Optionen durch Drücken der Funktionstasten [F1] bis [F6]. Drücken Sie z.B. [F2] für allgemeine Hinweise zu den Online-Hilfe-Bildschirmen.

14.2.2 Textmodus-Bootoptionen

Wenn Sie die [Eingabetaste] am Prompt `boot` drücken oder innerhalb der ersten Minute nach Anzeigen des Prompts `boot` keine Eingabe vornehmen, wird das grafische Installationsprogramm entsprechend der Beschreibung im *Offiziellen Red Hat Linux Installationshandbuch* gestartet. Um diese Automatik zu deaktivieren, drücken Sie die entsprechende Funktionstaste des Hilfebildschirms.

Zum Start des Textmodus-Installationsprogramms geben Sie vor dem Drücken der [Eingabetaste] diesen Bootbefehl ein:

```
boot: text
```

Wenn das Installationsprogramm die Hardware Ihres Systems nicht richtig erkennt, müssen Sie die Installation eventuell im "Expertenmodus" neu starten. In den Expertenmodus gelangen Sie über den folgenden Befehl:

```
boot: text expert
```

Im Expertenmodus ist die automatische Hardware-Erkennung größtenteils deaktiviert, und Sie haben die Möglichkeit, Treiber anzugeben, die während der Installation geladen werden sollen.

Bitte beachten

Die ersten Bootmeldungen verweisen nicht auf SCSI- oder Netzwerkkarten. Das ist normal. Diese Geräte werden durch Module unterstützt, die während des Installationsvorgangs geladen werden.

Beachten Sie, dass sich der Befehl zum Start einer seriellen Installation geändert hat. Wenn Sie die Installation im seriellen Modus ausführen müssen, geben Sie ein:

```
boot: linux console=<Gerät>
```

Hierbei gibt <*Gerät*> das Gerät an, das Sie verwenden (z.B. ttyS0 oder ttyS1).

Am Prompt boot können weitere Befehle eingegeben werden. Um den Kernel z.B. anzuweisen, in einem System mit 128 MB RAM den gesamten Speicher zu nutzen, geben Sie den folgenden Befehl ein:

```
boot: linux mem=128M
```

Um explizit ein Dialogfeld anzufordern, in dem Sie zusätzliche Geräte konfigurieren können (z.B. ISA-Geräte), müssen Sie ’isa’ in die Anweisung einfügen:

```
boot: linux isa
```

14.3 Auswählen einer Sprache

Wählen Sie mit der [Nach-oben-Taste] und der [Nach-unten-Taste] die gewünschte Sprache für das Installationsprogramm und die Standardeinstellung des Systems aus, und drücken Sie die [Eingabetaste] (Abbildung 14–3, *Auswählen einer Sprache*).

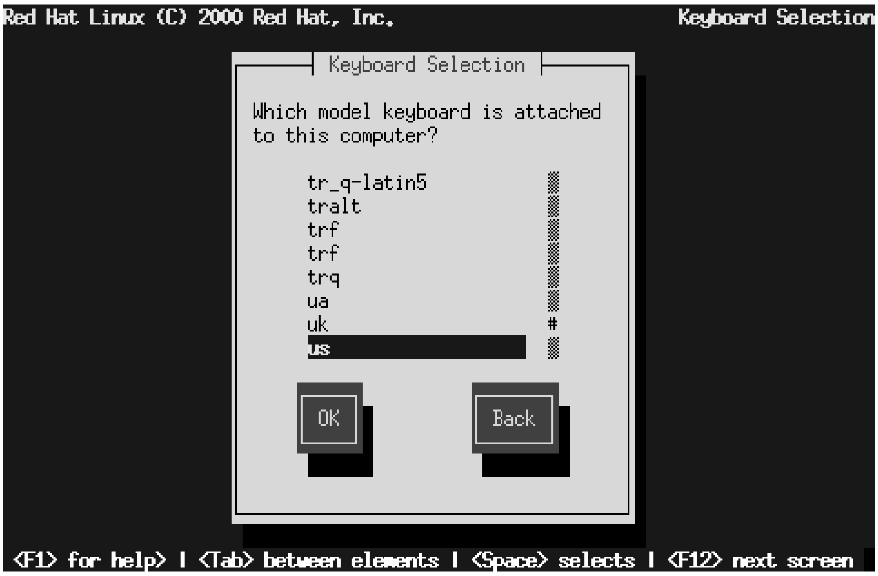
Abbildung 14–3 Auswählen einer Sprache

Eine Bildlaufleiste erscheint auf der rechten Seite der Liste. Sie weist darauf hin, dass nicht alle Einträge gleichzeitig angezeigt werden können. Solche Bildlaufleisten werden Ihnen während der Installation immer wieder begegnen.

14.4 Auswählen eines Tastaturtyps

Als Nächstes erhalten Sie die Möglichkeit, einen Tastaturtyp auszuwählen (Abbildung 14–4, *Auswählen eines Tastaturtyps*).

Abbildung 14–4 Auswählen eines Tastaturtyps



Drücken Sie nach Auswahl des gewünschten Tastaturtyps die [Eingabetaste]. Der Tastaturtyp wird nun jedesmal automatisch geladen, wenn Sie Ihr Red Hat Linux System starten. Er wird auch während des Installationsvorgangs verwendet.

Tipp

Wenn Sie den Typ Ihrer Tastatur nach der Installation Ihres Red Hat Linux-Systems ändern wollen, melden Sie sich als Root an und geben entweder `/usr/sbin/kbdconfig` oder `setup` ein.

14.5 Auswählen einer Installationsart

Wenn Sie das Installationsprogramm direkt von der Red Hat Linux CD-ROM gestartet haben, sehen Sie das Dialogfeld **Willkommen**: siehe Abschnitt 14.8, *Willkommen*.

Ist dies nicht der Fall, erscheint das Dialogfeld **Installationsmethode**. Die im Dialogfeld angezeigten Optionen sind abhängig von der Diskette, von der Sie das System gestartet haben (die Diskette aus der Linux-Packung oder eine von Ihnen erstellte Netzwerk- oder PCMCIA-Bootdiskette).

Abbildung 14–5, *Auswählen einer Installationsmethode* zeigt alle Auswahlmöglichkeiten.

Abbildung 14–5 Auswählen einer Installationsmethode

Bitte beachten

Wenn Sie eine Netzwerkinstallation durchführen und die Dateien von der Red Hat Linux CD-ROM oder einer FTP-Site kopieren, sollten Sie überprüfen, ob die Dateizugriffsrechte richtig festgelegt sind. Andernfalls können die kopierten Dateien nicht ausgeführt werden, und Sie müssen die Berechtigungen ändern, bevor Sie mit der Installation beginnen können.

Red Hat Linux kann mit einer der folgenden Methoden installiert werden:

Lokale CD-ROM

Sie haben das System von der Diskette gestartet, die in Ihrer Linux-Packung enthalten war, und führen die Installation mit der Red Hat Linux CD-ROM in einem lokalen Laufwerk durch. Wenn Sie diese Installationsmethode verwenden, wird als Nächstes das Dialogfeld **Willkommen** angezeigt: siehe Abschnitt 14.8, *Willkommen*.

NFS-Image

Sie haben das System von einer Netzwerk- oder PCMCIA-Bootdiskette gestartet und führen die Installation mit einem NFS-Image-Server durch, von dem der Inhalt der Red Hat Linux CD-ROM (oder eine Kopie davon) exportiert wird. Wenn Sie diese Methode wählen, erscheint als Nächstes das Dialogfeld **NFS-Setup**: siehe Abschnitt 14.7, *Installieren über ein Netzwerk*.

FTP

Sie haben das System von einer Netzwerk- oder PCMCIA-Bootdiskette gestartet und installieren direkt von einem FTP-Server. Wenn Sie diese Methode wählen, erscheint als Nächstes das Dialogfeld **FTP-Setup**: siehe Abschnitt 14.7, *Installieren über ein Netzwerk*.

HTTP

Sie haben das System von einer Netzwerk- oder PCMCIA-Bootdiskette gestartet und installieren direkt von einem HTTP-Web-Server. Wenn Sie diese Methode wählen, erscheint als Nächstes das Dialogfeld **HTTP-Setup**: siehe Abschnitt 14.7, *Installieren über ein Netzwerk*.

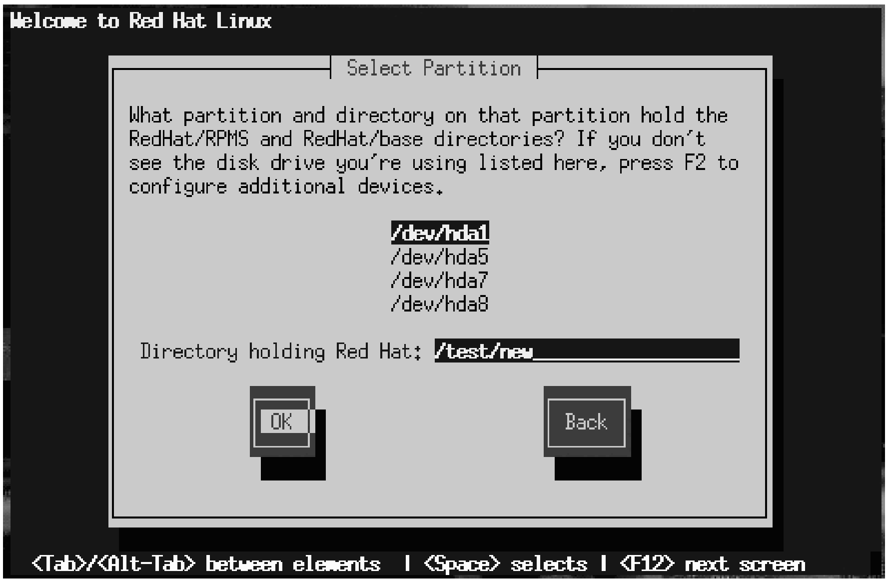
Festplatte

Sie haben das System von der in Ihrer Linux-Packung enthaltenen Diskette gestartet und führen die Installation mit den Red Hat Linux Dateien durch, die Sie zuvor auf eine lokale Festplatte kopiert haben. Wenn Sie diese Methode wählen, wird als Nächstes das Dialogfeld **Partition auswählen** angezeigt: siehe Abschnitt 14.6, *Festlegen der Festplattenpartition für die Installation*.

14.6 Festlegen der Festplattenpartition für die Installation

Der Bildschirm **Partition auswählen** (Abbildung 14–6, *Auswählen der Partition für die Installation von Festplatte*) wird nur angezeigt, wenn Sie die Installation von einer Festplattenpartition ausführen (d.h. Sie haben im Dialogfeld **Installationsmethode** die Option **Festplatte** ausgewählt. In diesem Dialogfeld können Sie die Festplattenpartition angeben, von der installiert werden soll.

Abbildung 14–6 Auswählen der Partition für die Installation von Festplatte



Geben Sie den Namen der Partition ein, auf der sich der Verzeichnisbaum `RedHat` befindet. Es gibt auch ein Feld mit der Bezeichnung **Verzeichnis, in dem sich Red Hat befindet**. Wenn sich das Verzeichnis `RedHat` nicht im Root-Verzeichnis befindet, geben Sie den Pfad zum Verzeichnis `RedHat` ein (wenn das Verzeichnis `RedHat` beispielsweise unter `/test/new/RedHat` installiert ist, geben Sie `/test/new`) ein.

Nachdem Sie die Festplattenpartition angegeben haben, wird als Nächstes das Dialogfeld **Willkommen** angezeigt: siehe Abschnitt 14.8, *Willkommen*.

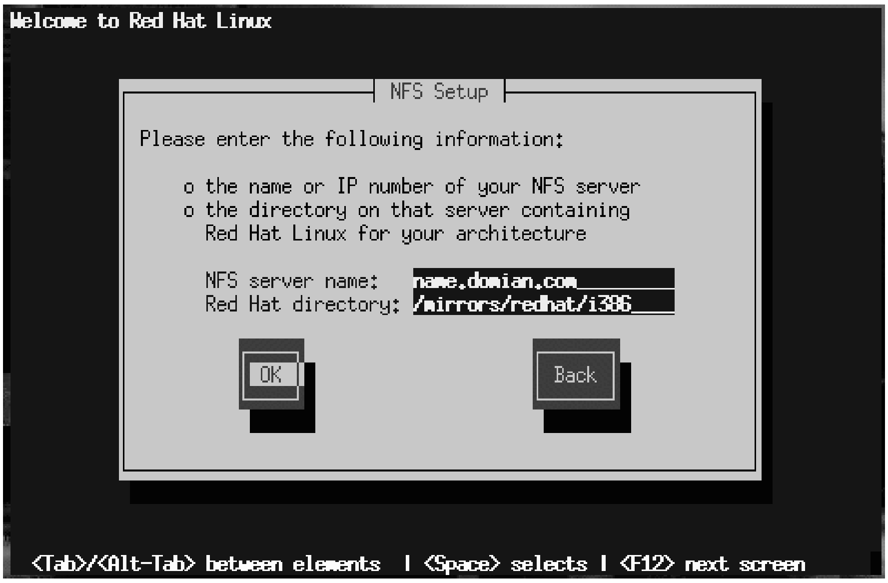
14.7 Installieren über ein Netzwerk

Wenn Sie eine Netzwerkinstallation durchführen, erscheint das Dialogfeld **TCP/IP konfigurieren**. Informationen hierzu finden Sie in Abschnitt 14.14, *Konfigurieren einer Netzwerkverbindung*. Kehren Sie danach hierher zurück.

14.7.1 NFS-Setup

Das Dialogfeld NFS-Setup (Abbildung 14–7, *Dialogfeld NFS-Setup*) wird nur angezeigt, wenn Sie die Installation von einem NFS-Server ausführen (d.h. Sie haben das System von einer Netzwerk- oder PCMCIA-Bootdiskette gestartet und im Dialogfeld **Installationsmethode** die Option **NFS Image** ausgewählt).

Abbildung 14–7 Dialogfeld NFS-Setup



Geben Sie den vollständigen Domänennamen oder die IP-Adresse des NFS-Servers sowie den Namen des exportierten Verzeichnisses ein, in dem sich die Installationsdateien oder die CD-ROM für Red Hat Linux befinden. Wenn Sie beispielsweise von einem Host mit der Bezeichnung `eastcoast` in der Domäne `redhat.com` installieren, geben Sie `eastcoast.redhat.com` im Feld **NFS-Server** ein.

Wenn auf dem NFS-Server die Red Hat Linux CD unter `/mnt/cdrom` gemountet ist, geben Sie `/mnt/cdrom` in das Feld **Red Hat Verzeichnis** ein. Exportiert der NFS-Server ein Image des Red Hat Linux Installationsbaums anstatt einer CD, geben Sie das Verzeichnis ein, das das Verzeichnis `RedHat` enthält. Befindet sich auf dem

NFS-Server beispielsweise das Verzeichnis `/mirrors/redhat/i386/RedHat`, geben Sie `/mirrors/redhat/i386` ein.

Bitte beachten

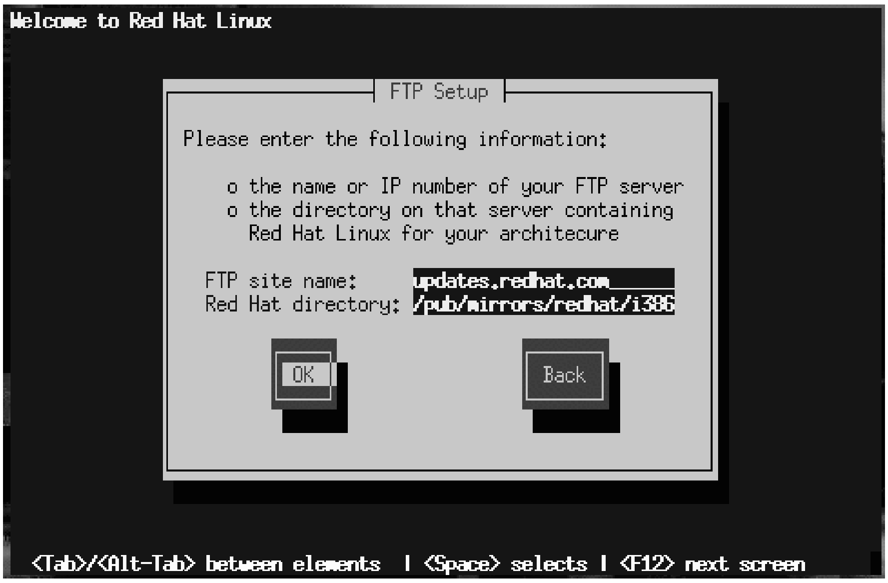
Wenn Sie eine NFS-Installation durchführen und die Dateien von der Red Hat Linux CD-ROM kopieren, sollten Sie überprüfen, ob die Dateizugriffsrechte richtig eingestellt sind. Andernfalls können die kopierten Dateien nicht ausgeführt werden, und Sie müssen die Berechtigungen ändern, bevor Sie mit der Installation beginnen können.

Als Nächstes wird das Dialogfeld **Willkommen** angezeigt: siehe Abschnitt 14.8, *Willkommen*.

14.7.2 FTP-Setup

Der Bildschirm **FTP-Setup** (Abbildung 14–8, *Dialogfeld FTP-Setup*) wird nur angezeigt, wenn Sie die Installation über einen FTP-Server durchführen (d.h. nur wenn im Dialogfeld **Installationsmethode** die Option **FTP** ausgewählt wurde). In diesem Dialogfeld können Sie den FTP-Server angeben, von dem installiert werden soll.

Abbildung 14–8 Dialogfeld FTP-Setup



Geben Sie den vollständigen Domänennamen oder die IP-Adresse der FTP-Site ein, von der installiert werden soll, sowie den Namen des Verzeichnisses, in dem sich die `RedHat`-Installationsdateien für Ihre Architektur befinden. Wenn die FTP-Site beispielsweise das Verzeichnis `/pub/mirrors/redhat/i386/RedHat` enthält, geben Sie **`/pub/mirrors/redhat/i386`** ein.

Wenn alle Angaben korrekt sind, erhalten Sie die Meldung, dass `base/hdlist` abgerufen wird.

Als Nächstes wird das Dialogfeld **Willkommen** angezeigt: siehe Abschnitt 14.8, *Willkommen*.

14.7.3 HTTP-Setup

Der Bildschirm **HTTP-Setup** (Abbildung 14–9, *Dialogfeld HTTP-Setup*) wird nur angezeigt, wenn Sie von einem HTTP-Server installieren (d.h. Sie haben im Dialogfeld **Installationsmethode** die Option **HTTP** ausgewählt). In diesem Dialogfeld werden die

Angaben zu dem HTTP-Server angefordert, der für die Installation verwendet werden soll.

Abbildung 14–9 Dialogfeld HTTP-Setup

Geben Sie den Namen oder die IP-Adresse des HTTP-Servers ein, von dem installiert werden soll, sowie den Namen des Verzeichnisses, in dem sich die `RedHat`-Installationsdateien für Ihre Architektur befindet. Wenn auf dem HTTP-Server beispielsweise das Verzeichnis `/pub/mirrors/redhat/i386/RedHat` angelegt wurde, geben Sie **`/pub/mirrors/redhat/i386`** ein.

Wenn alle Angaben korrekt sind, erhalten Sie die Meldung, dass `base/hdlist` abgerufen wird.

Als Nächstes wird das Dialogfeld **Willkommen** angezeigt: siehe Abschnitt 14.8, *Willkommen*.

14.8 Willkommen

Sobald Sie Sprache und Tastatur ausgewählt und die Installationsmethode festgelegt haben, erscheint Abbildung 14–10, *Dialogfeld Willkommen*. Wählen Sie **OK**, um fortzufahren.

Abbildung 14–10 Dialogfeld Willkommen

14.9 Aktualisieren oder installieren

Das Dialogfeld **Installationstyp** (Abbildung 14–11, *Dialogfeld Installationstyp*) bietet fünf Auswahlmöglichkeiten, die weiter unten beschrieben werden.

Abbildung 14–11 Dialogfeld Installationstyp

- **Workstation installieren** - Installation in einem System, das primär als Workstation verwendet wird. Laden Sie die GNOME-GUI (und/oder die KDE-GUI), und konfigurieren Sie das System, so dass GNOME (oder KDE) als Standard-Desktop geladen wird. Das Installationsprogramm löscht alle Daten in vorhandenen Linux-Partitionen, legt fest, wie die Festplatte für die neue Version partitioniert wird und welche Software-Pakete geladen werden.

WARNUNG

Wenn die Festplatte für Linux und Windows NT gemeinsam genutzt werden soll, dürfen Sie diese Methode nicht verwenden, da Windows NT sonst nicht mehr gestartet werden kann. LILO überschreibt den Bootloader von NT, und Sie können NT nicht mehr booten. Sie müssen eine benutzerdefinierte Installation durchführen und LILO so konfigurieren, dass er nicht im Master Boot Record (MBR) installiert wird.

Bei der Einrichtung einer Dual-Boot-Umgebung auf einem System, auf dem NT installiert ist, müssen Sie LILO statt im MBR im ersten Sektor der Root-Partition installieren. Sie müssen in diesem Fall unbedingt eine Bootdiskette erstellen. In diesem Fall müssen Sie zum Starten von Linux entweder eine Bootdiskette verwenden oder den Loader von Windows NT so konfigurieren, dass LILO vom ersten Sektor der Root-Partition gestartet wird. Weitere Informationen zum Einrichten von LILO und NT finden Sie unter http://www.linuxdoc.org/HOWTO/mini/Linux+NT-Loader.html. Bitte lesen Sie sich diese Informationen sorgfältig durch.

Im Folgenden ist aufgeführt, wie viel Festplattenplatz mindestens für eine Installation der Klasse Workstation erforderlich ist.

– Workstation mit GNOME - 900 MB
– Workstation mit KDE - 900 MB

  - Workstation mit GNOME und KDE - 1,1 GB

  Falls Sie vorhaben, alle Gruppenpakete (GNOME ist z.B. eine Paketgruppe) sowie alle zusätzlichen individuellen Pakete auszuwählen, sollten Sie dafür 1,7 GB oder mehr an Festplattenplatz vorsehen. Auf diese Weise steht Ihnen außerdem etwas Platz zum Schreiben von zusätzlichen Daten zur Verfügung.

- **Server-System installieren** - Installation auf einem System, das primär als Server genutzt werden soll. Das X Window System wird nicht konfiguriert, und beim Systemstart wird keine grafische Benutzeroberfläche gestartet. Das Installationsprogramm löscht *alle* Daten in *allen* vorhandenen Partitionen, legt fest, wie die Festplatte für die neue Version partitioniert wird und welche Software-Pakete geladen werden.

  Im Folgenden ist aufgeführt, wie viel Festplattenplatz mindestens für eine Installation der Klasse Server erforderlich ist.

  - Server (mindestens) - 450 MB
  - Server (alle Pakete) - 1 GB

  Falls Sie vorhaben, alle Gruppenpakete sowie zusätzliche individuelle Pakete auszuwählen, sollten Sie dafür 1,7 GB oder mehr an Festplattenplatz vorsehen. Auf diese Weise steht Ihnen außerdem etwas Platz zum Schreiben von zusätzlichen Daten zur Verfügung.

- **Benutzerdefiniertes System installieren** - Ermöglicht eine benutzerdefinierte Installation. Alle Entscheidungen bezüglich Festplattenpartitionierung und -initialisierung, Auswahl der zu installierenden Software-Pakete sowie Konfiguration von X Window System und Benutzeroberfläche werden von Ihnen getroffen.

  Im Folgenden ist aufgeführt, wie viel Festplattenplatz mindestens für eine Installation der Klasse Benutzerdefiniert erforderlich ist.

  - Benutzerdefiniert (mindestens) - 250 MB
  - Benutzerdefiniert (alles) - 1,7 GB

- **Vorhandene Installation aktualisieren** - Aktualisiert eine frühere Version von Red Hat Linux (3.0.3 oder später), ohne dass vorhandene Daten gelöscht werden. Das

Installationsprogramm aktualisiert den modularen Kernel der Version 2.2.x und alle bereits installierten Software-Pakete.

14.9.1 Aktualisieren

Wenn Sie Aktualisieren wählen und das Installationsprogramm mehr als eine installierte Linux-Version im System findet, werden Sie gefragt, welche Version aktualisiert werden soll. Wenn Sie dies angegeben haben, oder wenn nur eine installierte Linux-Version im System vorliegt, prüft das Installationsprogramm das vorhandene System, um festzustellen, welche Software-Pakete aktualisiert werden müssen. Daraufhin wird das Dialogfeld **Konfigurieren der zu aktualisierenden Pakete** (Abbildung 14–12, *Dialogfeld Konfigurieren der zu aktualisierenden Pakete*) geöffnet.

Abbildung 14–12 Dialogfeld Konfigurieren der zu aktualisierenden Pakete

Wenn Sie mit **Nein** antworten, beginnt das Installationsprogramm mit der Aktualisierung vorhandener Pakete.

Geben Sie **Ja** ein, wenn Sie in der Liste der zu aktualisierenden Pakete einzelne Pakete hinzufügen oder entfernen möchten. Das Dialogfeld Auswählen von Paketen finden

Sie in Abschnitt 14.20.1, *Auswählen von Einzelpaketen*. Sobald Sie alle Änderungen vorgenommen haben, wird die Aktualisierung gestartet.

Bitte beachten

Einige der aktualisierten Programmpakete funktionieren möglicherweise nur in Verbindung mit anderen Paketen. Der Aktualisierungsvorgang erkennt diese **Abhängigkeiten** und installiert gegebenenfalls die zusätzlichen Pakete.

Der Aktualisierungsvorgang sichert vorhandene Konfigurationsdateien durch Anhängen der Erweiterung `.rpmsave` (z.B. `sendmail.cf.rpmsave`) und protokolliert alle ausgeführten Aktionen in der Datei `/tmp/upgrade.log`. Da sich in neuen Software-Versionen auch die Formate der Konfigurationsdateien ändern können, sollten Sie die ursprünglichen Konfigurationsdateien mit den neuen Dateien vergleichen, bevor Sie diese in Ihr System integrieren.

Als Nächstes erscheint das Dialogfeld Abbildung 14–40, *Dialogfeld zur Anzeige des Installationsstatus*. Es wird so lange auf dem Bildschirm angezeigt, bis die Aktualisierung abgeschlossen ist.

14.10 Automatisches Partitionieren

Bei Auswahl einer Workstation- oder Server-Installation erscheint Abbildung 14–13, *Dialogfeld Automatisch Partitionieren*.

Abbildung 14–13 Dialogfeld Automatisch Partitionieren

Wenn Sie **Weiter** und dann **OK** wählen, partitioniert das Installationsprogramm Ihre Festplatte und legt fest, welche Software-Pakete installiert werden. Als Nächstes erscheint das Dialogfeld **Rechnername**, das in Abschnitt 14.13, *Benennen von Computern* beschrieben wird.

Wenn Sie **Manuell partitionieren** auswählen oder sich für eine benutzerdefinierte Installation entscheiden, wird Disk Druid gestartet. Es erscheinen die im nächsten Abschnitt beschriebenen Dialogfelder, in denen angezeigt wird, wie Ihre Festplatte zurzeit partitioniert ist. Sie entscheiden, welche Partitionen und Mount-Points für die Installation dieser Version von Red Hat Linux verwendet werden sollen.

ACHTUNG

Wenn Sie Red Hat Linux über eine bereits vorhandene Version von Linux (auch Red Hat Linux) installieren, werden alle Informationen (Dateien und Daten) der früheren Version überschrieben . Sichern Sie deshalb alle wichtigen Dateien! Falls Sie die in Ihrem Red Hat Linux System gespeicherten Daten beibehalten möchten, ohne ein eigenes Backup zu erstellen, sollten Sie eine Aktualisierung in Erwägung ziehen.

14.11 Partitionieren der Festplatte für Red Hat Linux

Wenn Sie noch nicht entschieden haben, wie Sie Ihre Partitionen einrichten möchten, fahren Sie mit Anhang B, *Eine Einführung in Festplattenpartitionen* fort. Dort finden Sie eine Einführung zu grundlegenden Festplatten-Partitionierungskonzepten. Als Mindestanforderung benötigen Sie eine ausreichend große Root-Partition und eine Swap-Partition von mindestens 16 MB.

Abbildung 14–14, *Dialogfeld Festplatte einrichten* zeigt die zwei Festplatten-Partitionierungsprogramme, die Sie verwenden können.

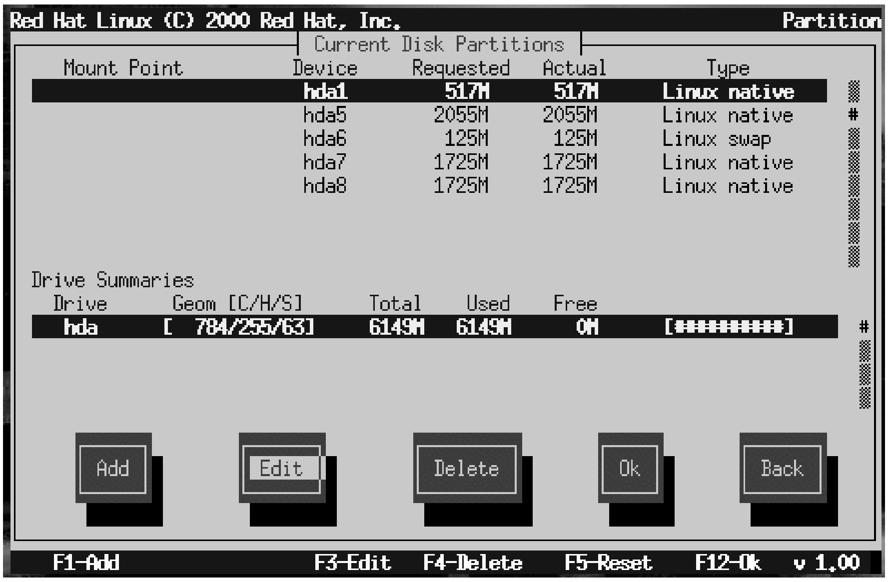
Wenn Sie zum Partitionieren Ihrer Festplatte fdisk verwenden wollen, finden Sie die entsprechende Anleitung in Abschnitt 14.11.12, *Arbeiten mit* fdisk. Wenn Sie sich für Disk Druid entscheiden, lesen Sie hier weiter.

Abbildung 14–14 Dialogfeld Festplatte einrichten

Die folgenden Abschnitte beschreiben den Aufbau Abbildung 14–15, *Hauptfenster von Disk Druid* und die Verwendung der Buttons zur Konfiguration der Partitionen. Wenn Sie mit Disk Druid bereits vertraut sind, können Sie Ihre Festplatte partitionieren und mit Abschnitt 14.11.11, *Dialogfeld Zu formatierende Partitionen auswählen* fortfahren.

Mit den Dialogfeldern zur Festplattenpartitionierung wird dem Installationsprogramm mitgeteilt, wo Red Hat Linux (Abbildung 14–15, *Hauptfenster von Disk Druid*) installiert werden soll.

Abbildung 14–15 Hauptfenster von Disk Druid



14.11.1 Der Bereich "Aktuelle Partitionen der Festplatte"

Jede Zeile in Bereich **Aktuelle Partitionen der Festplatte** steht für eine Festplattenpartition. In diesem Beispiel (Abbildung 14–15, *Hauptfenster von Disk Druid*) sind Linux-Partitionen vorhanden.

Die Bildlaufleiste rechts der Auflistung zeigt an, dass mehr Partitionen vorhanden sein können, als gleichzeitig auf dem Bildschirm angezeigt werden können. Mit der [Nach-oben-Taste] bzw. [Nach-unten-Taste] können Sie eventuell vorhandene weitere Partitionen anzeigen. Die einzelnen Zeilen sind in fünf Felder unterteilt:

- **Mount-Point** - Gibt an, wo die Partition bei der Installation von Red Hat Linux gemountet wird (z.B. `/`, `/boot` oder `swap`).
- **Gerät** - Zeigt spezifische Festplatten- und Partitionsinformationen an.
- **Angefordert** - Zeigt die ursprüngliche Größe der Partition an.
- **Tatsächlich** - Zeigt die tatsächliche Größe der Partition an.

- **Typ** - Gibt die Art der Partition an.

Beim Scrollen durch den Bereich **Aktuelle Partitionen der Festplatte** wird möglicherweise die Titelleiste `Nicht zugewiesene angeforderte Partitionen` angezeigt, unter der eine oder mehr Partitionen aufgelistet sind. Diese Partitionen sollten erstellt werden, es konnte ihnen jedoch aus verschiedenen Gründen kein Speicherplatz zugewiesen werden. Möglicherweise ist nicht genügend Speicherplatz verfügbar. Die Begründung für die nicht erfolgte Zuweisung wird nach dem Mount-Point der Partition angezeigt.

14.11.2 Der Bereich "Laufwerkszusammenfassungen"

Jede Zeile im Bereich **Laufwerkszusammenfassungen** steht für eine in Ihrem Computer installierte Festplatte und umfasst die folgenden Felder:

- **Laufwerk** - Zeigt den Namen der Festplatte an.
- **Geom [Z/K/S]** - Zeigt die **Geometrie** der Festplatte an. Die Geometrie ergibt sich aus drei Werten, nämlich der Anzahl der Zylinder, Köpfe und Sektoren, wie sie von der Festplatte übermittelt werden.
- **Gesamt** - Zeigt den insgesamt verfügbaren Speicherplatz auf der Festplatte an.
- **Verwendet** - Zeigt an, wie viel Platz den Partitionen auf der Festplatte aktuell zugewiesen ist.
- **Frei** - Zeigt an, wie viel Platz auf der Festplatte noch nicht zugewiesen ist.
- **Balkendiagramm** - Eine visuelle Darstellung des aktuell auf der Festplatte belegten Speicherplatzes. Je mehr Gatter-Zeichen zwischen den eckigen Klammern angezeigt werden, desto weniger freier Speicherplatz ist vorhanden. In Abbildung 14–15, *Hauptfenster von Disk Druid* ist der gesamte Platz auf der Festplatte belegt.

Bitte beachten

Der Bereich **Laufwerkszusammenfassungen** dient nur der Anzeige der Festplattenkonfiguration Ihres Computers. Hier können keine Festplatten für bestimmte Partitionen ausgewählt werden. Weiter gehende Informationen zum Auswählen von Festplatten finden Sie in Abschnitt 14.11.5, *Hinzufügen einer Partition*.

14.11.3 Buttons in Disk Druid

Mit den Buttons können Sie die Aktionen von Disk Druid steuern. Im Einzelnen können Partitionen hinzugefügt bzw. gelöscht sowie Attribute der Partitionen geändert werden. Darüber hinaus gibt es Buttons, mit denen Sie Ihre Eingaben bestätigen oder Disk Druid verlassen können. Im Folgenden werden die einzelnen Buttons erläutert.

- **Hinzufügen** - Dient zum Erstellen einer neuen Partition. Mit diesem Button wird ein Dialogfeld geöffnet, dessen Felder ausgefüllt werden müssen.
- **Bearbeiten** - Ändern des Mount-Points der Partition, die im Bereich **Aktuelle Partitionen der Festplatte** markiert ist. Mit diesem Button wird ein Dialogfeld geöffnet, in dem Sie den Namen des Mount-Points ändern können.
- **Löschen** - Löschen der markierten Partition im Bereich **Aktuelle Partitionen der Festplatte**. Sie müssen den Löschvorgang in einem Dialogfeld bestätigen.
- **OK** - Alle Änderungen an den Partitionen Ihres Systems werden auf die Festplatte geschrieben. Sie werden aufgefordert, die Änderungen zu bestätigen, bevor Disk Druid die Partitionstabellen der Festplatte überschreibt. Darüber hinaus werden alle definierten Mount-Points an das Installationsprogramm übergeben und von Ihrem Red Hat Linux System dazu verwendet, das Dateisystem anzulegen.
- **Zurück** - Abbrechen, ohne Änderungen zu speichern. Die vorherige Bildschirmanzeige wird durch Wählen dieses Buttons erneut aufgerufen, und Sie können von vorn beginnen.

14.11.4 Nützliche Funktionstasten

Mit der Funktionstaste [F5] (Zurücksetzen) werden alle Änderungen verworfen, die Sie während der Arbeit mit Disk Druid vorgenommen haben. Die Liste der Partitionen wird auf die ursprüngliche Liste zurückgesetzt, die der/den Partitionstabelle(n) Ihrer Festplatte(n) entnommen wurden. Sie werden aufgefordert, diesen Vorgang zu bestätigen. Beachten Sie, dass alle bereits erstellten Mount-Points verloren gehen und neu eingegeben werden müssen.

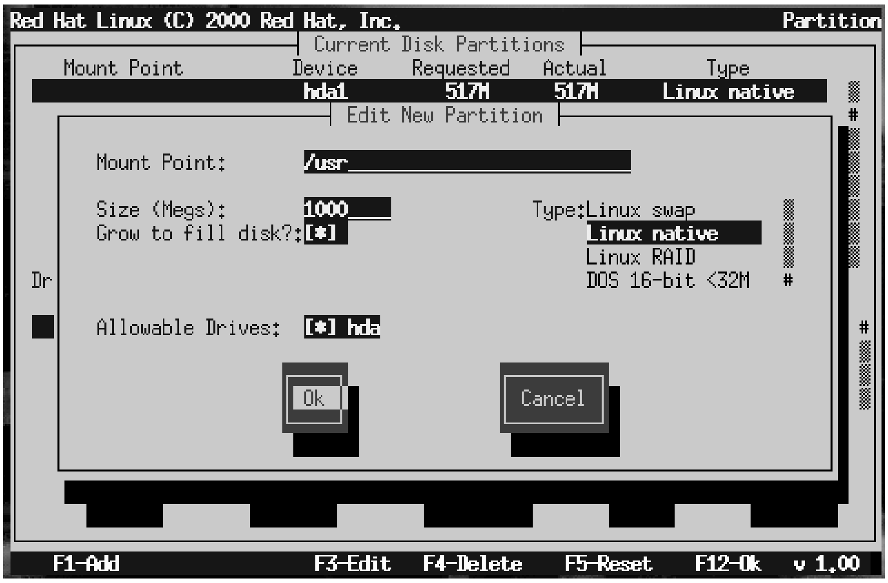
Bitte beachten

Sie müssen mindestens eine Partition (wahlweise auch mehrere) für Red Hat Linux reservieren. Weitere Informationen hierzu finden Sie in Abschnitt B.1.8, *Anzahl der Partitionen*.

14.11.5 Hinzufügen einer Partition

Um eine neue Partition hinzuzufügen, klicken Sie auf den Button **Hinzufügen** und drücken die [Leertaste] oder die [Eingabetaste]. Das Dialogfeld **Neue Partition bearbeiten** (Abbildung 14–16, *Dialogfeld Neue Partition bearbeiten*) wird aufgerufen.

Abbildung 14–16 Dialogfeld Neue Partition bearbeiten



Dieser Bildschirm enthält die folgenden Felder:

- **Mount-Point** - Markieren Sie dieses Feld, und geben Sie den Mount-Point für die Partition ein. Geben Sie z.B. für eine Root-Partition `/` für die Partition `/usr` `/usr` ein und so weiter.
- **Größe (in MB)** - Geben Sie hier die Größe der Partition in Megabyte ein. In diesem Feld ist bereits eine "1" vorgegeben, d.h. Sie legen eine Partition von 1 MB an, wenn Sie diesen Wert nicht ändern. Sie können den Wert mit der [Rücktaste] löschen und die gewünschte Partitionsgröße eingeben.
- **An Kapazität der Festplatte anpassen?** - Hier legen Sie fest, ob die eingegebene Größe als exakte Größe oder als Mindestgröße zu betrachten ist. Drücken Sie die [Leertaste], um diese Option auszuwählen. Wenn das Kontrollkästchen markiert ist, kann die Partition so weit wachsen, bis sie den gesamten verfügbaren Platz auf der Festplatte einnimmt. Ihre Größe ist variabel und hängt davon ab, wie Sie die anderen Partitionen festlegen. Sie können mehrere Partitionen gleichzeitig

variabel machen. Der freie Speicherplatz auf der Festplatte wird dann zwischen allen variablen Partitionen aufgeteilt.

- **Typ** - Enthält eine Liste verschiedener Partitionstypen. Wählen Sie den gewünschten Partitionstyp mit der [Nach-oben-Taste] bzw. [Nach-unten-Taste] aus.
- **Verfügbare Laufwerke** - Enthält eine Liste der in Ihrem System installierten Festplatten mit jeweils einem Kontrollkästchen. Wenn das Kontrollkästchen einer Festplatte aktiviert ist, kann eine Partition darauf erstellt werden. Über die Kontrollkästchen können Sie Disk Druid anweisen, wo Partitionen anzulegen sind oder aber die Entscheidung Disk Druid überlassen.
- **OK** - Klicken Sie auf diesen Button, und drücken Sie die [Leertaste], wenn Sie die Partition mit den festgelegten Parametern anlegen möchten.
- **Abbrechen** - Klicken Sie auf diesen Button, und drücken Sie die [Leertaste], wenn die Partition nicht erstellt werden soll.

14.11.6 Empfohlenes Partitionierungsschema

Sie sollten im Normalfall die folgenden Partitionen erstellen (es sei denn, Sie haben besondere Gründe für eine abweichende Partitionierung):

- Eine Swap-Partition (mindestens 16 MB) - Swap-Partitionen dienen zur Unterstützung des **virtuellen Speichers**. Dies bedeutet, dass die Daten in eine Swap-Partition geschrieben werden, wenn nicht ausreichend RAM zum Speichern der Daten vorhanden ist, die Ihr System gerade verarbeitet. Falls Ihr Computer über 16 MB RAM oder weniger verfügt, *müssen* Sie eine Swap-Partition erstellen. Auch wenn Sie mehr Speicher zur Verfügung haben, empfiehlt sich eine Swap-Partition. Die Mindestgröße der Swap-Partition sollte der Größe des Arbeitsspeichers des Computers bzw. 16 MB entsprechen (der jeweils größere Wert sollte verwendet werden). In Disk Druid sollte das Partitionsfeld für `swap` etwa wie folgt aussehen:

  ```
  <Swap>  hda2  125M   125M  Linux swap
  ```

- Eine `/boot`-Partition (maximal 16 MB) - Die in `/boot` eingebundene Partition enthält den Betriebssystem-Kernel (der erforderlich ist, damit Ihr System Red

Hat Linux booten kann) sowie Dateien, die während des Systemstarts verwendet werden. Wegen der Einschränkungen der meisten PC-BIOS-Versionen sollten Sie zur Aufnahme dieser Dateien nur eine kleine Partition erstellen. Sie sollte nicht größer als 16 MB sein. In Disk Druid sollte das Partitionsfeld für `/boot` etwa wie folgt aussehen:

```
/boot  hda1  16M   19M  Linux native
```

- Eine `root`-Partition (900 MB - 1,7 GB) - In dieser Partition befindet sich "`/`" (das Root-Verzeichnis). In dieser Konfiguration befinden sich alle Dateien (mit Ausnahme der in `/boot` gespeicherten Dateien) in der Root-Partition. Eine Root-Partition von 850 MB erlaubt den Umfang einer Workstation-Installation (mit *sehr* wenig freiem Festplattenspeicher), während Sie auf einer Root-Partition von 1,7 GB alle Pakete installieren können. In Disk Druid sollte das Partitionsfeld für `/` etwa wie folgt aussehen:

```
/  hda2  900M   3669M   Linux native
```

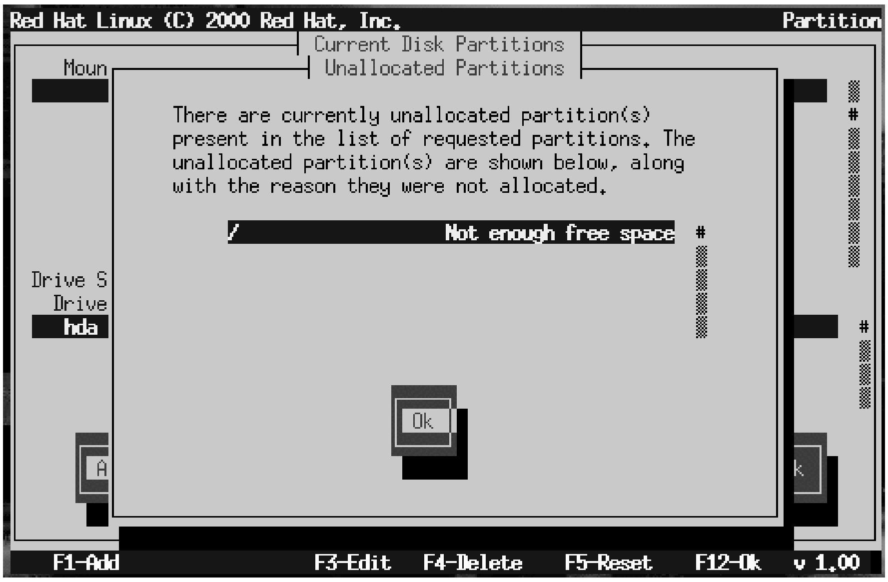
14.11.7 Probleme beim Hinzufügen von Partitionen

Bitte beachten

Wenn beim Hinzufügen von Partitionen Probleme auftreten, finden Sie in Anhang B, *Eine Einführung in Festplattenpartitionen* hilfreiche Informationen.

Wenn Disk Druid die von Ihnen gewünschte Partition nicht anlegen kann, wird ein Dialogfeld wie in Abbildung 14–17, *Dialogfeld Nicht zugewiesene Partitionen* angezeigt. Es enthält eine Liste aller Partitionen, denen noch kein Speicherplatz zugewiesen wurde, sowie eine Begründung für die nicht erfolgte Zuweisung. Klicken Sie auf den Button **OK**, und drücken Sie die [Leertaste], um fortzufahren. Beachten Sie, dass die nicht zugewiesenen Partitionen ebenfalls auf dem Disk Druid Hauptbildschirm angezeigt werden (möglicherweise müssen Sie im Bereich **Aktuelle Partitionen der Festplatte** scrollen, um sie zu sehen).

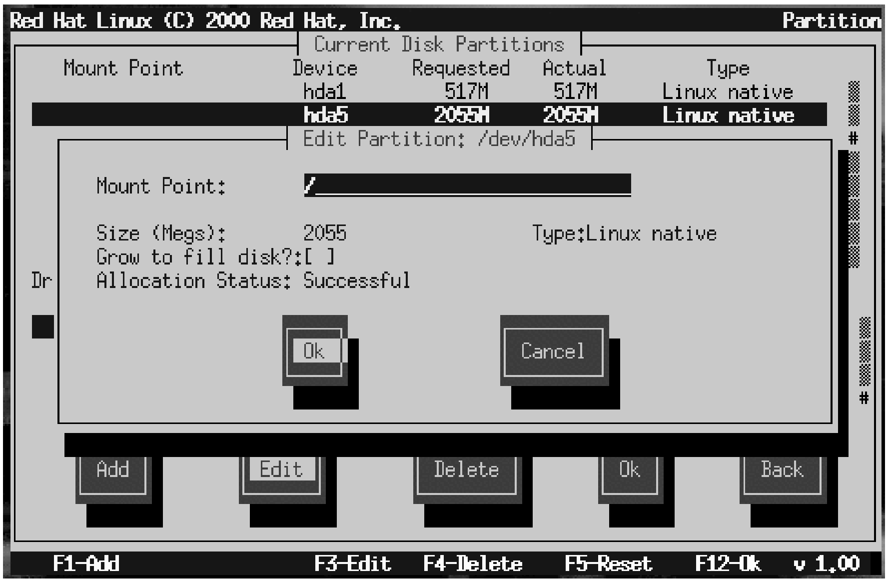
Abbildung 14–17 Dialogfeld Nicht zugewiesene Partitionen



14.11.8 Bearbeiten von Partitionen

Um den Mount-Point für eine Partition zu ändern, markieren Sie die Partition im Bereich **Aktuelle Partitionen der Festplatte**, wählen den Button **Bearbeiten** und drücken die [Leertaste]. Das Dialogfeld **Partition bearbeiten** ähnelt dem in Abbildung 14–16, *Dialogfeld Neue Partition bearbeiten*, mit dem Unterschied, dass mit Ausnahme von Mount-Point alle Felder schreibgeschützt sind. Wenn Sie einen der anderen Parameter ändern möchten, löschen Sie die Partition, und fügen Sie eine neue Partition mit den gewünschten Werten hinzu.

Abbildung 14–18 Dialogfeld Partition bearbeiten



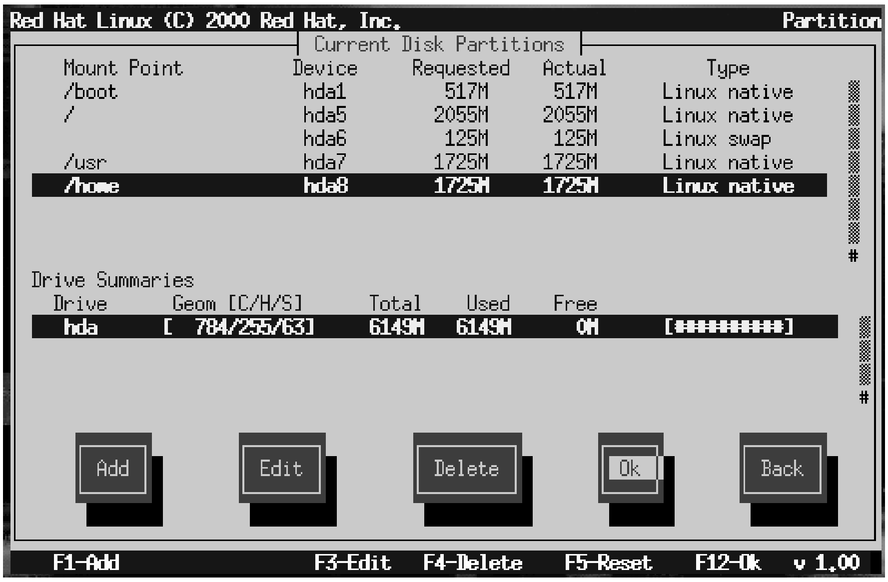
14.11.9 Löschen von Partitionen

Um eine Partition zu löschen, markieren Sie diese im Bereich **Aktuelle Partitionen der Festplatte**, wählen den Button **Löschen** und drücken die [Leertaste]. Sie werden aufgefordert, den Löschvorgang zu bestätigen.

14.11.10 Wenn Sie fertig sind

Wenn Sie die Konfiguration der Partitionen und das Eingeben der Mount-Points abgeschlossen haben, sollte Ihr Bildschirm in etwa dem in Abbildung 14–19, *Dialogfeld Aktuelle Partitionen der Festplatte* entsprechen.

Abbildung 14–19 Dialogfeld Aktuelle Partitionen der Festplatte



14.11.11 Dialogfeld Zu formatierende Partitionen auswählen

Wählen Sie dann die zu formatierenden Partitionen aus (Abbildung 14–20, *Auswählen der zu formatierenden Partitionen*). Sie müssen alle neu erstellten Partitionen sowie andere Partitionen mit alten Daten formatieren (vorausgesetzt, diese enthalten keine Daten, die Sie erhalten wollen).

Abbildung 14–20 Auswählen der zu formatierenden Partitionen

ACHTUNG

Wählen Sie keine bereits vorhandenen Partitionen wie `/home` oder `/usr/local` zum Formatieren aus, die Daten enthalten, die Sie erhalten wollen.

Wählen Sie die zu formatierenden Partitionen aus, und drücken Sie die [Leertaste]. Wenn das Dateisystem während der Formatierung auf defekte Blöcke überprüft werden soll (empfehlenswert für ältere Festplatten), aktivieren Sie das Kontrollkästchen **Beim Formatieren auf defekte Blöcke überprüfen**. Klicken Sie auf **OK**, und drücken Sie die [Leertaste].

Bitte beachten

Durch die Funktion **Beim Formatieren auf defekte Blöcke überprüfen** kann sich die für die Installation benötigte Gesamtzeit deutlich erhöhen. Da die meisten neueren Festplatten recht groß sind, kann die Überprüfung auf defekte Blöcke je nach der Größe Ihrer Festplatte eine gewisse Zeit dauern.

14.11.12 Arbeiten mit fdisk

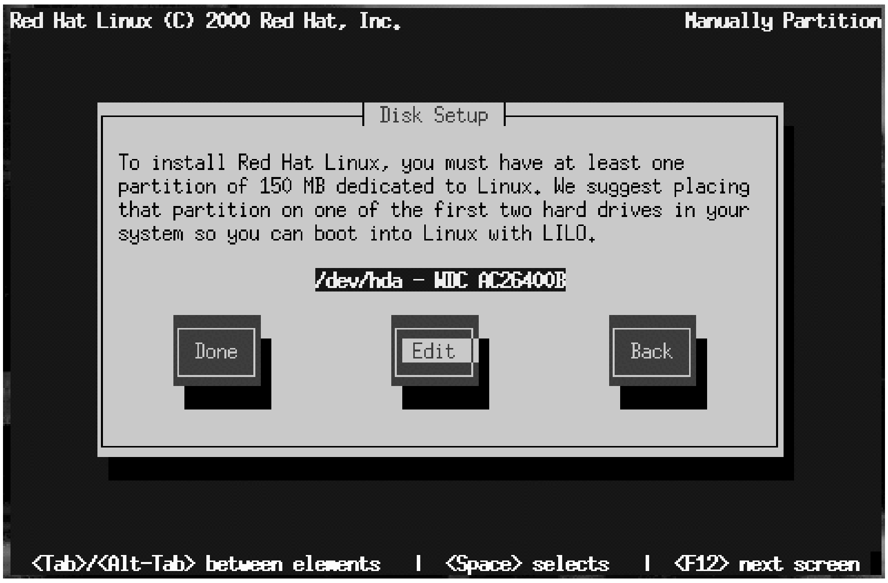
Wenn Sie eine benutzerdefinierte Installation auswählen, können Sie auch das zu verwendende Partitionierungsprogramm auswählen. Lesen Sie diesen Abschnitt nur durch, wenn Sie sich für fdisk entschieden haben.

Wenn Sie sich für fdisk entschieden haben, wird das Dialogfeld **Datenträger partitionieren** aufgerufen (Abbildung 14–21, *Dialogfeld Festplatte einrichten*). Es enthält eine Liste aller Festplatten in Ihrem Computer.

Markieren Sie mit der [Tabulatortaste], der [Nach-oben-Taste] und der [Nach-unten-Taste] die Festplatte, die formatiert werden soll, klicken Sie auf **Bearbeiten**, und drücken Sie die [Leertaste].

Es wird fdisk gestartet, und Sie können die ausgewählte Festplatte partitionieren. Wiederholen Sie diesen Vorgang für jede Festplatte, die Sie partitionieren möchten. Klicken Sie zum Schluss auf **Fertig**.

Abbildung 14–21 Dialogfeld Festplatte einrichten



Überblick über fdisk

fdisk verfügt über eine knappe, aber nützliche Online-Hilfe. Hier einige Tipps:

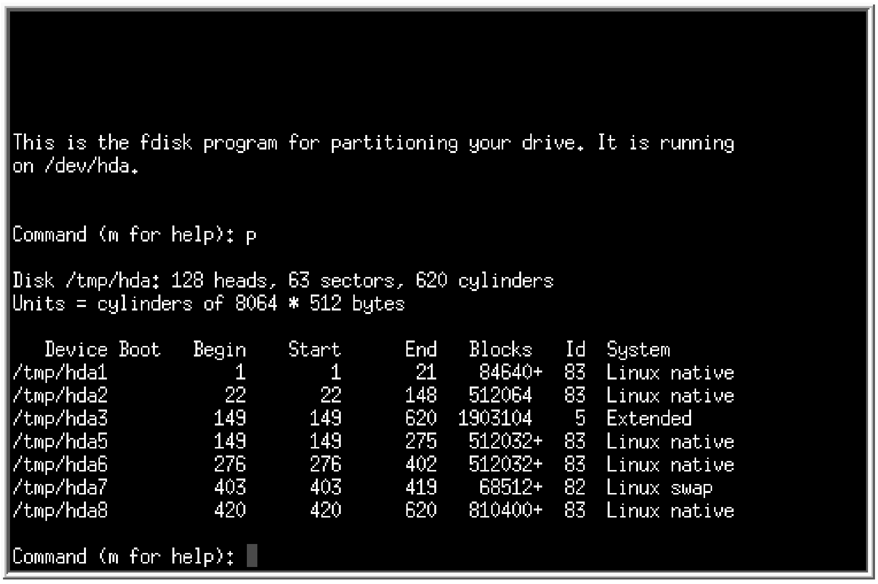
- Mit dem Befehl `m` rufen Sie die Hilfe auf.
- Der Befehl `p` listet die aktuelle Partitionstabelle auf (siehe Abbildung 14–22, *Beispielausgabe von* fdisk).
- Mit `n` fügen Sie eine neue Partition hinzu.
- Linux fdisk erstellt standardmäßig Partitionen des Typs **Linux native**. Wenn Sie eine Swap-Partition anlegen, vergessen Sie nicht, sie mit Hilfe des Befehls `t` in den Typ **Linux swap** umzuwandeln. Der Wert für den Typ **Linux swap** ist `82`. Andere Partitionstypen und die zugehörigen Werte können mit dem Befehl `l` angezeigt werden.

- Linux unterstützt bis zu vier (4) Partitionen auf einer Festplatte. Wenn Sie mehr als vier Partitionen anlegen möchten, kann eine (und nur eine) der vier Partitionen eine **erweiterte** Partition sein, die als Container-Partition für eine oder mehr **logische** Partitionen dient. Die Container-Partition muss mindestens so groß sein wie alle darin enthaltenen logischen Partitionen zusammen.
- Es empfiehlt sich, bei der Partitionierung zu notieren, welche Partitionen (z.B. `/dev/hda2`) für welche Dateisysteme (z.B. `/usr`) vorgesehen sind.

Bitte beachten

Die Änderungen treten erst in Kraft, wenn Sie die Eingaben speichern und fdisk mit dem Befehl `w` verlassen. Mit dem Befehl `q` können Sie fdisk jederzeit ohne Speichern der Änderungen beenden.

Abbildung 14–22 Beispielausgabe von fdisk



```
This is the fdisk program for partitioning your drive. It is running
on /dev/hda.


Command (m for help): p

Disk /tmp/hda: 128 heads, 63 sectors, 620 cylinders
Units = cylinders of 8064 * 512 bytes

   Device Boot   Begin    Start      End   Blocks   Id  System
/tmp/hda1            1        1       21    84640+  83  Linux native
/tmp/hda2           22       22      148   512064   83  Linux native
/tmp/hda3          149      149      620  1903104    5  Extended
/tmp/hda5          149      149      275   512032+  83  Linux native
/tmp/hda6          276      276      402   512032+  83  Linux native
/tmp/hda7          403      403      419    68512+  82  Linux swap
/tmp/hda8          420      420      620   810400+  83  Linux native

Command (m for help):
```

Ändern der Partitionstabelle

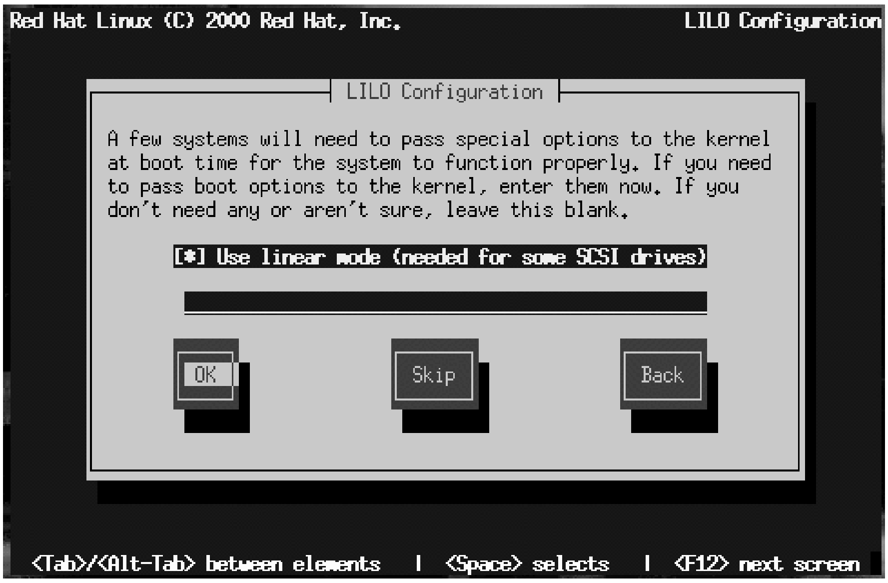
Klicken Sie auf den Button **Fertig**, wenn Sie die Partitionierung Ihrer Festplatten abgeschlossen haben. In einer Meldung wird Ihnen eventuell mitgeteilt, dass das Installationsprogramm neu gestartet werden muss. Das ist normal, wenn Partitionsdaten einer Festplatte geändert wurden, d.h. wenn Sie erweiterte Partitionen erstellt, geändert oder gelöscht haben. Klicken Sie auf **OK**, um den Rechner neu zu starten und die Installation neu zu beginnen. Führen Sie dann die gleichen Installationsschritte bis zum Dialogfeld **Datenträger partitionieren** aus, und klicken Sie auf **Fertig**.

14.12 Installieren von LILO

Im `LI`nux `LO`ader (LILO) können Sie beim Booten angeben, ob Linux oder ein anderes Betriebssystem gestartet werden soll. (Bei einer Workstation- oder Server-Installation wird LILO automatisch im Master Boot Record [MBR] installiert.) Wenn Sie eine benutzerdefinierte Installation durchführen, können Sie in den Dialogfeldern **LILO installieren** festlegen, wie und ob LILO installiert werden soll.

Im Dialogfeld **LILO konfigurieren** (Abbildung 14–23, *Dialogfeld LILO konfigurieren*) können Sie Standardoptionen zum LILO-Bootbefehl hinzufügen. Die Optionen, die Sie eingeben, werden bei jedem Bootvorgang an den Linux-Kernel übergeben.

Abbildung 14–23 Dialogfeld LILO konfigurieren



In Abschnitt 13.1.1, *Grundlegende Hardware-Konfiguration* wurden Sie aufgefordert, die BIOS-Einstellungen Ihres Computers zu überprüfen. Wenn Sie festgestellt haben, dass der Computer auf eine Festplatte nicht im linearen Modus zugreift, müssen Sie diese Option deaktivieren. **Linearen Modus verwenden** ist standardmäßig aktiviert. Klicken Sie auf **OK**, und drücken Sie die [Leertaste], um fortzufahren.

Klicken Sie auf **Überspringen**, wenn Sie LILO nicht installieren wollen.

WARNUNG

Wenn Sie Überspringen wählen, können Sie Ihr Red Hat Linux System nicht direkt starten und müssen auf andere Weise booten, z.B. mit einer Bootdiskette. Verwenden Sie diese Option nur, wenn Sie wissen, wie Sie Ihr Red Hat Linux System auf andere Weise booten können!

14.12.1 Alternativen zu LILO

Wenn Sie Ihr Red Hat Linux System nicht mit LILO booten möchten, gibt es mehrere Alternativen:

Bootdiskette

Sie können die vom Installationsprogramm erstellte Bootdiskette verwenden (falls Sie eine erstellt haben).

LOADLIN

LOADLIN kann Linux von MS-DOS aus laden. Allerdings wird dazu eine auf einer MS-DOS-Partition verfügbare Kopie des Linux-Kernels benötigt (und eine initiale Ramdisk, sofern Sie über einen SCSI-Adapter verfügen). Diese Kopie können Sie nur erstellen, indem Sie das Red Hat Linux System mit einem anderen Verfahren starten (z.B. von LILO auf einer Diskette) und anschließend den Kernel in eine MS-DOS-Partition kopieren. LOADLIN können Sie von der Site ftp://metalab.unc.edu/pub/Linux/system/boot/dualboot/ und zugehörigen Mirror Sites herunterladen.

SYSLINUX

SYSLINUX ist ein MS-DOS-Programm, das LOADLIN sehr ähnlich ist. Sie können es ebenfalls von der Site ftp://metalab.unc.edu/pub/Linux/system/boot/loaders/ und zugehörigen Mirror Sites herunterladen.

Kommerzielle Bootloader

Einige kommerzielle Bootloader können Linux zwar booten, erfordern aber dennoch, dass LILO in Ihrer Linux-Root-Partition installiert ist.

14.12.2 LILO konfigurieren

Wählen Sie, wo LILO installiert werden soll (Abbildung 14–24, *Dialogfeld LILO konfigurieren*).

Abbildung 14–24 Dialogfeld LILO konfigurieren

Sie können LILO an einem von zwei Orten installieren:

WARNUNG

Bei der Einrichtung einer Dual-Boot-Umgebung auf einem System, auf dem NT installiert ist, müssen Sie LILO statt im MBR im ersten Sektor der Root-Partition installieren. Sie müssen in diesem Fall unbedingt eine Bootdiskette erstellen. In diesem Fall müssen Sie zum Starten von Linux entweder eine Bootdiskette verwenden oder den Loader von Windows NT so konfigurieren, dass LILO vom ersten Sektor der Root-Partition gestartet wird. Weitere Informationen zum Einrichten von LILO und NT finden Sie unter http://www.linux-doc.org/HOWTO/mini/Linux+NT-Loader.html. Bitte lesen Sie sich diese Informationen sorgfältig durch.

Der Master Boot Record (MBR)

Es empfiehlt sich, LILO im MBR zu installieren, sofern sich hier nicht bereits der Loader eines anderen Betriebssystems befindet, z.B. System Commander oder der Boot-Manager von OS/2. Der Master Boot Record ist ein spezieller Bereich auf der Festplatte, der vom BIOS Ihres Computers automatisch geladen wird. Dies ist der früheste Zeitpunkt, ab dem LILO die Steuerung des Bootprozesses übernehmen kann. Wenn Sie LILO im MBR installieren, zeigt LILO beim Booten Ihres Rechners den Prompt `boot:` ein. Sie können dann entweder Red Hat Linux oder ein beliebiges anderes Betriebssystem starten, für das Sie LILO konfigurieren.

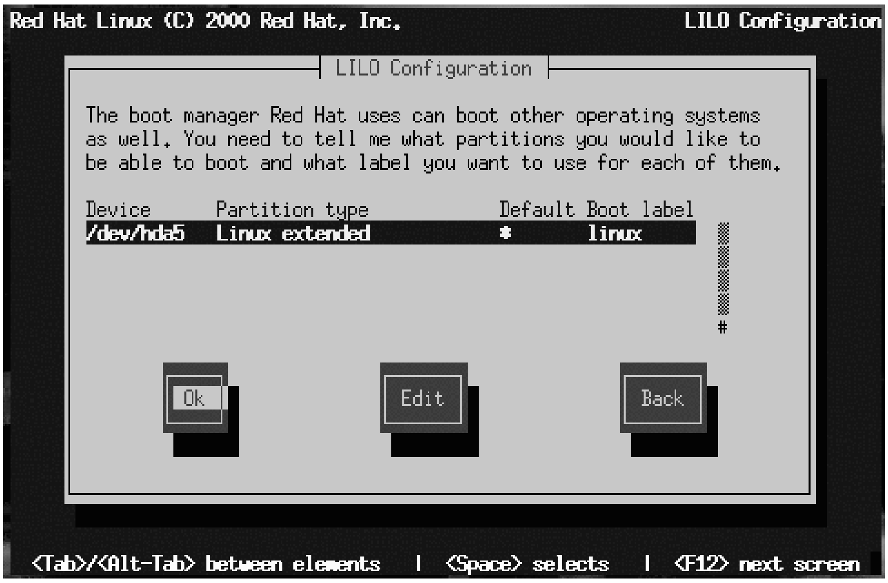
Der erste Sektor der Boot-Partition

Der empfohlene Installationsort, wenn bereits ein anderer Bootloader in Ihrem System verwendet wird (z.B. der Boot-Manager von OS/2). In diesem Fall übernimmt zunächst der andere Bootloader die Steuerung. Sie können diesen Bootloader dann zum Booten von LILO konfigurieren (LILO wiederum startet Red Hat Linux).

Wählen Sie den Ort aus, an dem Sie LILO installieren möchten, und klicken Sie auf **OK**.

Zuletzt können Sie im Installationsprogramm das Standardbetriebssystem festlegen und Bootkennungen angeben, siehe Abbildung 14–25, *Auswählen bootbarer Partitionen im Dialogfeld LILO konfigurieren*.

Abbildung 14–25 Auswählen bootbarer Partitionen im Dialogfeld LILO konfigurieren



Jede bootbare Partition wird aufgelistet, einschließlich der Partitionen, die von anderen Betriebssystemen verwendet werden. In die Spalte **Bootkennung** wird das Wort `linux` neben der Partition eingefügt, die das Root-Dateisystem des Red Hat Linux Systems enthält. Andere Partitionen sind möglicherweise auch durch Bootkennungen gekennzeichnet (z.B. durch die Bootkennung `dos` für Windows 95/98-Partitionen).

Um eine Bootkennung für eine Partition hinzuzufügen (oder eine vorhandene Bootkennung zu ändern), markieren Sie die gewünschte Partition mit den Pfeiltasten. Verwenden Sie dann die [Tabulatortaste], um den Button **Bearbeiten** auszuwählen, und drücken Sie die [Leertaste]. Nun wird ein kleines Dialogfeld angezeigt, in dem Sie die Bootkennung der Partition eingeben bzw. ändern können. Klicken Sie auf **OK**, wenn Sie fertig sind.

Tipp

Der Inhalt der Spalte **Bootkennung** entspricht dem, was Sie am LILO-Prompt `boot:` eingeben müssen, um das gewünschte Betriebssystem zu booten. Sollten Sie die in Ihrem System definierten Bootkennungen vergessen haben, drücken Sie am LILO-Prompt `Boot:` die [Tabulatortaste], um eine Liste der definierten Bootkennungen anzuzeigen.

Eine weitere Spalte trägt den Titel **Standard**. Nur eine Partition ist in dieser Spalte durch einen Stern gekennzeichnet. Das ist die Standardpartition, die von LILO gebootet wird, wenn während des Bootprozesses keine Eingabe durch den Benutzer erfolgt. Zunächst wird die Root-Partition Ihrer Red Hat Linux Installation als Standardpartition ausgewählt. Wenn Sie diese Voreinstellung ändern möchten, können Sie die Partition, die Sie standardmäßig verwenden möchten, mit Hilfe der Cursortasten hervorheben. Drücken Sie anschließend [F2]. Der Stern wird nun an der ausgewählten Partition angezeigt. Wählen Sie dann **OK** , und drücken Sie die [Leertaste].

14.12.3 SMP-Mainboards und LILO

Wenn das Installationsprogramm ein Mainboard für mehrere Prozessoren (SMP) in Ihrem System erkennt, erstellt es automatisch zwei `lilo.conf`-Einträge: `linux`, der Standardeintrag, startet das System im SMP-Modus, und `linux-up` startet das System im Einzelprozessormodus.

14.13 Benennen von Computern

Das Dialogfeld **Konfiguration des Rechnernamens** fordert Sie auf, einen Namen für Ihren Computer einzugeben (der sog. **Hostname**).

Abbildung 14–26 Dialogfeld Konfiguration des Rechnernamens

Wenn Ihr Computer mit einer Netzwerkkarte ausgestattet ist, geben Sie einen **vollständigen Domänennamen** in diesem Format ein:

`Rechnername.Domänenname`

In diesem Beispiel ist *`Rechnername`* der Name, den Sie für Ihren Computer gewählt haben, und *`Domänenname`* ist die TCP/IP-Domäne. (Ein Domänenname kann mehrere Knoten enthalten: z.B. *eastcoast.mainserver.redhat.com* und *westcoast.mainserver.redhat.com*.)

Auch wenn Ihr Computer nicht in ein Netzwerk eingebunden ist, können Sie einen Namen für Ihr System eingeben. Nutzen Sie die Möglichkeit, und geben Sie einen

Namen ein. Wenn Sie keinen Namen angeben, wird Ihr System `localhost` genannt.

Tipp

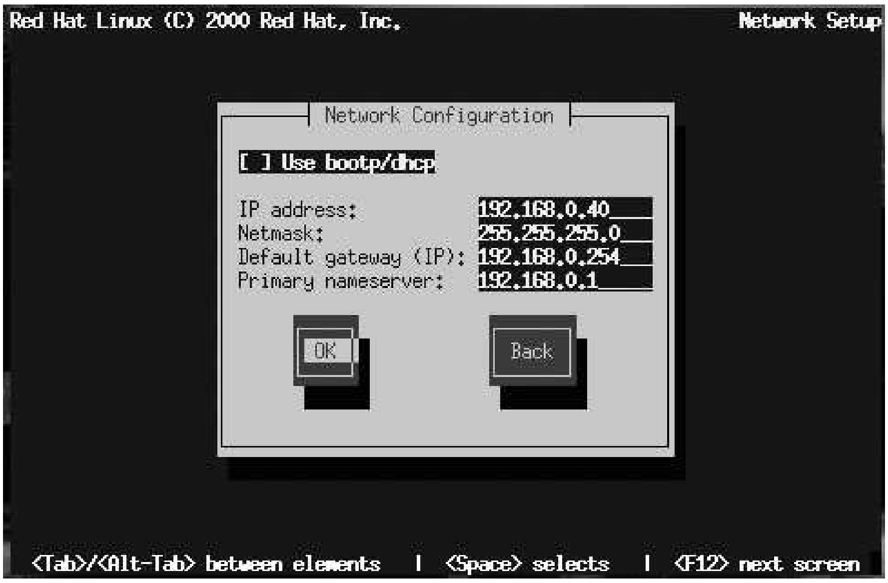
Um den Rechnernamen nach dem Neustart des Systems zu ändern, melden Sie sich als Root an. Geben Sie am Root-Prompt `hostname` *`Neuername`* ein, wobei *Neuername* der neue Rechnername ist. Wenn Sie den Rechnernamen nur anzeigen lassen wollen, geben Sie `hostname` ein. Auf dem Bildschirm wird dann der Rechnername des Systems angezeigt.

14.14 Konfigurieren einer Netzwerkverbindung

Wenn Sie die Installation über ein Netzwerk vornehmen, haben Sie die Netzwerkkonfiguration zu Beginn des Installationsprozesses vorgenommen und müssen diese Informationen nicht nochmals eingeben. Fahren Sie mit diesem Abschnitt fort, wenn Sie über einen lokalen Datenträger installieren und der Computer mit einer Netzwerkkarte ausgestattet ist.

Abbildung 14–27, *Dialogfeld Netzwerk-Konfiguration* wird nur angezeigt, wenn der Computer mit einer Netzwerkkarte ausgestattet ist. (Wenn mehr als eine Netzwerkkarte vorhanden ist, bezieht sich dieses Dialogfeld auf die erste Karte.)

Abbildung 14–27 Dialogfeld Netzwerk-Konfiguration



Dieses Dialogfeld bietet Ihnen zwei Möglichkeiten:

- Wählen Sie **bootp/dhcp verwenden** aus. In diesem Fall liefert ein in Ihrem LAN vorhandener Server dynamisch netzwerkspezifische Informationen, die benötigt werden, um dieses System zum Netzwerk hinzuzufügen. (Beachten Sie, dass in diesem Fall die übrigen Felder im Dialogfeld deaktiviert werden, da DHCP und BOOTP das Ausfüllen der leeren Felder automatisch für Sie erledigen.)
- Geben Sie die statischen Netzwerkinformationen in die angezeigten Felder ein. Diese Netzwerkinformationen werden diesem Computer auf Dauer zugeordnet.

14.15 Konfigurieren einer Maus

Als Nächstes durchsucht das Installationsprogramm Ihr System nach einer Maus (Abbildung 14–28, *Dialogfeld Maus auswählen*). Verwenden Sie die [Nach-oben-Taste] und die [Nach-unten-Taste], um die Auswahl zu bestätigen oder zu ändern.

Abbildung 14–28 Dialogfeld Maus auswählen

Wenn keine Maus erkannt wird, müssen Sie den Maustyp für Ihr System manuell angeben.

Die Schnittstelle Ihrer Maus können Sie ermitteln, indem Sie überprüfen, auf welche Weise das Mauskabel an Ihr System angeschlossen ist. Wenn der Stecker am Ende des Mauskabels mit einem rechteckigen Port verbunden ist, handelt es sich um eine serielle Maus. Ist der Port dagegen rund, besitzen Sie eine PS/2-Maus. Falls Sie Red Hat Linux auf einem Laptop-Computer installieren, so ist das Zeigegerät in den meisten Fällen PS/2-kompatibel.

Wenn Sie keine exakte Übereinstimmung finden können, wählen Sie je nach der Anzahl der Maustasten und Schnittstelle einen der **generischen** Einträge.

Mit Hilfe des Kontrollkästchens **Drei Tasten emulieren** können Sie eine Maus mit zwei Tasten als Drei-Tasten-Maus verwenden. Wenn Sie dieses Kontrollkästchen aktivieren, können Sie eine dritte, "mittlere" Maustaste emulieren, indem Sie beide Maustasten gleichzeitig drücken. Da die grafische Benutzeroberfläche mit drei Maustasten am leichtesten zu benutzen ist, empfiehlt es sich, bei einer Zwei-Tasten-Maus dieses Kontrollkästchen zu aktivieren.

Falls Sie eine Maus mit einer seriellen Schnittstelle ausgewählt haben, wählen Sie den entsprechenden Port, klicken Sie auf **OK**, und drücken Sie die [Leertaste].

Tipp

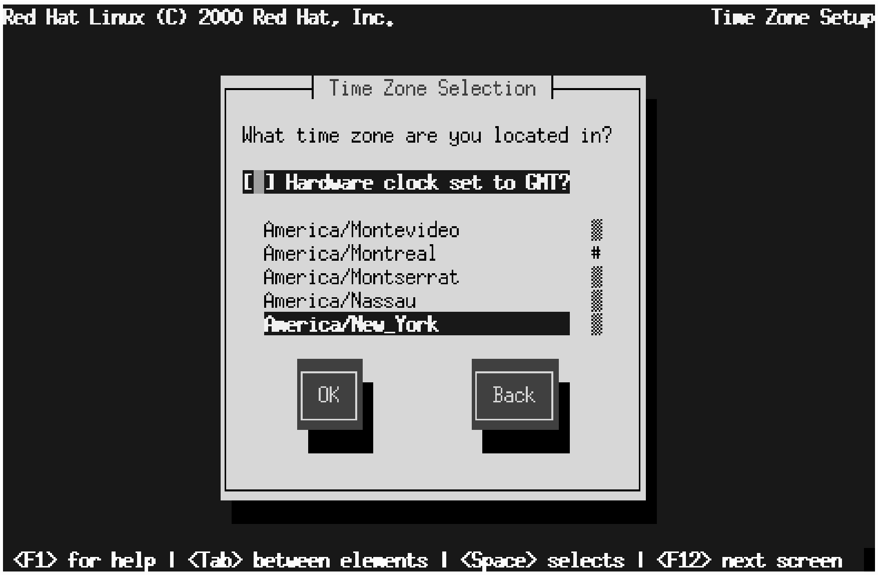
Falls Sie nach dem Start des Red Hat Linux Systems die Konfiguration Ihrer Maus ändern möchten, können Sie den Befehl `/usr/sbin/mouseconfig` verwenden, nachdem Sie sich als Root angemeldet haben.

Wenn Sie nach dem Start des Red Hat Linux Systems Ihre Maus für Linkshänder konfigurieren möchten, öffnen Sie ein Terminal, und geben Sie `gpm -B 321` ein.

14.16 Konfigurieren der Zeitzone

Geben Sie Ihre Zeitzone ein (siehe Abbildung 14–29, *Dialogfeld Zeitzone auswählen*).

Abbildung 14–29 Dialogfeld Zeitzone auswählen



Wenn Sie die Hardware- (CMOS) Uhr auf GMT (Greenwich Mean Time, auch bekannt als UTC, Universal Coordinated Time) einstellen möchten, aktivieren Sie **Hardware-Uhr auf GMT eingestellt**. Mit dieser Einstellung kann Ihr System die Sommerzeit berücksichtigen, sofern sie in Ihrer Zeitzone verwendet wird.

WARNUNG

Falls auf Ihrem Computer ein anderes Betriebssystem ausgeführt wird, kann das Einstellen der Uhr auf GMT dazu führen, dass das andere Betriebssystem die falsche Uhrzeit anzeigt. Außerdem ist es wahrscheinlich, dass die Uhrzeit falsch eingestellt wird, wenn mehr als ein Betriebssystem automatische Änderungen der Uhrzeit aufgrund der Sommerzeitregelung vornehmen darf.

Wählen Sie in der Liste Ihre Zeitzone aus, und drücken Sie die [Eingabetaste].

Tipp

Falls Sie die Zeitzoneneinstellung nach dem Start des Red Hat Linux Systems ändern möchten, können Sie dazu den Befehl `/usr/sbin/timeconfig` verwenden.

14.17 Setzen eines Root-Passworts

Das Dialogfeld **Root-Passwort** fordert Sie auf, für Ihr System ein **Root-Passwort** zu vergeben. Das Root-Passwort benötigen Sie, wenn Sie sich am Red Hat Linux System als Systemadministrator anmelden möchten.

Abbildung 14–30 Dialogfeld Root-Passwort

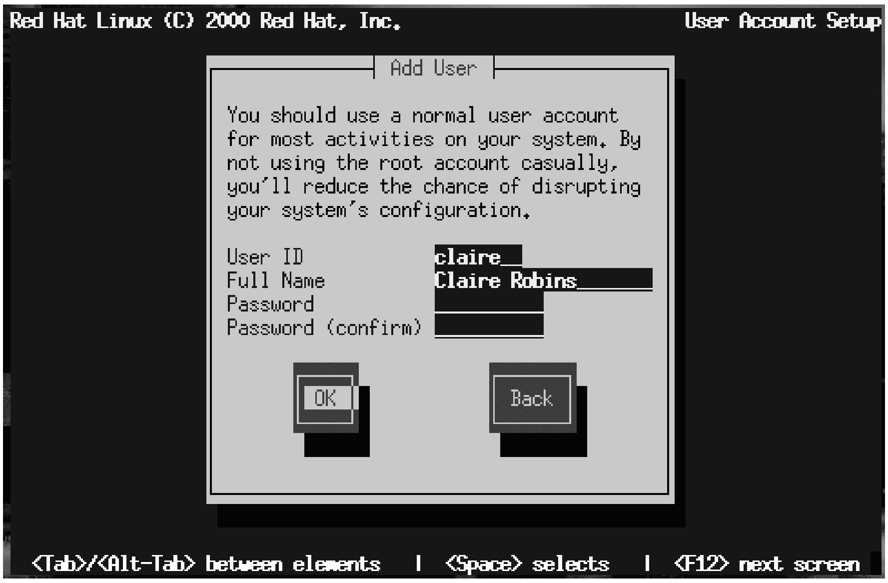
Das Root-Passwort muss aus mindestens sechs Zeichen bestehen. Es wird bei der Eingabe nicht auf dem Bildschirm angezeigt. Sie müssen das Passwort zweimal eingeben. Falls die beiden Eingaben nicht übereinstimmen, werden Sie vom Installationsprogramm aufgefordert, den Vorgang zu wiederholen.

Wählen Sie ein Passwort, das Sie sich gut merken können, das aber für andere Personen nicht leicht zu erraten ist. Ihr Name, Ihre Telefonnummer, **qwertz**, **Passwort**, **Root**, **123456**, und **Schnucki** sind Beispiele für schlechte Passwörter. Geeignete Passwörter bestehen aus einer Kombination von Zahlen und Groß-/Kleinbuchstaben und ergeben keine sinnvollen Wörter: z.B. **Aard387vark** oder **420BMttNT**. Beachten Sie, dass bei Passwörtern zwischen Groß- und Kleinschreibung unterschieden wird. Notieren Sie sich das Passwort, und bewahren Sie es an einem sicheren Ort auf.

14.18 Erstellen eines Benutzeraccounts

Sie können für sich einen Benutzeraccount für das tägliche Arbeiten mit dem System erstellen (siehe Abbildung 14–31, *Dialogfeld Benutzer hinzufügen*). Falls Sie dies nicht tun, müssen Sie sich nach der Installation als **Root** anmelden (auch **Superuser** genannt). Root hat vollständigen Zugriff auf das gesamte System. Deshalb sollten Sie sich *nur dann* als Root anmelden, wenn Sie Aufgaben der Systempflege oder -verwaltung ausführen möchten. Anweisungen, wie Benutzeraccounts nach der Installation erstellt oder geändert werden, finden Sie in Kapitel 3, *Systemkonfiguration* oder im Kapitel *Willkommen bei Linux* im *Offiziellen Red Hat Linux Handbuch Erste Schritte*.

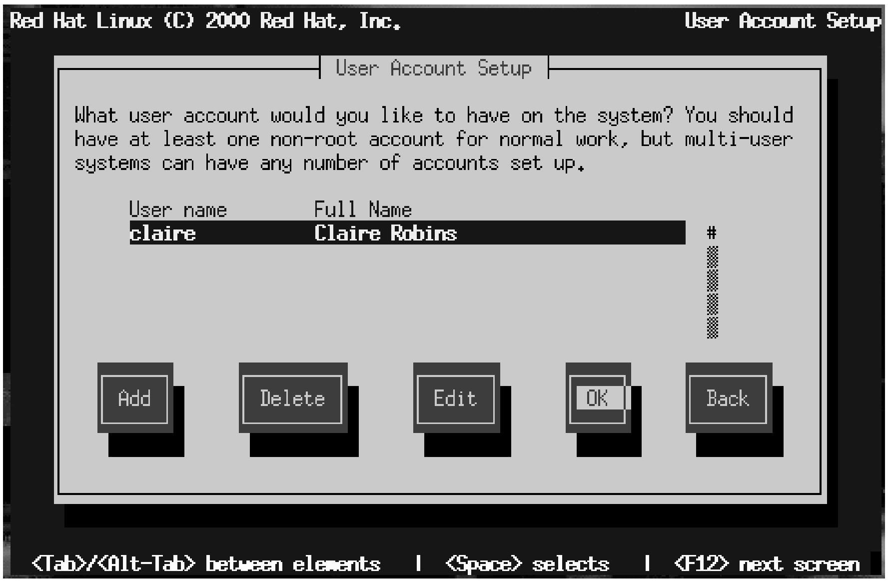
Abbildung 14–31 Dialogfeld Benutzer hinzufügen



Wenn ein Benutzeraccount erstellt werden soll, wird ein Verzeichnis für Ihren Account unter dem Pfad `/home` eingerichtet (z.B. `/home/claire`). Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen aus mindestens 6 Zeichen bestehen.

Nachdem Sie einen eigenen Benutzeraccount hinzugefügt haben, wird das Dialogfeld **Benutzeraccount einrichten** (Abbildung 14–32, *Dialogfeld Benutzeraccount einrichten*) angezeigt, in dem Sie weitere Accounts einrichten können. Wählen Sie dazu **Hinzufügen**, oder klicken Sie auf **OK**, um fortzufahren.

Abbildung 14–32 Dialogfeld Benutzeraccount einrichten

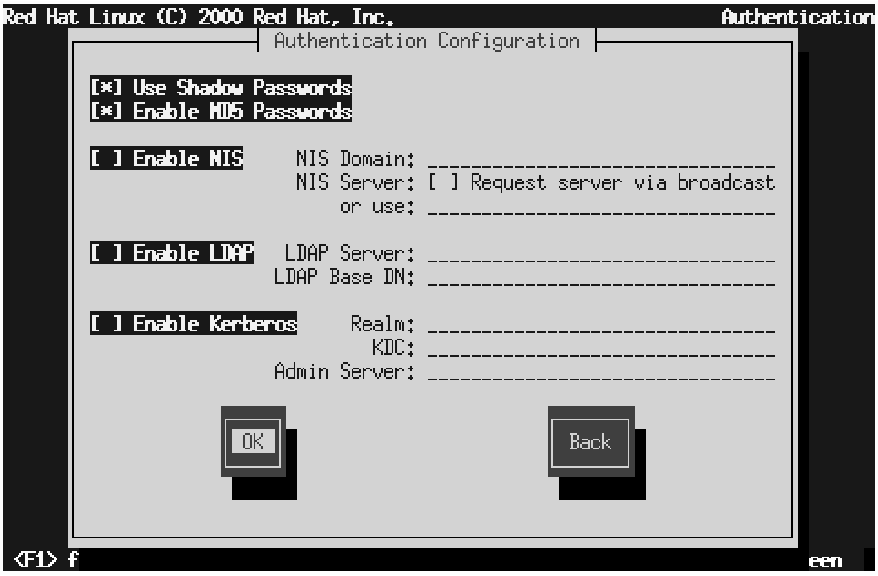


Bei einer Workstation- oder Server-Installation müssen Sie als Nächstes die Einstellungen für Ihre Grafikkarte bestätigen: siehe Abschnitt 14.21, *Konfigurieren der Grafikkarte*. Andernfalls lesen Sie bitte hier weiter.

14.19 Authentifizierung konfigurieren

Wenn Sie eine benutzerdefinierte Installation durchführen, können Sie im nächsten Schritt den Typ der Passwort-Authentifizierung für Ihr Red Hat Linux System konfigurieren (siehe Abbildung 14–33, *Dialogfeld Authentifizierung konfigurieren*). Sie können außerdem NIS-Unterstützung konfigurieren. Wenn Sie sich nicht sicher sind, ob Sie diese Möglichkeit nutzen sollen, fragen Sie Ihren Netzwerkadministrator.

Abbildung 14–33 Dialogfeld Authentifizierung konfigurieren



Die einzelnen Passwortoptionen für die Authentifizierung sind wie folgt:

- **Shadow-Passwörter verwenden** - Stellt eine sehr sichere Methode zur Verwaltung der Passwörter dar. Das Passwortfeld in `/etc/passwd` wird in die Datei `/etc/shadow` ausgelagert, die ausschließlich von Root gelesen werden kann.
- **MD5-Passwörter aktivieren** - Ermöglicht das Verwenden langer Passwörter mit bis zu 256 Zeichen anstelle der standardmäßig maximal acht Zeichen.
- **NIS aktivieren** - Eine Gruppe von Rechnern kann mit einer gemeinsamen Passwort- und Gruppendatei in derselben Network Information Service-Domäne betrieben werden. Sie können zwischen zwei Optionen wählen:
  - **NIS-Domäne** - Sie geben an, welcher Domäne oder Rechnergruppe Ihr System angehören soll.
  - **NIS-Server** - Mit dieser Option kann Ihr Computer einen bestimmten NIS-Server verwenden, statt eine Broadcast-Anforderung an das lokale Netzwerk auszugeben, um nach verfügbaren Servern für das System zu fragen.

- **LDAP aktivieren** - LDAP fasst bestimmte Informationsarten innerhalb Ihrer Organisation zusammen. So können zum Beispiel alle Benutzerlisten in Ihrer Organisation in einem LDAP-Verzeichnis untergebracht werden. Weitere Informationen zu LDAP finden Sie im Kapitel 7, *Lightweight Directory Access Protocol (LDAP)*. Ihnen stehen zwei Optionen zur Auswahl:
  - **LDAP Server** - Mit dieser Option können Sie auf einen Server zugreifen, der den LDAP-Dienst zur Verfügung stellt.
  - **LDAP Basis-DN** - Mit dieser Option können Sie anhand des eindeutigen Namens (*Distinguished Name*, DN) nach Benutzerinformationen suchen.
- **Kerberos aktivieren** - Bei Kerberos handelt es sich um ein sicheres System, das Authentifizierungsdienste für Netzwerke zur Verfügung stellt. Weitere Informationen zu Kerberos finden Sie in Kapitel 8, *Verwenden von Kerberos 5 in Red Hat Linux*. Ihnen stehen drei Optionen zur Auswahl:
  - **Realm** - Mit dieser Option können Sie auf ein Netzwerk zugreifen, das Kerberos verwendet und aus einem oder einigen Servern (auch als KDCs bezeichnet) sowie einer (potentiell sehr großen) Zahl von Clients besteht.
  - **KDC** - Mit dieser Option können Sie auf das Key Distribution Center (KDC) zugreifen. Hierbei handelt es sich um ein Gerät, das Kerberos-Tickets ausgibt (manchmal auch als Ticket Granting Server oder TGS bezeichnet).
  - **Admin-Server** - Mit dieser Option können Sie auf einen Server zugreifen, der `kadmind` ausführt.

Bitte beachten

Um die NIS-Option zu konfigurieren, muss Ihr Computer an ein NIS-Netzwerk angeschlossen sein. Wenn Sie sich nicht sicher sind, ob dies der Fall ist, wenden Sie sich bitte an Ihren Netzwerkadministrator.

Sie werden bemerken, dass sowohl Shadow-Passwörter als auch MD5-Passwörter aktiviert sind, wenn Sie NIS nicht einrichten. Es empfiehlt sich, beide Optionen zu verwenden, um Ihren Computer so sicher wie möglich zu machen.

14.20 Auswählen und Installieren der Pakete

Abbildung 14–34, *Dialogfeld Auswahl von Paketgruppen* wird nur bei einer benutzerdefinierten Installation angezeigt. In diesem Dialogfeld können Sie die Typen von Software-Paketen auswählen, die Sie installieren möchten.

Abbildung 14–34 Dialogfeld Auswahl von Paketgruppen

Wenn Sie **Alles** auswählen (befindet sich am Ende der Komponentenliste), werden alle Pakete installiert, die zum Lieferumfang von Red Hat Linux gehören. Sie benötigen dann etwa 1,7 GB freien Festplattenspeicher.

14.20.1 Auswählen von Einzelpaketen

Sie können auch einzelne Pakete in einer Anwendungskategorie auswählen oder aus der Auswahl entfernen. Aktivieren Sie hierzu das Kontrollkästchen **Einzelne Pakete**

auswählen. Wenn Sie **OK** auswählen, wird ein Bildschirm wie Abbildung 14–35, *Auswählen von Einzelpaketen* angezeigt.

Abbildung 14–35 Auswählen von Einzelpaketen

Um z.B. eine Liste der Pakete in der Kategorie **Anwendungen/Editoren** anzuzeigen, wählen Sie diese Gruppe mit den Cursortasten aus und drücken die [Eingabetaste] oder [Leertaste]. Dabei ändert sich das **+**-Zeichen (komprimiert) in ein **-**-Zeichen (aufgeklappt), und eine Liste der Pakete in dieser Kategorie wird angezeigt. Aktuell ausgewählte Pakete sind mit einem ***** gekennzeichnet. Drücken Sie die [Eingabetaste] oder die [Leertaste], um Pakete auszuwählen bzw. abzuwählen.

Sie können eine Beschreibung des jeweiligen Pakets anzeigen. Markieren Sie dazu das Paket, und drücken Sie [F1].

Beachten Sie, dass einige Pakete, die für jedes Red Hat Linux System benötigt werden (z.B. der Kernel und bestimmte Bibliotheken) in den Dialogfeldern für die Paketauswahl nicht erscheinen.

14.20.2 Ungelöste Paketabhängigkeiten

Viele der Software-Pakete können nur in Verbindung mit anderen Paketen oder Bibliotheken, die auf Ihrem System installiert sind, korrekt ausgeführt werden. Beispielsweise sind für viele der grafischen Systemadministrations-Tools die Pakete `python` und `pythonlib` erforderlich. Um sicherzustellen, dass alle Pakete zur Verfügung stehen, die Ihr System benötigt, überprüft Red Hat Linux diese **Paketabhängigkeiten** bei jeder Installation oder Deinstallation von Software-Paketen.

Abbildung 14–36 Dialogfeld Paketabhängigkeiten

Nachdem Sie die gewünschten Pakete ausgewählt haben, überprüft das Installationsprogramm die Liste der von Ihnen ausgewählten Pakete nach Abhängigkeiten. Falls Pakete fehlen, die andere Pakete zur korrekten Ausführung benötigen, zeigt das Programm eine Liste dieser **ungelösten Abhängigkeiten** an und gibt Ihnen die Möglichkeit, diese zu lösen (siehe Abbildung 14–36, *Dialogfeld Paketabhängigkeiten*). Das Programm kann die Abhängigkeiten auch automatisch lösen und alle erforderlichen

Pakete zur Liste der ausgewählten Pakete hinzufügen. Klicken Sie hierzu einfach auf **OK**.

14.21 Konfigurieren der Grafikkarte

Das Installationsprogramm sucht jetzt nach Ihrer Grafikkarte. Wenn die Karte gefunden wurde, klicken Sie auf **OK**, um fortzufahren.

Abbildung 14–37 Dialogfeld Grafikkarte bestätigen

Wenn das Installationsprogramm die Grafikkarte nicht erkennt, erscheint Abbildung 14–38, *Dialogfeld Grafikkarte auswählen*. In diesem Fall müssen Sie die Grafikkarte mit den Cursortasten und der [Leertaste] aus der Liste auswählen.

Abbildung 14–38 Dialogfeld Grafikkarte auswählen

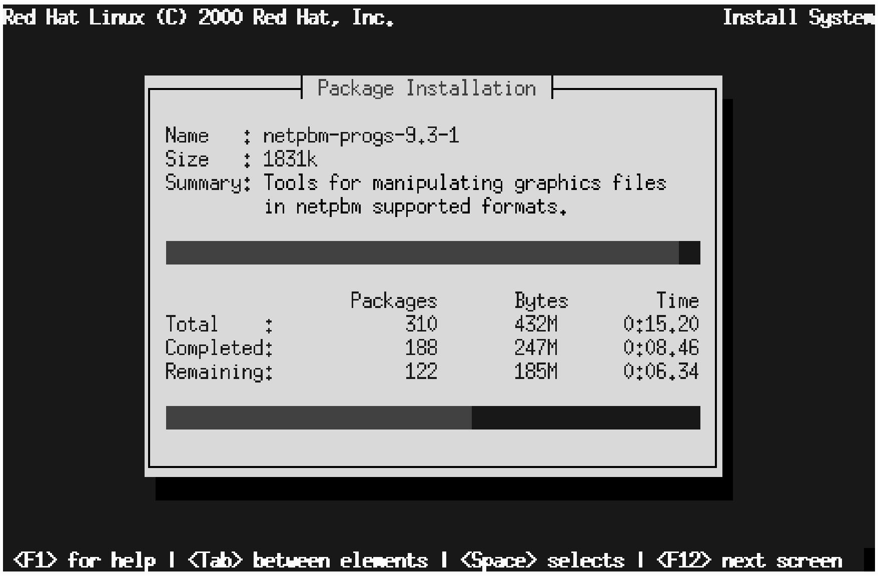
14.22 Installation von Paketen

Abbildung 14–39, *Dialogfeld Installation beginnt* wird angezeigt, wenn das Installationsprogramm bereit ist, Partitionen zu formatieren und Software-Pakete zu laden. Das Installationsprogramm gibt die Protokolldatei (`/tmp/install.log`) für diese Red Hat Linux Installation an. Klicken Sie auf **OK**, und drücken Sie die [Leertaste], um fortzufahren.

Abbildung 14–39 Dialogfeld Installation beginnt

Während Software-Pakete geladen werden, wird ein ähnlicher Bildschirm wie Abbildung 14–40, *Dialogfeld zur Anzeige des Installationsstatus* angezeigt.

Abbildung 14–40 Dialogfeld zur Anzeige des Installationsstatus



Sobald der Installationsvorgang für ein Software-Paket beginnt, werden dessen Name, Größe und eine Kurzbeschreibung der Funktionalität im oberen Teil des Bildschirms **Installation von Paketen** angezeigt.

Im unteren Bereich des Bildschirms **Installation von Paketen** werden in der Zeile **Gesamt** die Gesamtzahl der Pakete, die installiert werden sollen, die Gesamtgröße aller Pakete sowie die Zeit angezeigt, die zur Installation aller Pakete erforderlich ist. Sobald der Ladevorgang für ein Paket gestartet oder abgeschlossen wird, werden die Zeilen "Abgeschlossen" und "Verbleibend" aktualisiert.

Wenn Sie eine Server-Installation durchführen, sind Sie fast fertig: siehe Abschnitt 14.25, *Abschließende Arbeiten*.

14.23 Erstellen einer Bootdiskette

Bei einer benutzerdefinierten Installation haben Sie im Dialogfeld **Bootdiskette** (siehe Abbildung 14–41, *Erstellen einer Bootdiskette*) die Möglichkeit, eine individuelle Bootdiskette für Ihr Red Hat Linux System zu erstellen.

Abbildung 14–41 Erstellen einer Bootdiskette

Die Verwendung einer Bootdiskette ist aus mehreren Gründen sinnvoll:

- Anstelle von LILO - Sie können eine Bootdiskette anstelle von LILO verwenden. Dies ist hilfreich, wenn Sie zum ersten Mal mit Red Hat Linux arbeiten. Außerdem brauchen Sie sich keine Sorgen um die Boot-Einstellungen für Ihr anderes Betriebssystem zu machen. Wenn Sie eine Bootdiskette verwenden, können Sie problemlos zu Ihrem anderen Betriebssystem zurückkehren, indem Sie die Bootdiskette aus dem Laufwerk nehmen und das System neu starten.

- Wenn ein anderes Betriebssystem LILO überschreibt - Andere Betriebssysteme sind möglicherweise nicht so flexibel wie Red Hat Linux, wenn es um die unterstützten Bootmethoden geht. Sehr oft wird durch die Installation oder Aktualisierung eines anderen Betriebssystems der Master Boot Record Ihrer Festplatte überschrieben, in dem sich LILO befindet, so dass Sie die Red Hat Linux Installation nicht mehr booten können. In diesem Fall können Sie Red Hat Linux mit der Bootdiskette starten, um LILO anschließend neu zu installieren.

Wählen Sie **Ja** aus, und drücken Sie die [Leertaste], um eine Bootdiskette zu erstellen. Anschließend wird ein Dialogfeld angezeigt, das Sie auffordert, eine leere, formatierte Diskette in das Diskettenlaufwerk des Computers einzulegen.

Abbildung 14–42 Dialogfeld Bootdiskette

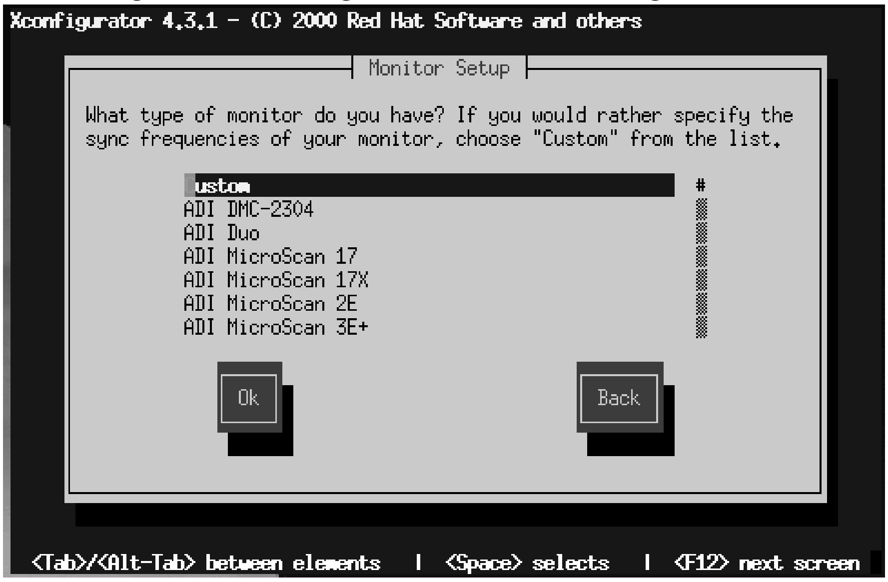
Anweisungen zum Erstellen einer Bootdiskette nach der Installation finden Sie auf der man-Seite zu `mkbootdisk`. Denken Sie bitte daran, nach jeder Änderung am Kernel eine neue Bootdiskette zu erstellen.

14.24 Konfigurieren des X Window Systems

Mit dem Dienstprogramm `Xconfigurator` erhalten Sie die Möglichkeit, den X-Server für Ihr System zu konfigurieren.

Zunächst zeigt `Xconfigurator` eine Liste von Bildschirmen an (siehe Abbildung 14–43, *Dialogfeld Bildschirm konfigurieren*). Wenn Ihr Bildschirm in der Liste enthalten ist, markieren Sie ihn und drücken die [Eingabetaste]. Andernfalls wählen Sie bitte **Benutzerdefiniert** aus.

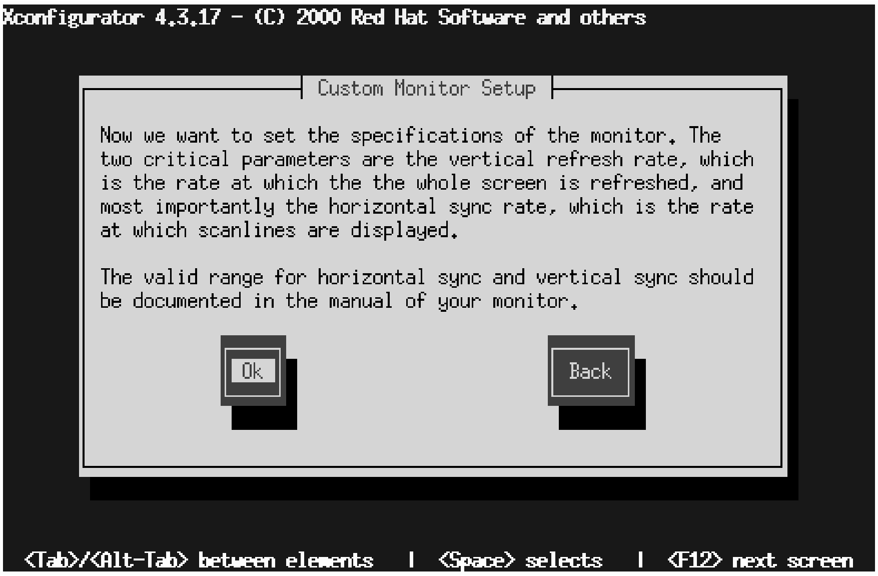
Abbildung 14–43 Dialogfeld Bildschirm konfigurieren



Wenn Sie einen Bildschirm in der Liste auswählen, geben Sie als Nächstes den Grafikspeicher ein (siehe Abbildung 14–48, *Grafikspeicher*).

Wenn Sie **Benutzerdefiniert** auswählen, fordert `Xconfigurator` Sie auf, den Horizontalfrequenzbereich und die Bildwiederholrate Ihres Bildschirms auszuwählen. (Diese Informationen können Sie normalerweise der Dokumentation zu Ihrem Bildschirm entnehmen. Sie können sie aber auch vom Händler oder Hersteller des Bildschirms beziehen.)

Abbildung 14–44 Benutzerdefinierte Bildschirmkonfiguration

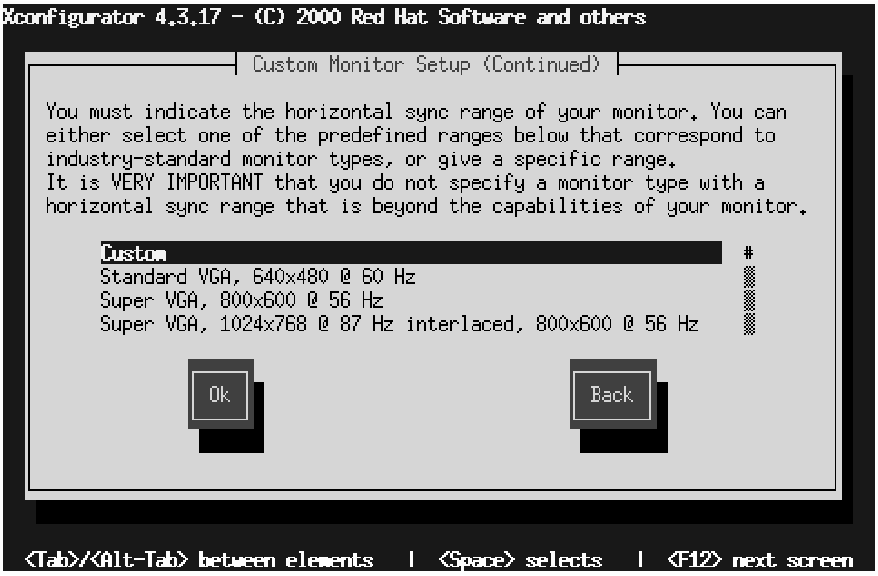


ACHTUNG

Wählen Sie bitte keine Werte aus, die die Leistungsfähigkeit Ihres Bildschirms übersteigen. In diesem Fall könnte Ihr Bildschirm überlastet und dadurch beschädigt oder zerstört werden.

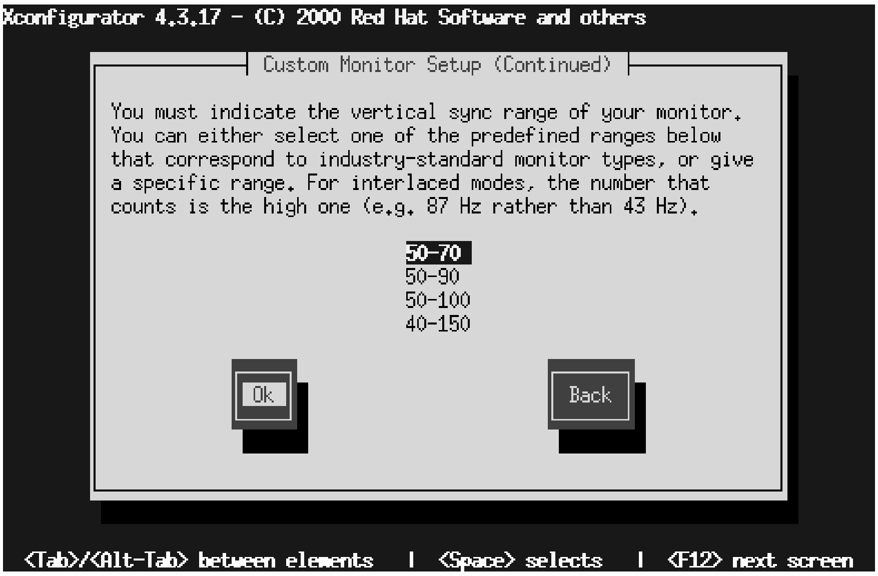
Wählen Sie eine Horizontalfrequenz für den Bildschirm aus (siehe Abbildung 14–45, *Benutzerdefinierte Bildschirmkonfiguration - Horizontalfrequenz*). Denken Sie bitte daran, *keinen* Bereich auszuwählen, der die Leistungsfähigkeit des Bildschirms übersteigt. Weitere Informationen über benutzerdefinierte Einstellungen finden Sie in Abbildung 14–47, *Benutzerdefinierte Bildschirminformationen*.

Abbildung 14–45 Benutzerdefinierte Bildschirmkonfiguration - Horizontalfrequenz



Wählen Sie als Nächstes einen Bereich für die Bildwiederholrate aus.

Abbildung 14–46 Benutzerdefinierte Bildschirmkonfiguration - Bildwiederholrate



Wenn Sie sich entschieden haben, benutzerdefinierte Bildschirmeinstellungen einzugeben, geben Sie den Bereich sowohl für die Horizontalfrequenz als auch für die Bildwiederholrate des Bildschirms ein (siehe Abbildung 14–47, *Benutzerdefinierte Bildschirminformationen*).

Abbildung 14–47 Benutzerdefinierte Bildschirminformationen

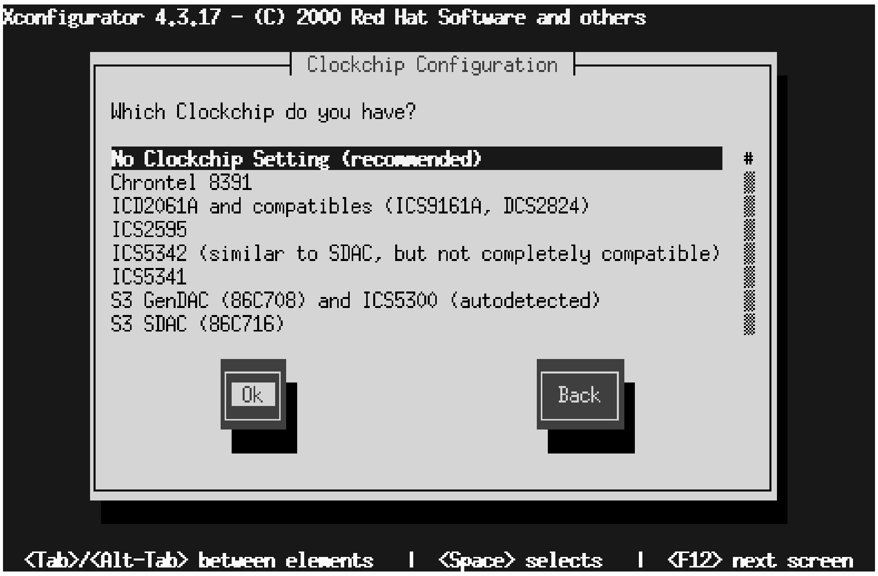
Nachdem Sie den Bildschirm (und die entsprechenden Einstellungen) ausgewählt haben, müssen Sie die Speichergröße der Grafikkarte angeben (siehe Abbildung 14–48, *Grafikspeicher*).

Abbildung 14–48 Grafikspeicher

Wenn Sie nicht genau wissen, wie groß der Speicher der Grafikkarte ist, informieren Sie sich in der Bedienungsanleitung, die zum Lieferumfang der Grafikkarte gehört, über diesen Wert. Wenn Sie einen größeren Wert auswählen, als auf der Karte installiert ist, wird die Grafikkarte zwar nicht beschädigt, aber der Server XFree86 wird möglicherweise nicht ordnungsgemäß gestartet.

Wählen Sie als Nächstes eine Clockchip-Einstellung aus, sofern diese Einstellung von der Grafikkarte unterstützt wird (und die Grafikkarte darüber verfügt). Hier wird die Auswahl **Keine Clockchip-Einstellung** empfohlen, da XFree86 in den meisten Fällen den richtigen Clockchip automatisch erkennt.

Abbildung 14–49 Dialogfeld Clockchip konfigurieren



Mit dem Bildschirm **Nach Taktraten suchen** (siehe Abbildung 14–50, *Nach Taktraten suchen*) werden Sie aufgefordert, das Installationsprogramm erkennen zu lassen, in welchen Grafikmodi die Grafikkarte und der Bildschirm betrieben werden können.

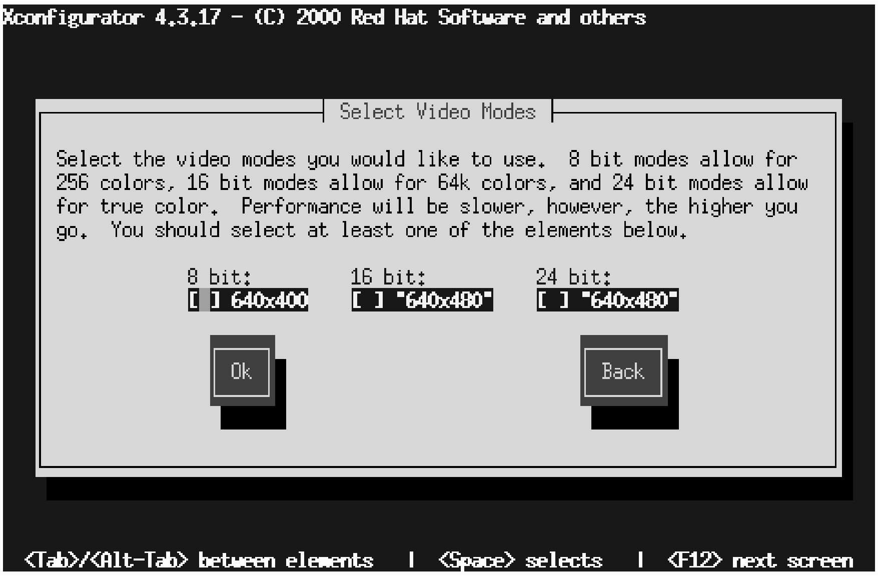
Um optimale Ergebnisse zu erzielen, sollten Sie die Option **Suchen** aktivieren. Wenn Sie zulassen, dass das Installationsprogramm diese Modi für Sie erkennt, reduzieren sich möglicherweise Ihre Auswahlmöglichkeiten für die Grafikmodi (siehe Abbildung 14–51, *Grafikmodi auswählen*) entsprechend der Leistungsfähigkeit von Grafikkarte und Bildschirm.

Wenn bei einem Versuch, die Grafikmodi erkennen zu lassen, ein Fehler auftrat (so dass Sie beispielsweise das System neu starten mussten), sollten Sie die Option **Überspringen** auswählen und anschließend Ihre bevorzugten Grafikmodi (siehe Abbildung 14–52, *Grafikmodi auswählen*) auswählen.

Abbildung 14–50 Nach Taktraten suchen

Um Ihren bevorzugten Anzeigemodus zu aktivieren (siehe Abbildung 14–51, *Grafikmodi auswählen* und Abbildung 14–52, *Grafikmodi auswählen*), wählen Sie einen oder mehrere Modi aus, indem Sie die [Leertaste] drücken.

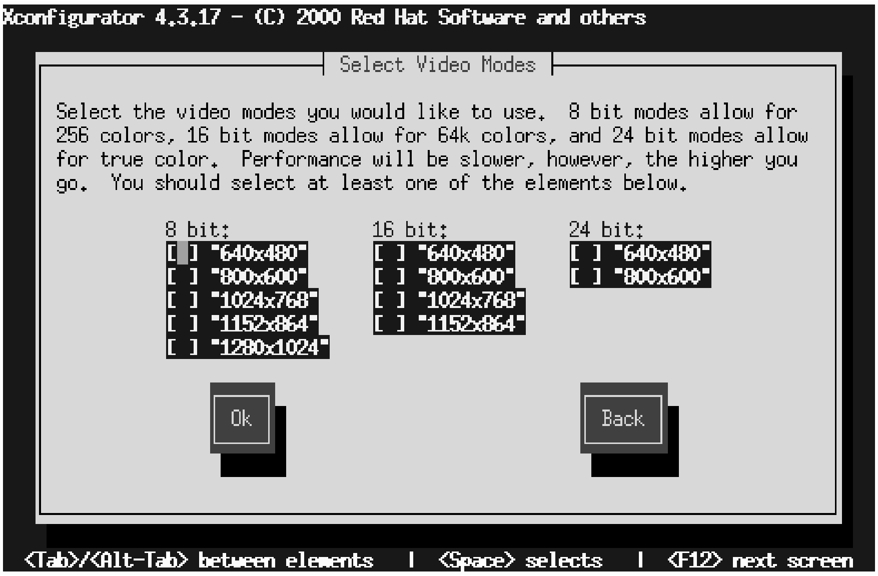
Abbildung 14–51 Grafikmodi auswählen



Tipp

16 Bit ist die empfohlene Minimaleinstellung für die Grafikmodi der meisten Anwendungen bei einer Auflösung von 1024 x 768 (Grafikmodi mit mehr als 16 Bit werden im Allgemeinen langsamer ausgeführt).

Abbildung 14–52 Grafikmodi auswählen



Wählen Sie keinen Modus aus, der die Leistungsfähigkeit Ihres Bildschirms überschreitet.

Wenn Sie den Standardgrafikmodus ausgewählt oder einen anderen Modus angegeben haben, können Sie mit dem Dialogfeld **X wird gestartet** Ihre X-Konfiguration testen.

Abbildung 14–53 X-Konfiguration testen

Wenn Sie auf **OK** klicken, haben Sie die Möglichkeit, zum entsprechenden Bildschirm zurückzuspringen und andere Werte einzugeben, sofern ein Fehler auftritt. Wird kein Fehler erkannt, wird X gestartet, und Sie werden in einem kleinen Dialogfeld gefragt, ob Sie die Anzeige auf dem Bildschirm klar erkennen können. Klicken Sie innerhalb von 10 Sekunden mit der Maus auf **Ja**. Sie werden anschließend gefragt, ob X beim Systemstart gestartet werden soll.

In den meisten Fällen ist die X-Konfiguration an dieser Stelle beendet, und der entsprechende Bildschirm wird angezeigt.

`Xconfigurator` speichert anschließend alle Einstellungen in der Konfigurationsdatei `/etc/X11/XF86Config`. Um die X-Konfiguration nach der Installation zu ändern, geben Sie als Root den Befehl `Xconfigurator` ein.

14.25 Abschließende Arbeiten

Wenn die Installation abgeschlossen ist, wird das Dialogfeld **Fertig** angezeigt (siehe Abbildung 14–54, *Dialogfeld Fertig*), in dem Sie aufgefordert werden, den Computer neu zu starten. Nehmen Sie die Diskette aus dem Diskettenlaufwerk bzw. die Red Hat Linux CD aus dem CD-ROM-Laufwerk, falls Ihr System von CD-ROM gebootet wurde. Wenn Sie jedoch die standardmäßige LILO-Installation übersprungen haben, müssen Sie zum Neustart die während der Installation erstellte Bootdiskette verwenden.

Abbildung 14–54 Dialogfeld Fertig

Klicken Sie auf **OK**, und starten Sie Ihr neu installiertes System. Sobald die normale Startsequenz des Computers abgeschlossen ist, sollte der GUI-Prompt von LILO angezeigt werden. An diesem Prompt sind folgende Eingaben möglich:

- [Eingabetaste] drücken - Der Standardbooteintrag von LILO (wie in Abbildung 14–25, *Auswählen bootbarer Partitionen im Dialogfeld LILO konfigurieren* dargestellt) wird gebootet.

- Bootkennung auswählen und anschließend [Eingabetaste] drücken - LILO startet das Betriebssystem entsprechend der Bootkennung. (Durch Drücken der Taste [?] am LILO Prompt `boot:` wird eine Liste der gültigen Bootkennungen angezeigt.)
- Keine Aktion - Nach Ablauf der Zeitüberschreitung (standardmäßig 5 Sekunden) startet LILO automatisch den Standardbooteintrag.

Führen Sie die erforderlichen Schritte aus, um Red Hat Linux zu booten. Zunächst scrollen zahlreiche Meldungen über Ihren Bildschirm. Schließlich sehen Sie ein grafisches Dialogfeld für die Anmeldung oder einen `login:`-Prompt ein.

Herzlichen Glückwunsch! Ihre Red Hat Linux Installation ist beendet!

15 Installieren von Red Hat Linux über die grafische Benutzeroberfläche

Dieses Kapitel erläutert, wie Sie Red Hat Linux von der CD-ROM installieren und dabei das grafische, mausbasierte Installationsprogramm verwenden.

15.1 Die Benutzeroberfläche des Installationsprogramms

Wenn Sie bereits mit **grafischen Benutzeroberflächen (GUI)** gearbeitet haben, werden Sie mit der Vorgehensweise vertraut sein. Haben Sie noch keine Erfahrung mit Benutzeroberflächen erworben, erhalten Sie hier ganz kurz einige Informationen. Für das Navigieren in den Bildschirmen verwenden Sie die Maus, mit der Sie auf Buttons klicken oder Textfelder für die Texteingabe aktivieren können. Sie können auch die [Tabulatortaste] und die [Eingabetaste] verwenden, um in den Bildschirmen des Installationsprogramms zu navigieren.

Bitte beachten

Wenn Sie das grafische Installationsprogramm nicht verwenden möchten, steht Ihnen auch weiterhin das textbasierte Installationsprogramm zur Verfügung. Geben Sie folgenden Bootbefehl ein, um den Textmodus aufzurufen:

```
boot: text
```

Hinweise zur Installation im Textmodus finden Sie im Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm*.

15.1.1 Ein Hinweis zu virtuellen Konsolen

Das Red Hat Linux Installationsprogramm bietet Ihnen mehr als nur die Dialogfelder, die während der Installation angezeigt werden. So stehen Ihnen verschiedene

Diagnosemeldungen zur Verfügung, und Sie können Befehle vom Shell Prompt aus eingeben. Diese Informationen werden an fünf **virtuellen Konsolen** angezeigt, zwischen denen Sie einfach mit Tastaturbefehlen umschalten können.

Diese virtuellen Konsolen sind sehr hilfreich, wenn bei der Installation von Red Hat Linux Probleme auftreten. Über die Meldungen an den Installations- oder Systemkonsolen können Probleme genauer eingegrenzt werden. In Tabelle 15–1, *Konsole, Tasten und Inhalt* finden Sie einen Überblick über die virtuellen Konsolen, deren Inhalt und die Tastenkombinationen zum Umschalten zwischen diesen Konsolen.

Tabelle 15–1 Konsole, Tasten und Inhalt

Konsole	Tasten	Inhalt
1	[Strg]-[Alt]-[F1]	Installationsdialogfeld
2	[Strg]-[Alt]-[F2]	Shell Prompt
3	[Strg]-[Alt]-[F3]	Installationsprotokoll (Meldungen des Installationsprogramms)
4	[Strg]-[Alt]-[F4]	Systembezogene Meldungen
5	[Strg]-[Alt]-[F5]	Weitere Meldungen
7	[Strg]-[Alt]-[F7]	Grafikanzeige unter X

Eigentlich gibt es keinen Grund, die Standardkonsole (virtuelle Konsole Nr. 7) zu verlassen, es sei denn, Sie möchten Problemen bei der Installation auf den Grund gehen. Wenn Sie jedoch neugierig sind, können Sie sich gern etwas umsehen.

15.2 Starten des Installationsprogramms

Nun ist es an der Zeit, mit der Installation von Red Hat Linux zu beginnen. Hierfür müssen Sie zunächst das Installationsprogramm starten. Stellen Sie zuvor sicher, dass Sie über alle Ressourcen für die Installation verfügen. Wenn Sie das *Offizielle Red Hat Linux Installationshandbuch* bereits gelesen und die Anweisungen ausgeführt haben, sollten Sie startklar sein.

Bitte beachten

Gelegentlich benötigen einige Hardware-Komponenten während der Installation eine **Treiberdiskette**. Durch eine Treiberdiskette kann Unterstützung für Hardware hinzugefügt werden, die nicht vom Installationsprogramm unterstützt wird. Die Treiberdiskette kann von Red Hat oder von Ihnen erstellt worden sein oder von einem Hardware-Händler mit einem Gerät mitgeliefert werden.

Wenn Sie im Bildschirm dazu aufgefordert werden, eine Treiberdiskette einzulegen, und Sie über eine von einem Hardware-Händler mitgelieferte Diskette verfügen, legen Sie diese bitte ein. Darüber hinaus können Sie auch unter http://www.redhat.com/support/errata/ Treiberdisketten erhalten. Weitere Informationen zu Treiberdisketten, siehe Anhang C, *Treiberdisketten*.

15.2.1 Starten des Installationsprogramms

Bitte beachten

Falls Sie eine Bootdiskette erstellen müssen, lesen Sie hierzu bitte den Abschnitt *Schritt 5 - Können Sie für die Installation die Red Hat Linux CD-ROM verwenden?* im *Offiziellen Red Hat Linux Installationshandbuch*.

Legen Sie die Bootdiskette in das erste Diskettenlaufwerk Ihres Computers ein, und starten Sie Ihr System neu (oder booten Sie direkt von CD-ROM, wenn Ihr Computer dies unterstützt). Möglicherweise müssen Sie die Einstellungen im BIOS ändern, um das Booten von Diskette oder CD-ROM zu ermöglichen.

Tipp

Um die BIOS-Einstellungen zu ändern, müssen Sie beim Starten des Computers die angezeigten Meldungen auf dem Bildschirm genau verfolgen. Oft wird zu Anfang des Bootvorgangs die Meldung angezeigt, dass Sie die [Entf]-Taste drücken müssen, um die BIOS-Einstellungen anzeigen zu können. Sobald Sie die BIOS-Einstellungen auf die von Ihrem BIOS vorgesehene Weise aufgerufen haben, können Sie die Bootreihenfolge ändern, damit Ihr Computer vom CD-ROM-Laufwerk oder dem Diskettenlaufwerk bootet, wenn in diesen Laufwerken ein bootfähiger Datenträger enthalten ist. Weitere Informationen finden Sie in der Dokumentation, die mit Ihrem System ausgeliefert wurde.

Es gibt vier verschiedene Bootmethoden:

- *Bootfähige CD-ROM* - Verwenden Sie diese Möglichkeit, wenn Ihr System über ein bootfähiges CD-ROM-Laufwerk verfügt und Sie Linux lokal von CD-ROM installieren möchten.
- *Lokale Bootdiskette* - Verwenden Sie diese Diskette in den Fällen, in denen der Computer über kein bootfähiges CD-ROM-Laufwerk verfügt und Sie die Installation von einem lokalen CD-ROM-Laufwerk oder einer Festplatte durchführen möchten.
- *Netzwerkbootdiskette* - Verwenden Sie diese Diskette für die NFS-, FTP- und HTTP-Installationsarten.
- *PCMCIA-Bootdiskette* - Verwenden Sie diese Diskette in den Fällen, in denen Sie PCMCIA-Unterstützung benötigen, aber Ihren Computer nicht vom CD-ROM-Laufwerk booten können, *oder* in denen Sie PCMCIA-Unterstützung benötigen, um das CD-ROM-Laufwerk in Ihrem System verwenden zu können. Diese Bootdiskette kann für alle Installationsarten verwendet werden (CD-ROM, Festplatte, NFS, FTP und HTTP).

Nach kurzer Wartezeit wird ein Bildschirm mit dem Prompt `boot:` eingeblendet. Er enthält Informationen zu vielen Bootoptionen, die außerdem durch eine oder mehrere Hilfebildschirme erläutert werden. Um einen Hilfebildschirm anzuzeigen, drücken Sie die entsprechende Funktionstaste (die Funktionstasten werden im unteren Bereich des Bildschirms aufgelistet).

Beachten Sie die folgenden Punkte:

- Der Ausgangsbildschirm startet das Installationsprogramm automatisch, wenn Sie innerhalb einer Minute keine Eingabe vornehmen. Um diese Automatik zu deaktivieren, drücken Sie die entsprechende Funktionstaste für den Hilfebildschirm.
- Wenn Sie eine der Funktionstasten für einen Hilfebildschirm betätigen, kommt es zu einer kurzen Verzögerung, da die Hilfe von Diskette abgerufen wird.

In der Regel brauchen Sie nur die [Eingabetaste] zu drücken, um den Bootvorgang zu starten. Verfolgen Sie anhand der Bootmeldungen, ob der Linux-Kernel Ihre Hardware erkennt. Falls dies nicht der Fall ist, müssen Sie gegebenenfalls die Installation im Expertenmodus neu starten. Wenn die Hardware richtig erkannt wird, fahren Sie bitte mit dem nächsten Abschnitt fort.

In den Expertenmodus gelangen Sie über den folgenden Bootbefehl:

```
boot: linux expert
```

Wenn Sie keine Installation mit dem grafischen Installer von CD-ROM durchführen möchten, können Sie durch Eingabe des folgenden Bootbefehls eine Installation im Textmodus vornehmen:

```
boot: text
```

Anweisungen zur Installation im Textmodus finden Sie im Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm*.

Der Befehl zum Starten einer **seriellen Installation** hat sich geändert. Sie müssen hierzu jetzt folgenden Befehl eingeben:

```
boot: linux console=<Gerät>
```

Hierbei gibt <*Gerät*> das Gerät an, das Sie verwenden (z.B. ttyS0 oder ttyS1).

Um explizit ein Dialogfeld anzufordern, in dem Sie zusätzliche Geräte konfigurieren können (z.B. ISA-Geräte), müssen Sie 'isa' in die Anweisung einfügen:

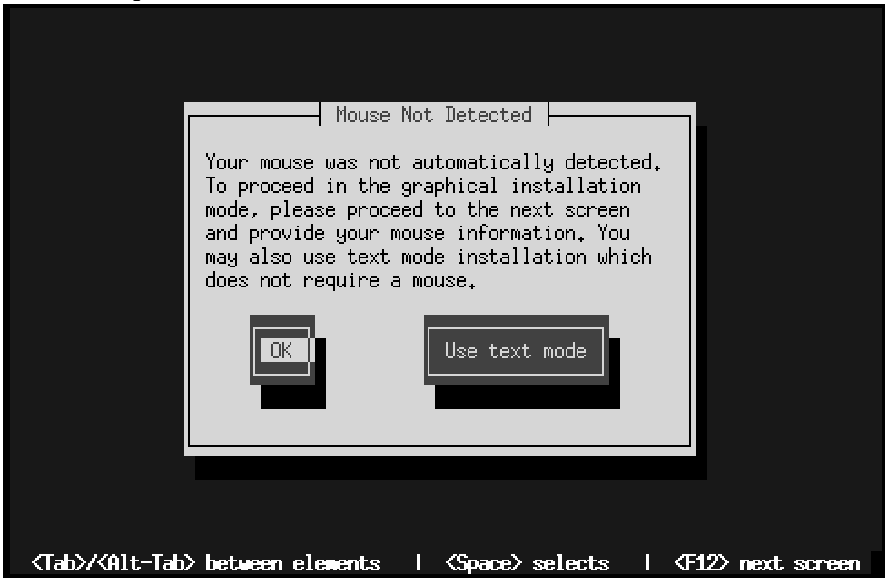
```
boot: linux isa
```

Bitte beachten

Wenn der Bildschirm **Maus nicht erkannt** erscheint (siehe Abbildung 15–1, *Maus nicht erkannt*), war das Installationsprogramm nicht in der Lage, Ihre Maus korrekt zu identifizieren.

Sie können nun wahlweise mit der Installation über die grafische Benutzeroberfläche fortfahren, oder zur Installation im Textmodus wechseln. Für die Installation im Textmodus ist keine Maus erforderlich. Wenn Sie sich dazu entscheiden, mit der Installation im Grafikmodus fortzufahren, müssen Sie dem Installationsprogramm die Konfigurationsinformationen zu Ihrer Maus mitteilen (siehe Abbildung 15–4, *Konfigurieren der Maus*).

Abbildung 15–1 Maus nicht erkannt



Anweisungen zur textbasierten Installation der Klasse Workstation finden Sie im *Offiziellen Red Hat Linux Installationshandbuch*.

Informationen zu benutzerspezifischen Anweisungen für die Installation im Textmodus finden Sie in Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm*.

Bitte beachten

Die ersten Bootmeldungen verweisen nicht auf SCSI- oder Netzwerkkarten. Dies ist normal, da diese Geräte durch Module unterstützt werden, die erst im Laufe des Installationsvorgangs geladen werden.

Sie können dem Kernel auch Optionen übergeben.

Wenn Sie den Kernel beispielsweise zur Verwendung des gesamten Speichers in einem System mit 128 MB Hauptspeicher anweisen möchten, geben Sie folgenden Befehl ein:

```
boot: linux mem=128M
```

Drücken Sie nach Eingabe der Optionen die [Eingabetaste], um unter Verwendung der festgelegten Optionen zu booten.

Wenn Sie Bootoptionen für die Erkennung Ihrer Hardware angeben müssen, notieren Sie diese, da die Optionen später beim Konfigurieren von LILO während des Installationsvorgangs angegeben werden müssen (siehe Abschnitt 15.16, *Installieren von LILO* für weitere Informationen).

Booten ohne Disketten

Die CD-ROM für Red Hat Linux/Intel kann von neueren Computern auch direkt gebootet werden, sofern diese das Booten von CD-ROM unterstützen. Nicht alle Computer unterstützen dieses Funktionsmerkmal. Falls Ihr Computer diese Funktion nicht unterstützt, gibt es noch eine andere Möglichkeit, die Installation ohne Bootdiskette zu starten. Diese Möglichkeit ist jedoch Computern auf Intel-Basis vorbehalten.

Wenn MS-DOS auf Ihrem System installiert ist, können Sie direkt vom CD-ROM-Laufwerk booten, ohne dass Sie eine Bootdiskette verwenden müssen.

Geben Sie hierzu die folgenden Befehle ein (die CD-ROM befindet sich in diesem Beispiel im Laufwerk `d:`):

```
C:\> d:
D:\> cd \dosutils
```

```
D:\dosutils> autoboot.bat
```

Beachten Sie, dass dieser Befehl nicht in einem DOS-Fenster ausgeführt werden kann. Die Datei `autoboot.bat` kann nur mit DOS als alleinigem Betriebssystem ausgeführt werden, d.h. Windows darf nicht aktiv sein.

Wenn Ihr Computer das Booten von CD-ROM nicht unterstützt und auch das DOS-basierte automatische Booten nicht möglich ist, müssen Sie auf eine Bootdiskette zurückgreifen.

15.3 Auswählen einer Installationsart

Als nächsten Schritt müssen Sie festlegen, welche Installationsart Sie verwenden möchten. Sie können Red Hat Linux mit einer der folgenden grundlegenden Methoden installieren:

CD-ROM

Wenn Sie über ein CD-ROM-Laufwerk und die Red Hat Linux-CD-ROM verfügen. Sie benötigen eine Bootdiskette, eine bootfähige CD-ROM oder eine PCMCIA-Bootdiskette.

Festplatte

Wenn Sie die Red Hat Linux-Dateien auf eine lokale Festplatte kopiert haben. Hinweise zur Festplatteninstallation siehe Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm*. Sie benötigen eine Bootdiskette oder eine PCMCIA-Bootdiskette.

NFS-Image

Wenn Sie die Installation von einem NFS-Server aus vornehmen, der die Red Hat Linux-CD-ROM oder eine gespiegelte Kopie von Red Hat Linux exportiert. Sie benötigen eine Netzwerk- oder PCMCIA-Bootdiskette. Anweisungen zur Installation über ein Netzwerk, siehe Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm*. Beachten Sie bitte, dass NFS-Installationen auch im GUI-Modus durchgeführt werden können.

FTP

Wenn Sie die Installation direkt von einem FTP-Server aus vornehmen. Sie benötigen eine Netzwerk- oder PCMCIA-Bootdiskette. Anweisungen zur FTP-Installation, siehe Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm*.

HTTP

Wenn Sie die Installation direkt von einem HTTP-Webserver aus vornehmen. Sie benötigen eine Netzwerk- oder PCMCIA-Bootdiskette. Anweisungen zur HTTP-Installation, siehe Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm*.

15.4 Starten der Installation

Wenn Sie die Installation von CD-ROM unter Verwendung der grafischen Benutzeroberfläche des Installers ausführen möchten, lesen Sie bitte weiter.

Bitte beachten

Falls Sie lieber eine Installation im Textmodus durchführen möchten, müssen Sie Ihr System neu starten und am Prompt `boot:` den Befehl **`text`** eingeben. Weitere Anweisungen hierzu, siehe Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm*.

15.4.1 Installieren von CD-ROM

Falls Sie Red Hat Linux von CD-ROM installieren möchten, wählen Sie "CD-ROM" und klicken anschließend auf **OK**. Legen Sie die Red Hat Linux CD-ROM in das CD-ROM-Laufwerk ein, wenn Sie dazu aufgefordert werden (falls Sie nicht schon von CD-ROM gebootet haben). Wählen Sie anschließend **OK**, und drücken Sie danach die [Eingabetaste].

Das Installationsprogramm sucht in Ihrem System nach einem CD-ROM-Laufwerk, und zwar zunächst nach einem IDE- bzw. ATAPI-Laufwerk. Falls ein solches Laufwerk vorhanden ist, wird die Installation mit dem nächsten Schritt fortgesetzt (siehe Abschnitt 15.5, *Auswählen der Sprache*).

Anderenfalls müssen Sie angeben, über welchen Typ von CD-ROM-Laufwerk Sie verfügen. Sie können die folgenden Laufwerksarten auswählen:

SCSI

Wählen Sie diese Option, wenn Ihr CD-ROM-Laufwerk an einen unterstützten SCSI-Adapter angeschlossen ist. Sie werden aufgefordert, einen SCSI-Treiber auszuwählen. Wählen Sie den Treiber aus, der Ihrem Adapter am ehesten entspricht. Geben Sie nötigenfalls zusätzliche Parameter für den Treiber an. Die meisten Treiber werden Ihren SCSI-Adapter jedoch automatisch erkennen.

Andere

CD-ROM-Laufwerke, die weder zu IDE noch zu SCSI gehören, sind unter der Option "Anderes CD-ROM-Laufwerk" erfasst. Soundkarten mit proprietären CD-ROM-Schnittstellen sind hierfür ein gutes Beispiel. Das Installationsprogramm bietet Ihnen eine Liste mit Treibern für die unterstützten CD-ROM-Laufwerke an. Wählen Sie den passenden Treiber aus, und geben Sie nötigenfalls zusätzliche Parameter an.

Tipp

Eine partielle Liste der optionalen Parameter für CD-ROM-Laufwerke finden Sie im Anhang A, *Allgemeine Parameter und Module*.

Wie müssen Sie vorgehen, wenn das IDE CD-ROM-Laufwerk nicht erkannt wird?

Wenn das Installationsprogramm Ihr IDE (ATAPI) CD-ROM-Laufwerk nicht erkennt und Sie fragt, welche Art von Laufwerk Sie verwenden, müssen Sie das Installationsprogramm neu starten und am Prompt `boot:` den Befehl **`linux hdX=cdrom`** eingeben. Ersetzen Sie das ***X*** durch einen der folgenden Buchstaben, je nachdem, an welcher Schnittstelle sich Ihr CD-ROM-Laufwerk befindet und ob es als Master oder Slave konfiguriert ist:

- a - erster IDE-Controller, Master
- b - erster IDE-Controller, Slave
- c - zweiter IDE-Controller, Master
- d - zweiter IDE-Controller, Slave

(Wenn Sie über einen dritten und/oder vierten Controller verfügen, fahren Sie mit der alphabetischen Zuweisung entsprechend fort.)

Sobald Ihr CD-ROM-Laufwerk erkannt wurde, werden Sie aufgefordert, die Red Hat Linux CD-ROM in das Laufwerk einzulegen. Klicken Sie anschließend auf **OK**. Nach kurzer Wartezeit wird das nächste Dialogfeld eingeblendet.

Nach dem Starten zeigt das Installationsprogramm den Bildschirm zur Sprachauswahl an.

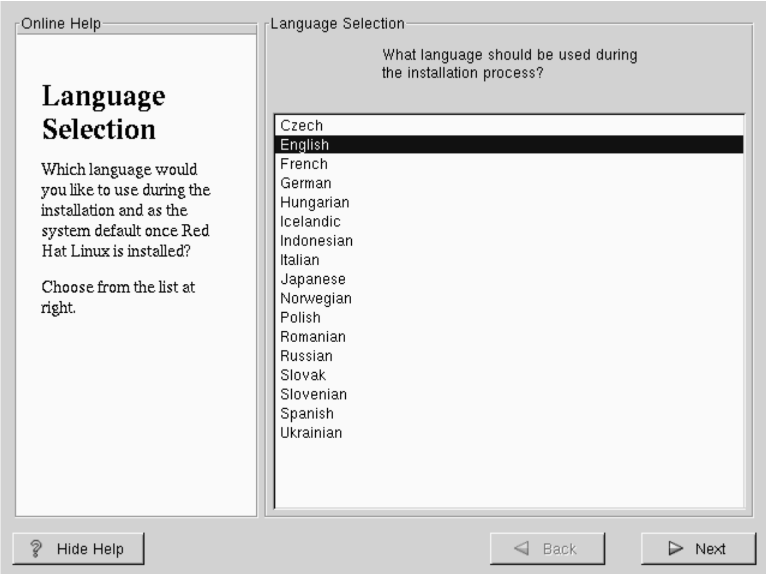
Bitte beachten

Wenn Sie den Installationsvorgang zum jetzigen Zeitpunkt abbrechen möchten, müssen Sie lediglich Ihren Rechner neu starten und die Bootdiskette oder CD-ROM aus dem jeweiligen Laufwerk entnehmen. Sie können die Installation bei jedem Schritt vor Erreichen des Bildschirms **Installation wird vorbereitet** abbrechen, siehe Abschnitt 15.23, *Installation wird vorbereitet*.

15.5 Auswählen der Sprache

Wählen Sie mit der Maus die gewünschte Sprache aus, die für die Installation und als Standardeinstellung für das System verwendet werden soll (siehe Abbildung 15–2, *Auswählen der Sprache*).

Abbildung 15–2 Auswählen der Sprache



15.6 Konfigurieren der Tastatur

Wählen Sie das Modell aus, das am besten zu Ihrem System passt (siehe Abbildung 15–3, *Konfigurieren der Tastatur*). Wenn Sie keinen exakten Eintrag für Ihre Tastatur finden, wählen Sie die für Ihren Tastaturtyp am besten geeignete **generische** Tastatur aus (beispielsweise eine **generische PC-Tastatur mit 101 Tasten**).

Wählen Sie dann den richtigen Belegungstyp für die Tastatur aus (z.B. Deutsch).

Die Eingabe von Sonderzeichen (wie Ñ, Ô und Ç) erfolgt mit der so genannten Dead-Key-Funktion, bei der nacheinander verschiedene Tasten gedrückt und dadurch zu einer Tastenfolge kombiniert werden. Die Dead-Key-Funktion ist standardmäßig aktiviert. Wenn Sie diese Funktion nicht nutzen möchten, wählen Sie die Option **Dead Keys deaktivieren** aus.

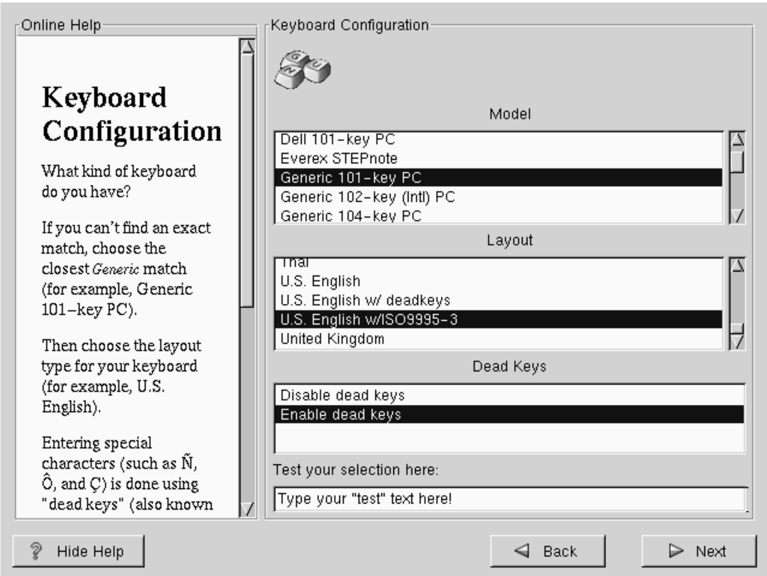
Zum Testen Ihrer Tastaturkonfiguration können Sie in das leere Textfeld am unteren Rand des Bildschirms Text eingeben.

Tipp

Wenn Sie nach der Installation Ihren Tastaturtyp ändern möchten, müssen Sie sich als **Root** anmelden und den Befehl `/usr/sbin/kbdconfig` verwenden. Sie haben auch die Möglichkeit, den Befehl `setup` am Prompt Ihres `Root`-Accounts einzugeben.

Um zum Root-Account zu wechseln, müssen Sie am Shell Prompt in einem Terminalfenster **`su`** eingeben und dann die [Eingabetaste] drücken. Geben Sie anschließend das Root-Passwort ein, und drücken Sie noch einmal die [Eingabetaste].

Abbildung 15–3 Konfigurieren der Tastatur



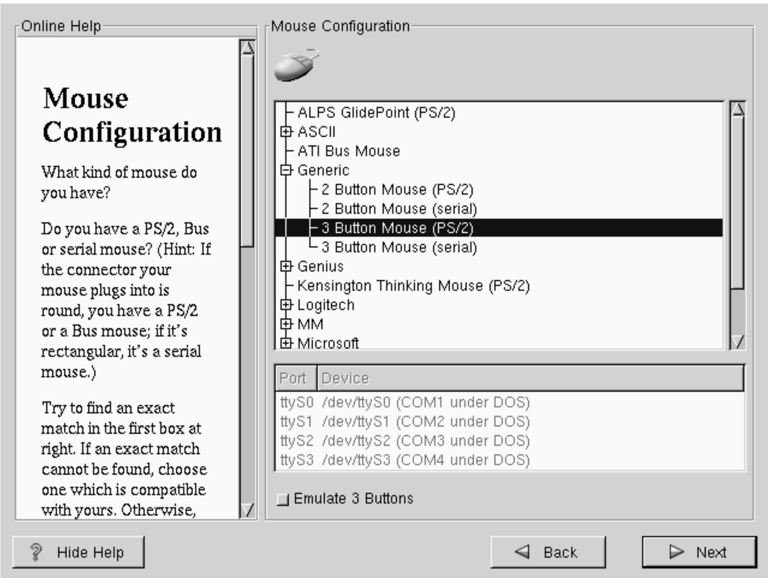
15.7 Konfigurieren der Maus

Wählen Sie jetzt den richtigen Maustyp für Ihr System aus. Wenn Sie keine genaue Entsprechung finden, wählen Sie einen Maustyp, bei dem Sie sicher sind, dass er mit Ihrem System kompatibel ist (siehe Abbildung 15–4, *Konfigurieren der Maus*).

Die Schnittstelle Ihrer Maus können Sie ermitteln, indem Sie überprüfen, auf welche Weise das Mauskabel an Ihr System angeschlossen ist. Wenn der Stecker am Ende des Mauskabels mit einem rechteckigen Port verbunden ist, handelt es sich um eine serielle Maus. Wenn der Port rund ist, haben Sie eine PS/2-Maus. Falls Sie Red Hat Linux auf einem Laptop-Computer installieren, so ist das Zeigegerät in den meisten Fällen PS/2-kompatibel.

Wenn Sie keine Maus finden können, die mit Ihrem System kompatibel ist, wählen Sie einen der **generischen** Einträge. Stützen Sie Ihre Auswahl hierbei auf die Anzahl der Maustasten und die Mausschnittstelle.

Abbildung 15–4 Konfigurieren der Maus



Wenn Sie eine PS/2- oder eine Bus-Maus haben, müssen Sie den Port und die Gerätebezeichnung nicht angeben. Wenn Sie eine serielle Maus haben, müssen Sie den richtigen Port und die Gerätebezeichnung wählen, an den Ihre serielle Maus angeschlossen ist.

Das Kontrollkästchen **Drei Tasten emulieren** ermöglicht es Ihnen, eine Zwei-Tasten-Maus auf gleiche Weise wie eine Drei-Tasten-Maus zu verwenden. Das X Window System kann im Allgemeinen am einfachsten mit einer Drei-Tasten-Maus bedient werden. Wenn Sie dieses Kontrollkästchen aktivieren, können Sie eine dritte, "mittlere" Maustaste emulieren, indem Sie beide Maustasten gleichzeitig drücken.

Tipp

Wenn Sie die Mauskonfiguration nach der Installation ändern möchten, müssen Sie sich zunächst als Root anmelden. Geben Sie dann am Shell Prompt den Befehl `/usr/sbin/mouseconfig` ein.

Wenn Sie Ihre Maus für Linkshänder einrichten möchten, können Sie die Belegung der Maustasten vertauschen. Hierzu können Sie am Shell Prompt den Befehl `gpm -B 321` eingeben, nachdem das Red Hat Linux System gestartet wurde.

15.8 Willkommen bei Red Hat Linux

Im **Willkommensbildschirm** (siehe Abbildung 15–5, *Willkommen bei Red Hat Linux*) werden Sie nicht aufgefordert, Befehle für die Installation einzugeben. Lesen Sie sich einfach den Hilfetext auf der linken Seite des Bildschirms durch, wo Sie weitere Anweisungen erhalten und erfahren, wie Sie Ihr offizielles Red Hat Linux Produkt registrieren können.

Abbildung 15–5 Willkommen bei Red Hat Linux

Beachten Sie bitte den Button **Hilfe ausblenden** in der linken unteren Ecke des Bildschirms. Der Hilfebildschirm wird standardmäßig angezeigt, kann jedoch durch Klicken auf den Button **Hilfe ausblenden** jederzeit minimiert werden.

Klicken Sie zum Fortfahren auf den Button **Weiter**.

15.9 Installationsoptionen

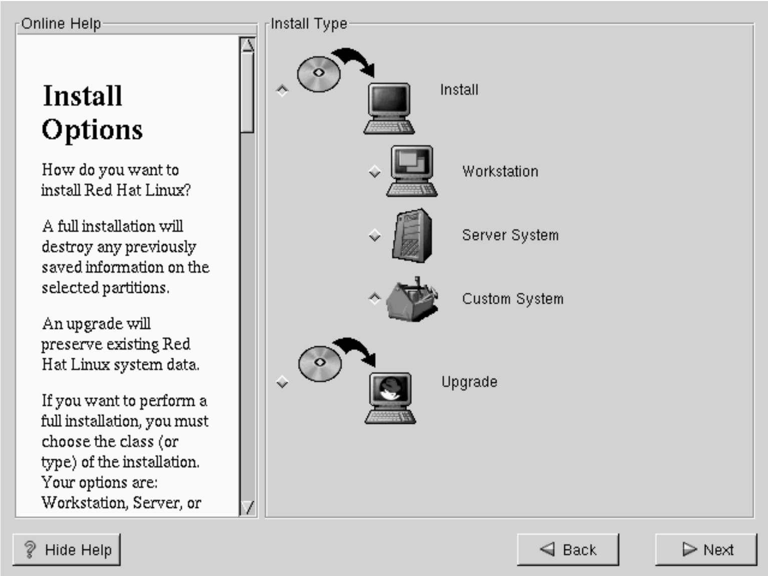
Bitte beachten

`Funktionsmerkmal:` Red Hat Linux 7.0 verfügt über eine Installationsart, die als "partitionslose" Installation bezeichnet wird. Wenn auf Ihrem System eine FAT-Partition (DOS/Windows) mit ausreichend freiem Platz vorhanden ist, können Sie Red Hat Linux installieren, ohne die Festplatte neu partitionieren zu müssen. Diese Methode ist vor allem für Benutzer geeignet, die sich mit Linux noch nicht auskennen und Red Hat Linux ausprobieren möchten, ohne größere Änderungen an ihrem System vornehmen zu müssen. Falls Sie mehr über diese Installationsart erfahren möchten, lesen Sie dazu bitte das Kapitel *Installation ohne Partitionieren* im *Offiziellen Red Hat Linux Installationshandbuch*.

Legen Sie zunächst fest, ob Sie eine vollständige Installation oder ein Upgrade ausführen möchten (siehe Abbildung 15–6, *Installieren oder Aktualisieren*).

In der rechten oberen Ecke des Bildschirms **Installationstyp** befindet sich ein Kontrollkästchen, das Sie aktivieren können, wenn Sie eine Partitionierung mit fdisk vornehmen möchten. Bitte beachten Sie in diesem Zusammenhang, dass fdisk nicht so intuitiv bedient werden kann wie Disk Druid und dass dieses Kontrollkästchen daher standardmäßig deaktiviert ist. Wenn Sie fdisk bislang noch nicht verwendet haben, sollten Sie sich sowohl über fdisk als auch über Disk Druid informieren, um dann das für Sie am besten geeignete Tool zum Partitionieren auszuwählen.

Abbildung 15–6 Installieren oder Aktualisieren



Falls Sie eine Aktualisierung durchführen möchten, lesen Sie hierzu bitte das Kapitel *Aktualisieren des vorhandenen Systems* im *Offiziellen Red Hat Linux Installationshandbuch*.

15.10 Fortfahren mit der Installation

In der Regel installieren Sie Red Hat Linux auf einer oder mehreren neu eingerichteten Partitionen der Festplatte oder über eine bereits vorhandene Version von Linux.

WARNUNG

Wenn Sie Red Hat Linux über eine bereits vorhandene Version von Linux (auch Red Hat Linux) installieren, werden *alle* Informationen (Dateien und Daten) der früheren Version überschrieben. Sichern Sie deshalb alle wichtigen Dateien! Falls Sie die in Ihrem System gespeicherten Daten beibehalten möchten, ohne ein eigenes Backup zu erstellen, sollten Sie eine Aktualisierung in Erwägung ziehen.

Wenn Sie sich für eine vollständige Installation entscheiden, müssen Sie auch die gewünschte Installationsklasse festlegen. Folgende Optionen stehen zur Verfügung: **Workstation**, **Server** oder **Benutzerdefiniert**.

Für neue Benutzer ist die Installationsklasse Workstation am besten geeignet. Sie installiert je nach der von Ihnen getroffenen Auswahl eine GNOME- oder KDE-Desktopumgebung (oder beides) sowie das X Window System.

WARNUNG

Wenn die Festplatte für Linux und Windows NT gemeinsam genutzt werden soll, dürfen Sie diese Methode nicht verwenden, da Windows NT sonst nicht mehr gestartet werden kann. LILO überschreibt den Bootloader von NT, und Sie können NT nicht mehr booten. Sie müssen eine benutzerdefinierte Installation durchführen und LILO so konfigurieren, dass er nicht im Master Boot Record (MBR) installiert wird.

Bei der Einrichtung einer Dual-Boot-Umgebung auf einem System, auf dem NT installiert ist, müssen Sie LILO statt im MBR im ersten Sektor der Root-Partition installieren. Sie müssen in diesem Fall unbedingt eine Bootdiskette erstellen. In diesem Fall müssen Sie zum Starten von Linux entweder eine Bootdiskette verwenden oder den Loader von Windows NT so konfigurieren, dass LILO vom ersten Sektor der Root-Partition gestartet wird. Weitere Informationen zum Einrichten von LILO und NT finden Sie unter http://www.linuxdoc.org/HOWTO/mini/Linux+NT-Loader.html. Bitte lesen Sie sich diese Informationen sorgfältig durch.

WARNUNG

Bei einer Workstation-Installation werden *alle Daten aller Linux-Partitionen* auf *allen* Festplatten des Computers gelöscht.

Im Folgenden ist aufgeführt, wie viel Festplattenplatz mindestens für eine Installation der Klasse Workstation erforderlich ist.

- Workstation mit GNOME - 900 MB
- Workstation mit KDE - 900 MB
- Workstation mit GNOME und KDE - 1,1 GB

Falls Sie vorhaben, alle Gruppenpakete (GNOME ist z.B. eine Paketgruppe) sowie alle zusätzlichen individuellen Pakete auszuwählen, sollten Sie dafür 1,7 GB oder mehr an Festplattenplatz vorsehen. Auf diese Weise steht Ihnen außerdem etwas Platz zum Schreiben von zusätzlichen Daten zur Verfügung.

Bitte beachten

Im Unterschied zu früheren Workstation-Installationen wird bei der Red Hat Linux 7.0 Workstation-Installation der Netzwerkdämon xinetd nicht installiert (inet-Dienste). Wird xinetd nicht installiert, erhöht sich die Sicherheit der Installation. Allerdings arbeiten ankommende, [1]netzwerk-bezogene Dienste wie Finger, Telnet, Talk und FTP nicht. Wenn Sie diese Dienste benötigen, sollten Sie eine Installation der Klassen Server oder Benutzerdefiniert auswählen.

Eine Server-Installation ist am besten geeignet, wenn Ihr System als Linux-basierter Server verwendet werden soll, ohne dass Sie sich im Detail mit der Systemkonfiguration befassen möchten.

Im Folgenden ist aufgeführt, wie viel Festplattenplatz mindestens für eine Installation der Klasse Server erforderlich ist.

- Server (mindestens) - 450 MB
- Server (alle Pakete) - 1 GB

[1] Ankommende Dienste bedeutet, dass Sie z.B. über Telnet hinauswählen, andere Systeme sich jedoch nicht über Telnet in Ihr System einwählen können.

Falls Sie vorhaben, alle Gruppenpakete sowie zusätzliche individuelle Pakete auszuwählen, sollten Sie dafür 1,7 GB oder mehr an Festplattenplatz vorsehen. Auf diese Weise steht Ihnen außerdem etwas Platz zum Schreiben von zusätzlichen Daten zur Verfügung.

WARNUNG

Bei einer Server-Installation werden *alle Partitionen* (sowohl Linux- als auch Nicht-Linux-Partitionen) auf *allen* Festplatten des Computers gelöscht.

Die *benutzerdefinierte Installation* gibt Ihnen das größte Maß an Flexibilität beim Installationsvorgang. Bei den Installationsklassen Workstation und Server läuft der Installationsvorgang automatisch ab, und einige Schritte werden übergangen. Bei einer benutzerdefinierten Installation haben Sie auch die Möglichkeit, die Festplatte *nach Ihren Wünschen* zu partitionieren Sie haben die vollständige Kontrolle darüber, welche Pakete im System installiert werden. Sie können auch festlegen, ob Sie LILO (den LInux LOader) für das Booten Ihres Systems verwenden möchten. Wenn Sie noch keine Erfahrung mit Linux haben, sollten Sie die benutzerdefinierte Installation nicht verwenden.

Im Folgenden ist aufgeführt, wie viel Festplattenplatz mindestens für eine Installation der Klasse Benutzerdefiniert erforderlich ist.

- Benutzerdefiniert (mindestens) - 250 MB
- Benutzerdefiniert (alles) - 1,7 GB

Falls Sie erfahren möchten, welche Schritte übersprungen werden, wenn Sie keine Installation der Klasse Benutzerdefiniert vornehmen, lesen Sie hierzu bitte *Schritt 6 - Ist eine Workstation-Installation die optimale Lösung für Sie?* im *Offiziellen Red Hat Linux Installationshandbuch*.

15.11 Automatisches Partitionieren

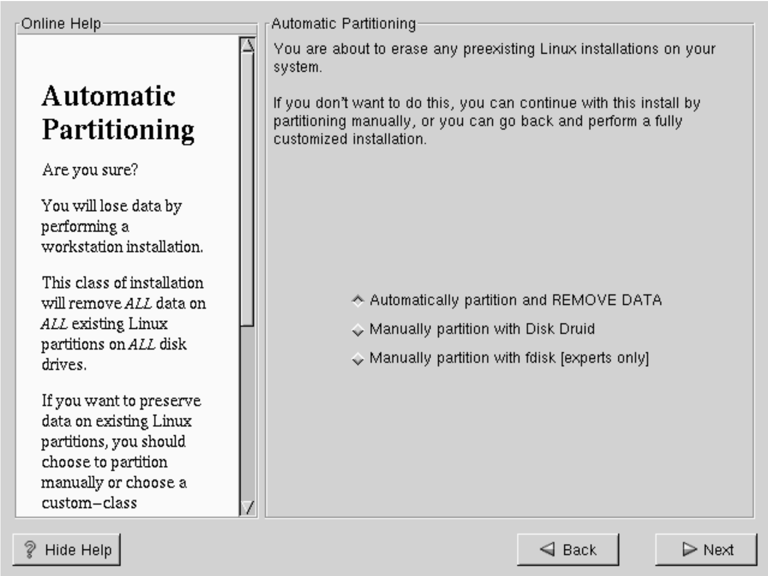
Das automatische Partitionieren ermöglicht Ihnen das Installieren von Linux, ohne dass Sie Ihre Festplatte(n) selbst partitionieren müssen. Wenn Sie mit dem Partitionieren Ihres Systems noch nicht vertraut sind, empfiehlt es sich, dass Sie die Festplatte(n) *nicht* manuell partitionieren, sondern stattdessen die Partitionierung automatisch durch das Installationsprogramm vornehmen lassen.

Der Bildschirm **Automatisch partitionieren** wird nur angezeigt, wenn Sie eine Installation der Klassen Workstation oder Server durchführen. Falls Sie eine benutzerdefinierte Installation durchführen oder Ihr System manuell partitionieren, finden Sie in Abschnitt 15.13, *Partitionieren des Systems* weitere Informationen.

In diesem Bildschirm können Sie wählen, ob Sie diese Installation fortsetzen, eine manuelle Partitionierung durchführen oder durch Klicken auf den Button **Zurück** eine andere Installationsart auswählen möchten (siehe Abbildung 15–7, *Automatisches Partitionieren*).

Wenn Sie *weder einige noch alle* Daten verlieren möchten, sollten Sie entweder die manuelle Partitionierung oder eine andere Installationsklasse wählen.

Abbildung 15–7 Automatisches Partitionieren



ACHTUNG

Bei einer Workstation-Installation werden alle Daten in allen vorhandenen Linux-Partitionen gelöscht.

Wenn Sie Red Hat Linux nicht im Master Boot Record (MBR) installieren oder einen anderen Bootmanager als LILO verwenden möchten, sollten Sie diese Installationsart nicht wählen.

ACHTUNG

Bei einer Server-Installation werden alle Daten in allen Partitionen auf allen Festplatten gelöscht.

Wenn Sie ein anderes installiertes Betriebssystem auf Ihrem System beibehalten möchten und Red Hat Linux nicht im Master Boot Record (MBR) installiert werden soll, oder Sie einen anderen Bootmanager als LILO verwenden möchten, wählen Sie nicht diese Installationsart.

Falls Sie sich noch nicht sicher sind, wie Ihr System partitioniert werden soll, lesen Sie bitte Anhang B, *Eine Einführung in Festplattenpartitionen*.

15.12 Manuelles Partitionieren

`Das manuelle Partitionieren` ermöglicht es Ihnen, Linux zu installieren und dabei Ihr(e) Laufwerk(e) selbst zu partitionieren. Falls Sie sich nicht sicher genug fühlen, um Ihr System selbst zu partitionieren, sollten Sie *auf keinen Fall* die Option zum manuellen Partitionieren auswählen, sondern stattdessen die Option zum **automatischen Partitionieren**. Dazu klicken Sie auf **Zurück** und wählen dann eine Installation der Klasse Workstation oder Server aus.

Abbildung 15–8 Manuelles Partitionieren

15.13 Partitionieren des Systems

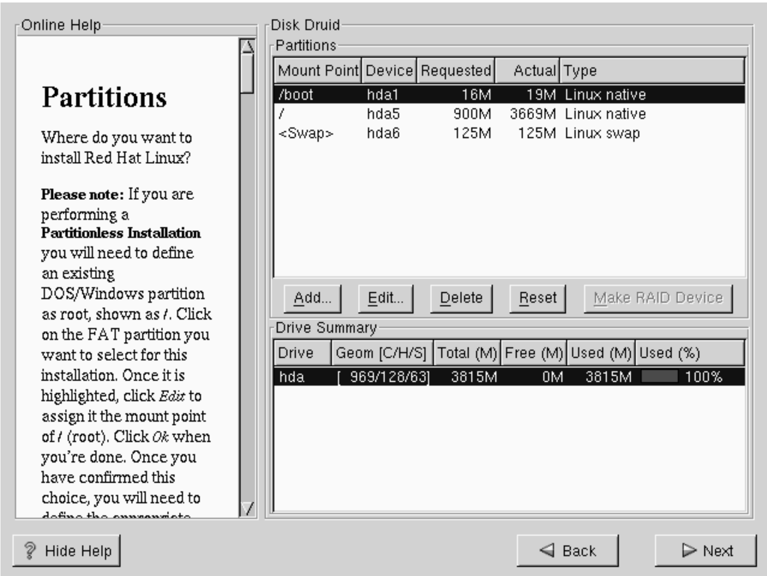
Wenn Sie eine Workstation- oder Server-Installation ausführen und *keine* manuelle Partitionierung durchführen möchten, fahren Sie mit Abschnitt 15.17, *Konfigurieren des Netzwerks* fort.

Legen Sie nun fest, wo Red Hat Linux installiert werden soll. Definieren Sie hierfür in allen Festplattenpartitionen, in denen Red Hat Linux installiert wird, Mountpoints. Gegebenenfalls müssen Sie Partitionen erstellen und/oder löschen (weitere Informationen finden Sie in Abbildung 15–9, *Partitionieren mit Disk Druid*).

Bitte beachten

Wenn Sie sich noch nicht sicher sind, wie Sie Ihre Partitionen einrichten sollen, lesen Sie bitte Anhang B, *Eine Einführung in Festplattenpartitionen*. Als Mindestanforderung benötigen Sie eine ausreichend große Root-Partition und eine Swap-Partition von mindestens 16 MB.

Abbildung 15–9 Partitionieren mit Disk Druid



Disk Druid ist das Partitionierungstool, das in Red Hat Linux 7.0 verwendet wird. Das Tool Disk Druid ist für die Partitionierung während einer normalen Installation von Red Hat Linux völlig ausreichend. Nur bestimmte, ganz ausgefallene Ausgangssituationen kann es nicht meistern.

15.13.1 Felder im Bereich Partitionen

Jede Zeile im Bereich "Partitionen" entspricht einer Festplattenpartition. Die einzelnen Zeilen sind in fünf Felder unterteilt:

Mountpoint:

Bei einem Mountpoint handelt es sich um den Ort in der Verzeichnishierarchie, an dem ein Laufwerk bzw. eine Partition eingebunden wird. In diesem Zusammenhang wird auch häufig davon gesprochen, dass das Laufwerk an diesem Ort gemountet wird. Dieses Feld gibt an, wo die Partition eingebunden wird. Wenn eine Partition vorhanden, aber "nicht gesetzt" ist, müssen Sie ihren Mount-Point definieren. Doppelklicken Sie auf die Partition, oder klicken Sie auf den Button **Bearbeiten**.

Gerät:

In diesem Feld wird der Gerätename der Partition angezeigt.

Angefordert:

In diesem Feld wird die ursprüngliche Größe der Partition angezeigt. Wenn Sie die Größe neu definieren möchten, müssen Sie die aktuelle Partition löschen und dann mit Hilfe des Buttons **Hinzufügen** neu erstellen.

Tatsächlich:

In diesem Feld wird der Speicherplatz angezeigt, der der Partition gegenwärtig zugewiesen ist.

Typ:

In diesem Feld wird der Partitionstyp angezeigt (wie Linux Native oder DOS).

15.13.2 Empfohlenes Partitionierungsschema

Sie sollten im Normalfall die folgenden Partitionen erstellen (es sei denn, Sie haben besondere Gründe für eine abweichende Partitionierung):

- Eine Swap-Partition (mindestens 16 MB) - Swap-Partitionen dienen zur Unterstützung des **virtuellen Speichers**. Dies bedeutet, dass die Daten in eine Swap-Partition geschrieben werden, wenn nicht ausreichend RAM zum Speichern der

Daten vorhanden ist, die Ihr System gerade verarbeitet. Falls Ihr Computer über 16 MB RAM oder weniger verfügt, *müssen* Sie eine Swap-Partition erstellen. Auch wenn Sie mehr Speicher zur Verfügung haben, empfiehlt sich eine Swap-Partition. Die Mindestgröße der Swap-Partition sollte der Größe des Arbeitsspeichers des Computers bzw. 16 MB entsprechen (der jeweils größere Wert sollte verwendet werden). In Disk Druid sollte das Partitionsfeld für `swap` etwa wie folgt aussehen:

```
<Swap>  hda2  125M   125M  Linux swap
```

- Eine `/boot`-Partition (maximal 16 MB) - Die in `/boot` eingebundene Partition enthält den Betriebssystem-Kernel (der erforderlich ist, damit Ihr System Red Hat Linux booten kann) sowie Dateien, die während des Systemstarts verwendet werden. Wegen der Einschränkungen der meisten PC-BIOS-Versionen sollten Sie zur Aufnahme dieser Dateien nur eine kleine Partition erstellen. Sie sollte nicht größer als 16 MB sein. In Disk Druid sollte das Partitionsfeld für `/boot` etwa wie folgt aussehen:

```
/boot  hda1  16M   19M  Linux native
```

- Eine `root`-Partition (900 MB - 1,7 GB) - In dieser Partition befindet sich "`/`" (das Root-Verzeichnis). In dieser Konfiguration befinden sich alle Dateien (mit Ausnahme der in `/boot` gespeicherten Dateien) in der Root-Partition. Eine Root-Partition von 850 MB erlaubt den Umfang einer Workstation-Installation (mit *sehr* wenig freiem Festplattenspeicher), während Sie auf einer Root-Partition von 1,7 GB alle Pakete installieren können. In Disk Druid sollte das Partitionsfeld für `/` etwa wie folgt aussehen:

```
/  hda2  900M   3669M   Linux native
```

15.13.3 Probleme beim Hinzufügen von Partitionen

Wenn Sie versuchen, eine Partition hinzuzufügen, und Disk Druid diese Anforderung nicht ausführen kann, wird ein Dialogfeld mit einer Liste aller Partitionen angezeigt, die zurzeit nicht zugewiesen sind. Außerdem erhalten Sie Informationen, weshalb die Zuweisung nicht möglich war. Nicht zugewiesene Partitionen werden auch im Hauptbildschirm von Disk Druid angezeigt (gegebenenfalls müssen Sie hierzu im Bereich "Partitionen" scrollen, um diese Partitionen zu sehen).

Wenn Sie im Bereich **Partitionen** scrollen, wird möglicherweise in roter Schrift die Meldung angezeigt, dass Partitionen noch nicht zugewiesen wurden ("Nicht zugewiesene angeforderte Partitionen"). Außerdem erfahren Sie, um welche Partitionen es sich dabei handelt. Häufig können Partitionen nicht zugewiesen werden, weil kein ausreichender Festplattenplatz zur Verfügung steht. Der Grund, warum eine Partition nicht zugewiesen werden konnte, wird auf jeden Fall hinter dem für die Partition angeforderten Mount-Point angezeigt.

Um dieses Problem zu beheben, müssen Sie die Partition auf ein anderes Laufwerk verschieben, das über ausreichenden Speicherplatz verfügt, und die Größe der Partition anpassen, damit sie auf das aktuelle Laufwerk passt, oder die Partition vollständig löschen. Wenn Sie auf den Button **Bearbeiten** klicken oder auf die Partition doppelklicken, können Sie Änderungen vornehmen.

15.13.4 Laufwerkszusammenfassungen

Jede Zeile im Bereich **Laufwerkszusammenfassungen** steht für eine in Ihrem Computer installierte Festplatte und umfasst die folgenden Felder:

Laufwerk:

Dieses Feld zeigt den Gerätenamen der Festplatte an.

Geom [Z/K/S]:

Dieses Feld zeigt die **Festplattengeometrie** an. Die Geometrie ergibt sich aus drei Werten, nämlich der Anzahl der Zylinder, Köpfe und Sektoren, wie sie von der Festplatte übermittelt werden.

Gesamt:

Dieses Feld zeigt den auf der Festplatte insgesamt verfügbaren Speicherplatz an.

Frei:

Dieses Feld zeigt, wie viel Speicherplatz der Festplatte noch nicht zugewiesen ist.

Verwendet:

In diesen Feldern wird in Megabyte und als Prozentwert angezeigt, wie groß der aktuell verschiedenen Partitionen zugewiesene Speicherplatz auf der Festplatte ist.

Der Bereich **Laufwerkszusammenfassungen** dient nur der Anzeige der Festplattenkonfiguration Ihres Computers. Hier können keine Festplatten für bestimmte Partitionen ausgewählt werden. Hierzu wird das Feld **Verfügbare Laufwerke** in Abschnitt 15.13.6, *Hinzufügen von Partitionen* verwendet.

15.13.5 Buttons in Disk Druid

Über die Buttons können Sie die Vorgänge in Disk Druid steuern. Im Einzelnen können Partitionen hinzugefügt bzw. gelöscht sowie Attribute der Partitionen geändert werden. Darüber hinaus gibt es Buttons, mit denen Sie vorgenommene Änderungen bestätigen oder Disk Druid beenden können. Im Folgenden werden die einzelnen Buttons erläutert.

Hinzufügen:

Dient zum Erstellen einer neuen Partition. Wenn Sie auf diesen Button klicken, wird ein Dialogfeld mit Feldern (wie beispielsweise Mount-Point und Größe) angezeigt. Diese Felder müssen ausgefüllt werden.

Bearbeiten:

Dient zum Ändern der Attribute der Partition, die aktuell im Bereich "Partitionen" ausgewählt ist. Wenn Sie auf **Bearbeiten** klicken, wird ein Dialogfeld geöffnet. Einige oder alle Felder dieses Dialogfelds können bearbeitet werden, je nachdem, ob die Partitionsdaten bereits auf die Festplatte geschrieben wurden oder nicht.

Löschen:

Dient zum Löschen der Partition, die gerade im Bereich **Aktuelle Partitionen der Festplatte** markiert ist. Sie werden aufgefordert, die Löschung einer Partition zu bestätigen.

Zurücksetzen:

Dient zum Wiederherstellen des ursprünglichen Zustands von Disk Druid. Alle vorgenommenen Änderungen gehen verloren, wenn Sie die Partitionen **zurücksetzen**.

RAID-Gerät erstellen:

RAID-Gerät erstellen kann verwendet werden, wenn Sie Redundanz für bestimmte oder alle Partitionen bereitstellen möchten. *Diese Funktion sollte nur von Benutzern mit ausreichend Erfahrung im Umgang mit RAID verwendet werden.* Weitere Informationen zu RAID, siehe Anhang E, *Redundant Array of Independent Disks (RAID)*.

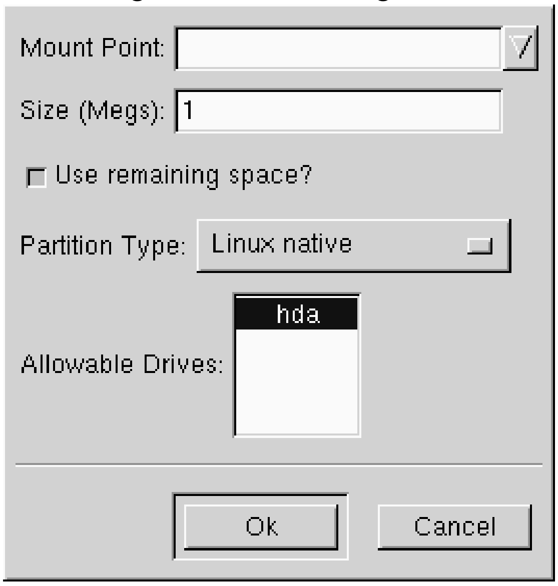
15.13.6 Hinzufügen von Partitionen

Wenn Sie eine neue Partition hinzufügen möchten, klicken Sie auf den Button **Hinzufügen**. Es wird ein Dialogfeld angezeigt (siehe Abbildung 15–10, *Hinzufügen einer Partition*).

Bitte beachten

Sie müssen mindestens eine Partition (wahlweise auch mehrere) für Red Hat Linux reservieren. Weitere Informationen hierzu finden Sie in Anhang B, *Eine Einführung in Festplattenpartitionen*.

Abbildung 15–10 Hinzufügen einer Partition



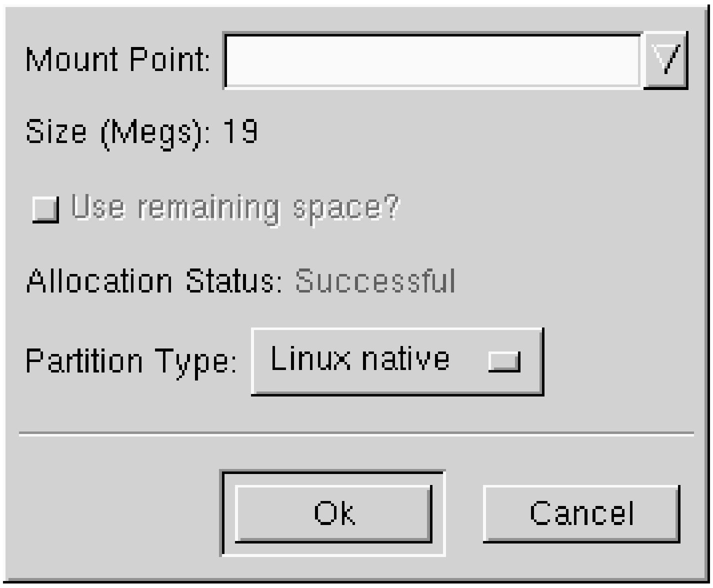
- **Mount-Point**: Klicken Sie in dieses Feld, und geben Sie den Mount-Point für die Partition ein. Geben Sie z.B. für eine Root-Partition `/` oder `/boot` für die Partition `/boot` ein usw. Sie können auch mit der Dropdown-Liste den korrekten Mount-Point für die Partition auswählen.
- **Größe (in MB)**: Geben Sie hier die Größe der Partition (in Megabyte) ein. Beachten Sie bitte, dass in diesem Feld bereits eine "1" vorgegeben ist - wenn Sie diesen Wert nicht ändern, erstellen Sie eine Partition von 1 MB.
- **Verbleibenden Platz verwenden**: Mit diesem Kontrollkästchen können Sie angeben, ob die im darüberliegenden Feld eingegebene Größe als exakte Größe oder als Mindestgröße der Partition verstanden werden soll. Wenn das Kontrollkästchen markiert ist, kann die Partition so weit wachsen, bis sie den gesamten verfügbaren Platz auf der Festplatte einnimmt. Die Partitionsgröße ist variabel und hängt davon ab, wie Sie die anderen Partitionen festlegen. Sie können diese Funktion auch auf mehrere Partitionen anwenden. In diesem Fall wird der zusätzliche freie Speicherplatz zwischen allen "dehnbaren" Partitionen aufgeteilt.

- **Partitionstyp**: Dieses Feld enthält eine Liste verschiedener Partitionstypen (z.B. Linux Native oder DOS). Wählen Sie den entsprechenden Partitionstyp mit der Maus.
- **Verfügbare Laufwerke**: Dieses Feld enthält eine Liste der in Ihrem System installierten Festplatten. Wenn das Kontrollkästchen für eine Festplatte aktiviert ist, kann eine gewünschte Partition auf dieser Festplatte erstellt werden. Wenn das Kontrollkästchen *nicht* aktiviert ist, wird die Partition *definitiv nicht* auf dieser Festplatte erstellt. Über die Kontrollkästchen können Sie selbst festlegen, wo Disk Druid Partitionen anlegen soll, oder aber die Entscheidung Disk Druid überlassen.
- **OK**: Klicken Sie auf **OK**, wenn Sie alle gewünschten Einstellungen vorgenommen haben und die Partition erstellen möchten.
- **Abbrechen**: Klicken Sie auf **Abbrechen**, wenn Sie die Partition nicht erstellen möchten.

15.13.7 Bearbeiten von Partitionen

Wenn Sie eine Partition bearbeiten möchten, klicken Sie auf den Button **Bearbeiten** oder doppelklicken auf die bestehende Partition (siehe Abbildung 15–11, *Bearbeiten von Partitionen*).

Abbildung 15–11 Bearbeiten von Partitionen



Bitte beachten

Wenn die Partition bereits auf Ihrer Festplatte angelegt wurde, können Sie lediglich den Mount-Point dieser Partition ändern. Weitere Änderungen können Sie nur vornehmen, indem Sie die Partition löschen und neu erstellen.

15.13.8 Löschen von Partitionen

Um eine Partition zu löschen, markieren Sie diese im Bereich "Partitionen" und doppelklicken auf den Button **Löschen**. Sie werden aufgefordert, den Löschvorgang zu bestätigen.

In Abschnitt 15.15, *Auswählen der zu formatierenden Partitionen* finden Sie weitere Installationsanweisungen.

15.14 Partitionieren mit fdisk

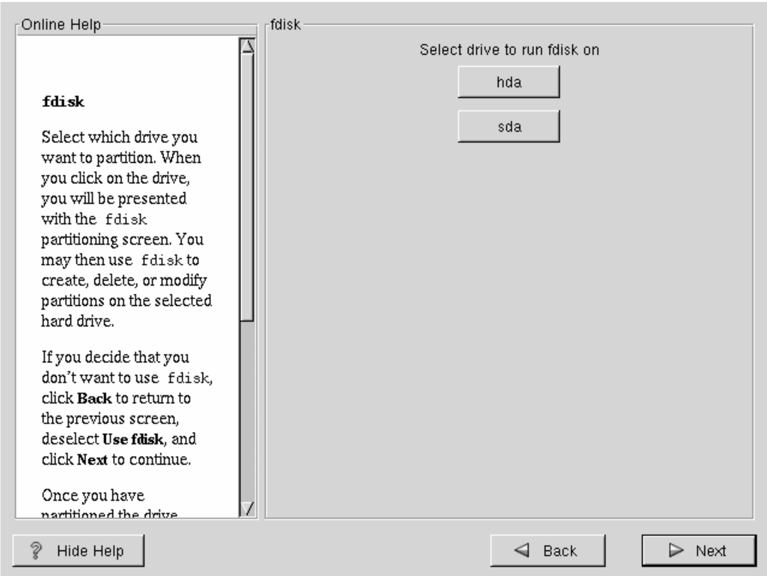
ACHTUNG

Wenn Sie noch nicht mit fdisk gearbeitet haben und mit dessen Funktionsweise nicht vertraut sind, sollten Sie dieses Tool nicht verwenden. Disk Druid ist für Benutzer, die sich mit der Partitionierung von Festplatten noch nicht im Detail auskennen, wesentlich übersichtlicher und einfacher zu bedienen. Um fdisk zu beenden, klicken Sie auf **Zurück**, um in den vorherigen Bildschirm zurückzukehren. Deaktivieren Sie dann das Kontrollkästchen fdisk, und klicken Sie auf **Weiter**.

Dieser Abschnitt ist nur dann für Sie von Interesse, wenn Sie fdisk für die Partitionierung Ihres Systems verwenden möchten. Wenn Sie fdisk nicht verwenden, lesen Sie bitte gleich in Abschnitt 15.11, *Automatisches Partitionieren* (falls Sie Ihr System automatisch partitionieren lassen möchten) oder in Abschnitt 15.13, *Partitionieren des Systems* (falls Sie Disk Druid verwenden) weiter.

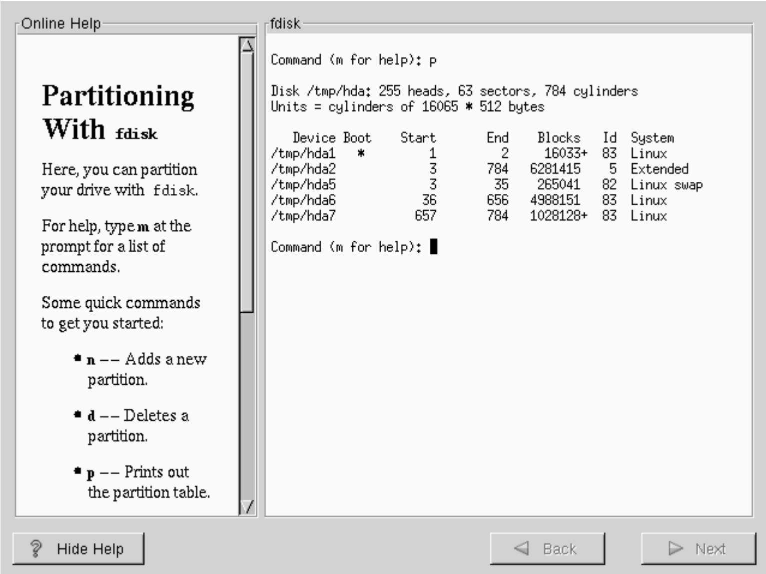
Falls Sie sich für die Verwendung von fdisk entschieden haben, müssen Sie im nächsten Bildschirm (siehe Abbildung 15–12, fdisk) ein Laufwerk für die Partitionierung mit fdisk auswählen.

Abbildung 15–12 fdisk



Sobald Sie das zu partitionierende Laufwerk ausgewählt haben, wird der fdisk Hauptbildschirm angezeigt, in dem Sie verschiedene Befehle eingeben können (siehe Abbildung 15–13, *Partitionieren mit* fdisk). Wenn Sie nicht sicher sind, welchen Befehl Sie verwenden sollen, empfiehlt sich die Eingabe des Befehls [m] am Prompt. Falls Sie weitere Informationen benötigen, enthält das Kapitel 14, *Installieren von Red Hat Linux mit dem Textmodus-Installationsprogramm* einen Überblick über fdisk. Sobald Sie die gewünschten Partitionen angelegt haben, können Sie durch Eingabe von `w` Ihre Änderungen speichern und das Programm beenden. Sie kehren nun zum ursprünglichen fdisk-Bildschirm zurück. In diesem Bildschirm können Sie nun ein anderes Laufwerk zur Partitionierung auswählen oder mit der Installation fortfahren.

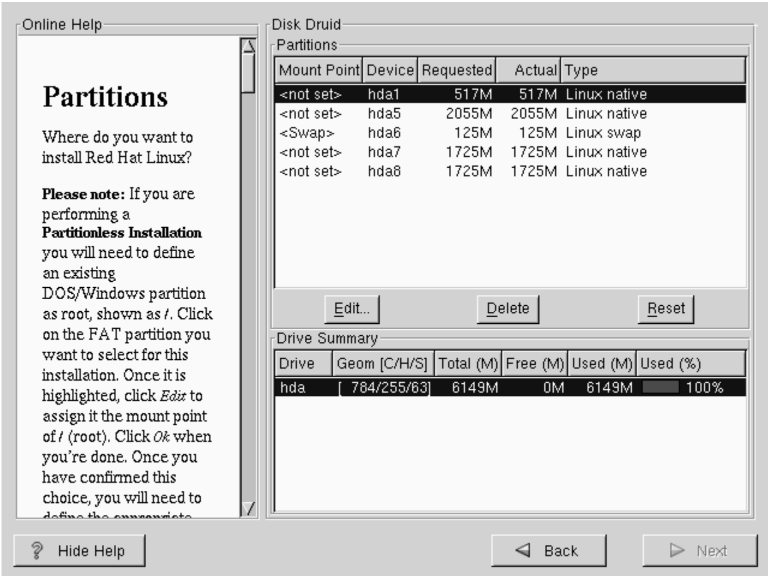
Abbildung 15–13 Partitionieren mit fdisk



Nach dem Partionieren Ihrer Festplatte(n) klicken Sie auf **Weiter**. Sie müssen nun mit Disk Druid Ihren Partitionen **Mount-Points** zuweisen.

Sie können mit Disk Druid keine neuen Partitionen hinzufügen; allerdings können Sie die Mount-Points für die von Ihnen bereits erstellten Partitionen bearbeiten.

Abbildung 15–14 Bearbeiten mit Disk Druid

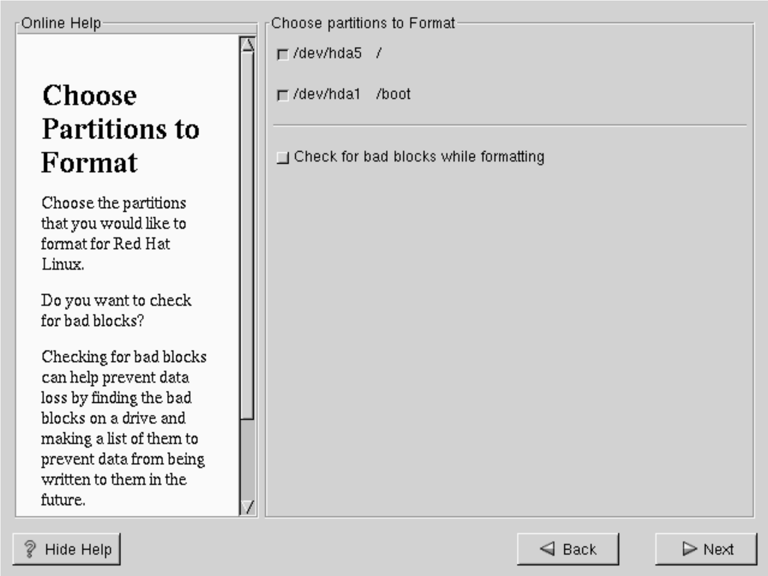


In Abschnitt 15.15, *Auswählen der zu formatierenden Partitionen* finden Sie weitere Installationsanweisungen.

15.15 Auswählen der zu formatierenden Partitionen

Wählen Sie die Partitionen aus, die formatiert werden sollen. Alle neu erstellten Partitionen sollten formatiert werden. Außerdem sollten alle vorhandenen Partitionen, die nicht mehr benötigte Daten enthalten, ebenfalls formatiert werden. Formatieren Sie jedoch keine Partitionen wie `/home` oder `/usr/local`, wenn Sie die darin gespeicherten Daten noch benötigen (siehe Abbildung 15–15, *Auswählen der zu formatierenden Partitionen*).

Abbildung 15–15 Auswählen der zu formatierenden Partitionen



Wenn die Festplatte während der Formatierung des Dateisystems auf defekte Blöcke überprüft werden soll, aktivieren Sie das Kontrollkästchen **Auf defekte Blöcke überprüfen.**

Wenn eine Überprüfung auf defekte Blöcke durchgeführt wird, kann ein Datenverlust dadurch verhindert werden, dass defekte Blöcke auf einer Festplatte erkannt und in einer Liste verzeichnet werden, damit die defekten Blöcke in Zukunft nicht mehr verwendet werden.

Bitte beachten

Durch die Funktion **Auf defekte Blöcke überprüfen** kann sich die für die Installation benötigte Gesamtzeit deutlich erhöhen. Da die meisten neueren Festplatten recht groß sind, kann die Überprüfung auf defekte Blöcke je nach der Größe Ihrer Festplatte eine gewisse Zeit dauern.

15.16 Installieren von LILO

Wenn Sie eine Workstation- oder Server-Installation ausführen, fahren Sie bitte mit Abschnitt 15.18, *Konfigurieren von Zeitzonen* fort.

Normalerweise müssen Sie LILO (den LInux LOader) installieren, um Ihr Red Hat Linux System booten zu können. Sie können LILO an einem von zwei Orten installieren:

Im Master Boot Record (MBR)

Der MBR ist der empfohlene Ort zur Installation von LILO, sofern der MBR nicht bereits einen anderen Betriebssystem-Loader startet, z.B. System Commander oder den Boot-Manager von . Der Master Boot Record ist ein spezieller Bereich auf der Festplatte, der vom BIOS Ihres Computers automatisch geladen wird. Dies ist der früheste Zeitpunkt, ab dem LILO die Steuerung des Bootprozesses übernehmen kann. Wenn Sie LILO im MBR installieren und Ihr Computer gebootet wird, zeigt LILO den Prompt `boot:` an. Sie können dann entweder Red Hat Linux oder ein beliebiges anderes Betriebssystem starten, für das Sie LILO konfigurieren.

Im ersten Sektor der Root-Partition

Dieser Sektor empfiehlt sich, wenn Sie bereits einen anderen Bootloader im System verwenden (z.B. den Boot-Manager von OS/2). In diesem Fall übernimmt zunächst der andere Bootloader die Steuerung. Sie können diesen Bootloader dann zum Booten von LILO konfigurieren (LILO wiederum startet Red Hat Linux).

Wenn Sie LILO installieren möchten, wählen Sie bitte aus, an welchem Ort im System LILO installiert werden soll (siehe Abbildung 15–16, *LILO konfigurieren*). Wenn Sie im System ausschließlich Red Hat Linux verwenden möchten, sollten Sie den Master Boot Record (MBR) auswählen. Bei Systemen, auf denen auch Windows 95/98 installiert ist, sollten Sie LILO im MBR installieren, so dass LILO beide Betriebssysteme starten kann.

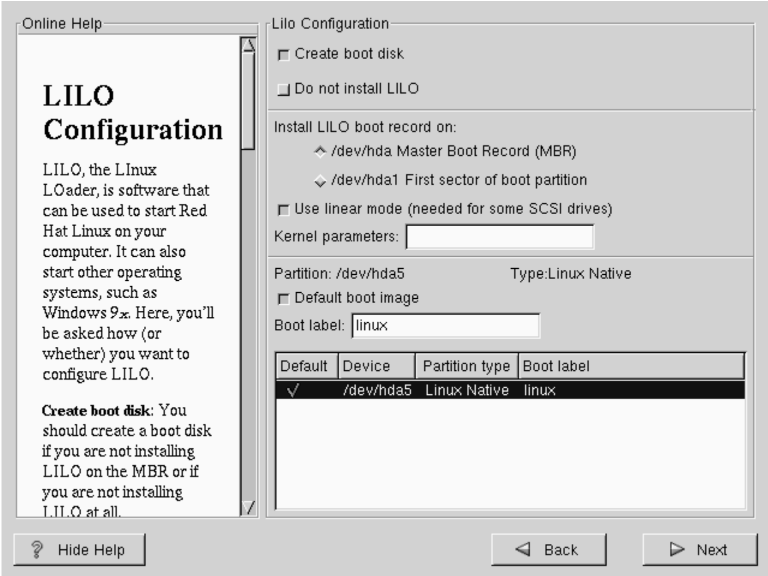
Wenn auf Ihrem System Windows NT installiert ist (und Sie LILO installieren möchten), sollte LILO im ersten Sektor der Root-Partition und nicht im MBR installiert werden. Sie müssen in diesem Fall unbedingt eine Bootdiskette erstellen. In diesem Fall müssen Sie zum Starten von Linux entweder eine Bootdiskette verwenden oder den Loader von Windows NT so konfigurieren, dass LILO vom ersten Sektor der Root-Partition gestartet wird. Weitere Informationen über die Konfiguration von LILO und NT finden Sie auf der Website http://www.linuxdoc.org/HOWTO/mini/Linux+NT-Loader.html.

ACHTUNG

Wenn Sie LILO aus bestimmten Gründen nicht installieren möchten, können Sie das Red Hat Linux System nicht direkt starten. Hierzu ist eine andere Bootmethode (z.B. eine Bootdiskette) erforderlich. Verwenden Sie diese Option nur, wenn Sie wissen, wie Sie Ihr Red Hat Linux System auf andere Weise booten können!

Das Kontrollkästchen `Linearen Modus verwenden` ist standardmäßig aktiviert. In den meisten Fällen sollte der lineare Modus verwendet werden, es sei denn, Ihr Computer kann nicht im linearen Modus auf die Festplatten zugreifen.

Abbildung 15–16 LILO konfigurieren



Falls Sie dem LILO-Bootbefehl weitere Standardoptionen hinzufügen möchten, geben Sie diese in das Feld für die Kernel-Parameter ein. Alle von Ihnen festgelegten Optionen werden bei jedem Booten an den Linux-Kernel übergeben.

Bootfähige Partition - Alle bootfähigen Partitionen werden aufgelistet. Hierzu gehören auch Partitionen, die von anderen Betriebssystemen verwendet werden. Für die Partition, in der sich das Root-Dateisystem Ihres Red Hat Linux Systems befindet, wird in die Spalte "Bootkennung" der Begriff `Linux` eingetragen. Andere Partitionen können ebenfalls Bootkennungen aufweisen. Wenn Sie Bootkennungen für andere Partitionen hinzufügen (oder eine bestehende Bootkennung ändern) möchten, klicken Sie einmal auf die Partition, um sie zu markieren. Anschließend können Sie die Bootkennung ändern.

Bitte beachten

In der Spalte "Bootkennung" wird angezeigt, was Sie am Prompt `boot:` eingeben müssen, um das gewünschte Betriebssystem zu booten. Wenn Sie die Bootkennungen vergessen, die im System definiert wurden, können Sie am Prompt `boot:` von LILO immer noch die [Tabulatortaste] drücken, um eine Liste der definierten Bootkennungen anzuzeigen.

15.16.1 Konfigurieren von LILO

- **Bootdiskette erstellen** - Das Kontrollkästchen **Bootdiskette erstellen** wird standardmäßig aktiviert. Wenn Sie keine Bootdiskette erstellen möchten, sollten Sie dieses Kontrollkästchen deaktivieren. Es wird jedoch dringend empfohlen, eine Bootdiskette zu erstellen. Die Verwendung einer Bootdiskette ist aus mehreren Gründen sinnvoll:
  - Statt LILO - Sie können statt LILO auch eine Bootdiskette verwenden. Dies ist hilfreich, wenn Sie zum ersten Mal mit Red Hat Linux arbeiten. Außerdem brauchen Sie sich keine Sorgen um die Boot-Einstellungen für Ihr anderes Betriebssystem zu machen. Wenn Sie eine Bootdiskette verwenden, können Sie problemlos zu Ihrem anderen Betriebssystem zurückkehren, indem Sie die Bootdiskette aus dem Laufwerk nehmen und das System neu starten. Wenn Sie es vorziehen, statt LILO eine Bootdiskette zu verwenden, müssen Sie sich vergewissern, dass Sie die Option **Keine Installation von LILO** aktiviert haben.
  - Wenn ein anderes Betriebssystem LILO überschreibt - Andere Betriebssysteme sind möglicherweise nicht so flexibel wie Red Hat Linux, was die Unterstützung von Bootmethoden anbelangt. Sehr oft wird durch die Installation oder Aktualisierung eines anderen Betriebssystems der Master Boot Record Ihrer Festplatte überschrieben, in dem sich LILO befindet, so dass Sie die Red Hat Linux Installation nicht mehr booten können. In diesem Fall können Sie Red Hat Linux mit der Bootdiskette starten, um LILO anschließend neu zu installieren.

- **Keine Installation von LILO** - Wenn Windows NT im System installiert ist, möchten Sie LILO möglicherweise nicht installieren. Wenn Sie LILO aus diesem Grund nicht installieren möchten, sollten Sie unbedingt eine Bootdiskette erstellen. Anderenfalls können Sie Linux möglicherweise nicht starten. Sie können auch festlegen, dass die Einrichtung von LILO übersprungen oder dass LILO nicht auf die Festplatte geschrieben werden soll.

Tipp

Für die Verwendung der Bootdiskette im Rettungsmodus haben Sie mehrere Optionen:

- Sie können das CD-ROM-Laufwerk verwenden, um das System zu starten. Geben Sie dann `linux rescue` am Prompt `boot:` ein.
- Sie können die Netzwerk-Bootdiskette verwenden, um das System zu starten. Geben Sie `linux rescue` am Prompt `boot:` ein. Sie werden anschließend aufgefordert, die Rettungsdiskette aus dem Netzwerk zu laden.
- Sie können die Bootdiskette verwenden, die zum Lieferumfang der Red Hat Linux Packung gehört. Geben Sie `linux rescue` am Prompt `boot:` ein. Sie können dann eine Installationsart und einen gültigen Installationsverzeichnisbaum für das Laden der Dateien auswählen.

Weitere Informationen zum Rettungsmodus. Siehe Kapitel 2, *Systemadministration*.

15.16.2 Alternativen zu LILO

Wenn Sie LILO nicht verwenden möchten, um das Red Hat Linux System zu starten, gibt es mehrere Alternativen:

Bootdiskette

Wie bereits weiter oben erwähnt, können Sie hierzu die Bootdiskette verwenden, die vom Installationsprogramm erstellt wurde (sofern Sie die entsprechende Option aktiviert haben).

LOADLIN

Sie können Linux über MS-DOS starten. Allerdings benötigt LOADLIN hierzu eine Kopie des Linux-Kernels (und eine initiale Ramdisk, sofern Sie über einen SCSI-Adapter verfügen) auf einer MS-DOS-Partition. Dazu müssen Sie Ihr Red Hat Linux System zunächst auf andere Weise booten (z.B. mit einer Diskette, auf der sich LILO befindet) und anschließend den Kernel in eine MS-DOS-Partition kopieren. `LOADLIN` finden Sie unter ftp://metalab.unc.edu/pub/Linux/system/boot/dualboot/ sowie auf den zugehörigen Mirror Sites.

SYSLINUX

Syslinux ist ein MS-DOS-Programm, das `LOADLIN` sehr ähnlich ist. Es ist ebenfalls unter ftp://metalab.unc.edu/pub/Linux/system/boot/loaders/ sowie auf den zugehörigen Mirror Sites erhältlich.

Einige kommerzielle Bootloader

Auch Programme wie z.B. System Commander und Partition Magic können Linux starten. Dennoch muss hierzu LILO in Ihrer Linux-Root-Partition installiert sein.

15.16.3 SMP-Mainboards und LILO

Dieser Abschnitt gilt ausschließlich für Computer mit einem SMP-Motherboard. Wenn der Installer ein SMP-Motherboard (also eine Hauptplatine mit mehreren Prozessoren) in Ihrem System erkennt, werden automatisch zwei Einträge in **lilo.conf** angelegt (während normalerweise nur ein Eintrag erstellt wird).

Ein Eintrag trägt die Bezeichnung **linux** und der andere **linux-up**. Mit *linux* wird das System standardmäßig gestartet. Falls Sie jedoch Schwierigkeiten mit dem SMP-Kernel haben, können Sie stattdessen den Eintrag *linux-up* zum Booten auswählen.

Dabei bleiben sämtliche Funktionen erhalten, nur arbeiten Sie jetzt mit einem einzelnen Prozessor.

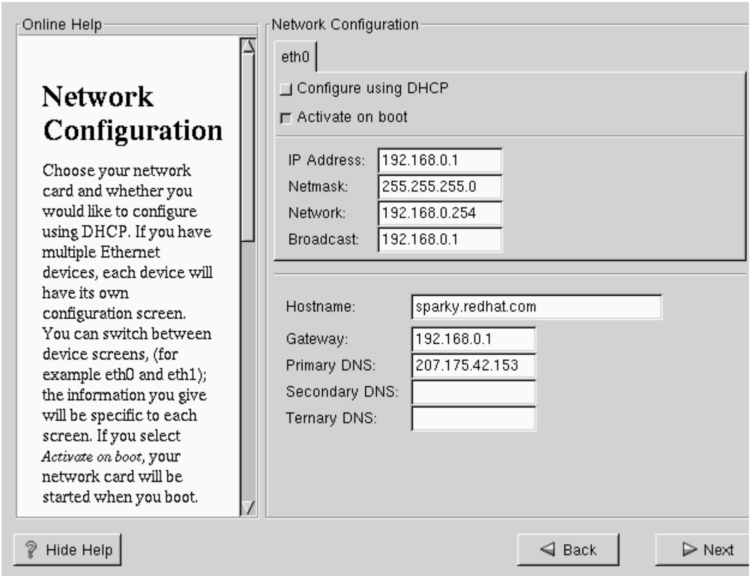
15.17 Konfigurieren des Netzwerks

Wenn Sie über eine Netzwerkkarte verfügen und die Netzwerkeinstellungen noch nicht konfiguriert haben, können Sie dies jetzt vornehmen (siehe Abbildung 15–17, *Konfigurieren des Netzwerks*).

Wählen Sie den geeigneten Gerätetyp aus, und legen Sie fest, ob Sie die Konfiguration mit Hilfe von DHCP durchführen möchten. Wenn Sie über mehrere Ethernet-Geräte verfügen, werden in allen Gerätebildschirmen die von Ihnen eingegebenen Daten gespeichert. Sie können auch zwischen den verschiedenen Gerätebildschirmen (wie beispielsweise eth0 und eth1) umschalten. Die von Ihnen eingegebenen Daten beziehen sich immer nur auf den jeweils ausgewählten Bildschirm für ein bestimmtes Gerät. Wenn Sie die Option **Beim Starten aktivieren** auswählen, wird Ihre Netzwerkschnittstelle beim Booten gestartet. Wenn Sie über keinen Client-Zugriff auf DHCP verfügen oder Fragen zu DHCP haben, wenden Sie sich bitte an Ihren Netzwerkadministrator.

Geben Sie dann, falls erforderlich, die **IP-Adresse** und die Adressen für **Netzmaske**, **Netzwerk** und **Broadcast** ein. Wenn Sie sich nicht sicher sind, welche Werte Sie eingeben sollen, sollten Sie sich auch in diesem Fall an Ihren Netzwerkadministrator wenden.

Abbildung 15–17 Konfigurieren des Netzwerks



Tipp

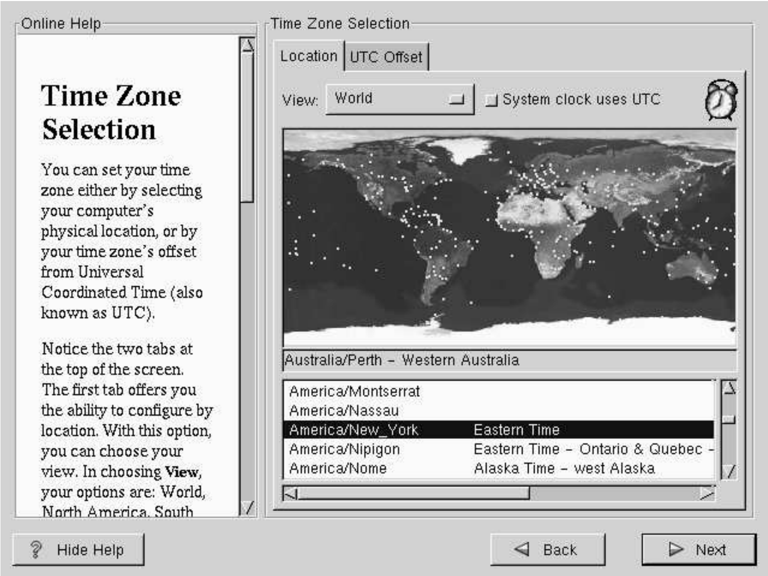
Auch wenn Ihr Computer nicht in ein Netzwerk eingebunden ist, können Sie einen Namen für Ihr System eingeben. Wenn Sie zum jetzigen Zeitpunkt keinen Namen eingeben, wird Ihrem System die Bezeichnung `localhost` zugewiesen.

Geben Sie schließlich noch die Informationen für das **Gateway** sowie die **erste DNS-Adresse** (und ggf. auch die **zweite** und **dritte DNS-Adresse**) an.

15.18 Konfigurieren von Zeitzonen

Sie können die Zeitzone entweder durch Angabe des physischen Standorts Ihres Computers oder Festlegen der Abweichung Ihrer Zeitzone von der UTC (Universal Coordinated Time = koordinierte Weltzeit) einstellen.

Abbildung 15–18 Konfigurieren der Zeitzone



Beachten Sie in diesem Zusammenhang bitte die beiden Registerkarten am oberen Bildschirmrand (siehe Abbildung 15–18, *Konfigurieren der Zeitzone*). Im ersten Register können Sie die Zeitzone durch Auswählen eines bestimmten geografischen Orts konfigurieren. Sie können selbst entscheiden, mit welcher Methode die Auswahl erfolgen soll. Wählen Sie unter **Anzeige** eine der folgenden Optionen aus: **Welt**, **Nordamerika**, **Südamerika**, **Pazifischer Raum**, **Europa**, **Afrika** und **Asien**.

Auf der interaktiven Karte können Sie auch auf eine der durch gelbe Punkte dargestellten Städte klicken. Die von Ihnen ausgewählte Stadt wird dann durch ein rotes **X** gekennzeichnet. Sie haben auch die Möglichkeit, in der Liste zu scrollen und die gewünschte Zeitzone auszuwählen.

Im zweiten Register können Sie die Abweichung Ihrer Zeitzone von der koordinierten Weltzeit UTC angeben. Hier können Sie in einer Liste mit verschiedenen Einstellungen die gewünschte Abweichung auswählen und darüber hinaus mit einem Kontrollkästchen festlegen, ob die Sommerzeit berücksichtigt werden soll.

Für beide Register steht das Kontrollkästchen **Systemuhr verwendet UTC** zur Verfügung. Aktivieren Sie dieses Kontrollkästchen, wenn Sie wissen, dass Ihr System die koordinierte Weltzeit verwendet.

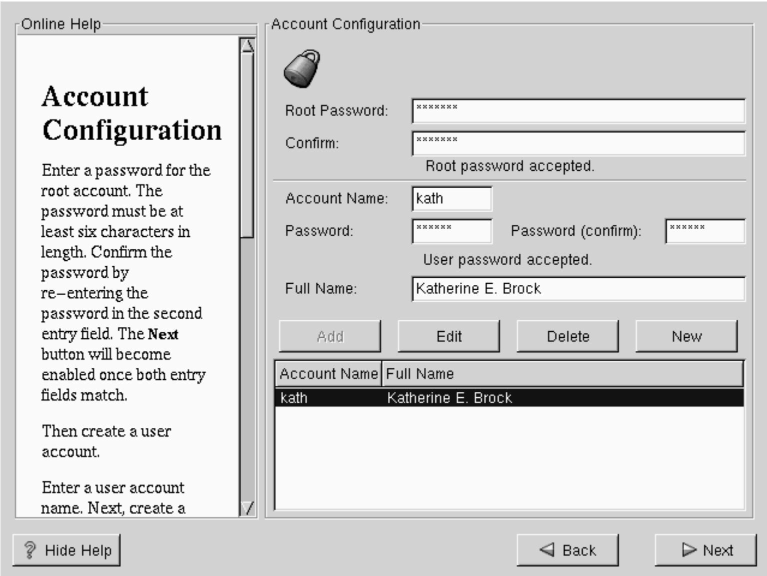
Tipp

Wenn Sie nach dem Booten des Red Hat Linux Systems Ihre Zeitzonenkonfiguration ändern möchten, müssen Sie sich hierzu als Root anmelden und den Befehl `/usr/sbin/timeconfig` verwenden.

15.19 Konfigurieren des Accounts

Im Dialogfeld **Account konfigurieren** können Sie das Root-Passwort festlegen. Außerdem können Sie Benutzeraccounts einrichten, unter denen Sie sich anmelden können, wenn die Installation abgeschlossen ist (siehe Abbildung 15–19, *Erstellen eines Benutzeraccounts*).

Abbildung 15–19 Erstellen eines Benutzeraccounts



15.19.1 Setzen des Root-Passworts

Das Installationsprogramm fordert Sie auf, ein **Root-Passwort** für das System einzugeben.

Das Root-Passwort muss aus mindestens sechs Zeichen bestehen. Es wird bei der Eingabe nicht auf dem Bildschirm angezeigt. Sie müssen das Passwort zweimal eingeben. Falls die beiden Eingaben nicht übereinstimmen, werden Sie vom Installationsprogramm aufgefordert, den Vorgang zu wiederholen.

Wählen Sie ein Passwort, das Sie sich gut merken können, das aber für andere Personen nicht leicht zu erraten ist. Ihr Name, Ihre Telefonnummer, **qwertz**, **Passwort**, **Root**, **123456**, und **Schnucki** sind Beispiele für schlechte Passwörter. Geeignete Passwörter bestehen aus einer Kombination von Zahlen und Groß-/Kleinbuchstaben und ergeben keine sinnvollen Wörter: z.B. **Aard387vark** oder **420BMttNT**. Beachten Sie, dass bei Passwörtern zwischen Groß- und Kleinschreibung unterschieden wird. Notieren Sie sich das Passwort, und bewahren Sie es an einem sicheren Ort auf.

Bitte beachten

Der **Root**-Benutzer (auch **Superuser** genannt) hat vollständigen Zugriff auf das gesamte System. Deshalb sollten Sie sich *nur dann* als Root anmelden, wenn Sie Aufgaben zur Systemwartung oder Systemadministration ausführen möchten.

15.19.2 Einrichten von Benutzeraccounts

Wenn Sie jetzt einen Benutzeraccount erstellen, verfügen Sie über einen Account, unter dem Sie sich nach Abschluss der Installation anmelden können. Damit können Sie sich sicher und einfach am Computer anmelden, ohne für das Erstellen weiterer Konten auf **Root** zurückgreifen zu müssen.

Geben Sie einen Namen für den Benutzeraccount ein. Legen Sie dann ein Passwort für diesen Benutzeraccount fest, und bestätigen Sie dieses. Geben Sie schließlich noch den vollständigen Namen für den Benutzer des Kontos ein, und drücken Sie die [Eingabetaste]. Die von Ihnen für den Account eingegebenen Daten werden in die Liste mit den Benutzeraccounts eingefügt. Die Felder für den Benutzeraccount werden anschließend gelöscht, so dass Sie einen weiteren Benutzer hinzufügen können.

Sie können auch auf **Neu** klicken, um einen neuen Benutzer hinzuzufügen. Geben Sie die Benutzerdaten ein, und klicken Sie auf den Button **Hinzufügen**, um den Benutzer in die Liste mit den Benutzeraccounts einzufügen.

Sie können die bereits erstellten Benutzeraccounts mit Hilfe der Buttons **Bearbeiten** oder **Löschen** ändern bzw. entfernen (falls Sie diese nicht mehr benötigen).

15.20 Authentifizierung konfigurieren

Wenn Sie eine Workstation-Installation durchführen, lesen Sie bitte gleich in Abschnitt 15.22, *X-Konfigurationstool mit grafischer Benutzeroberfläche* weiter.

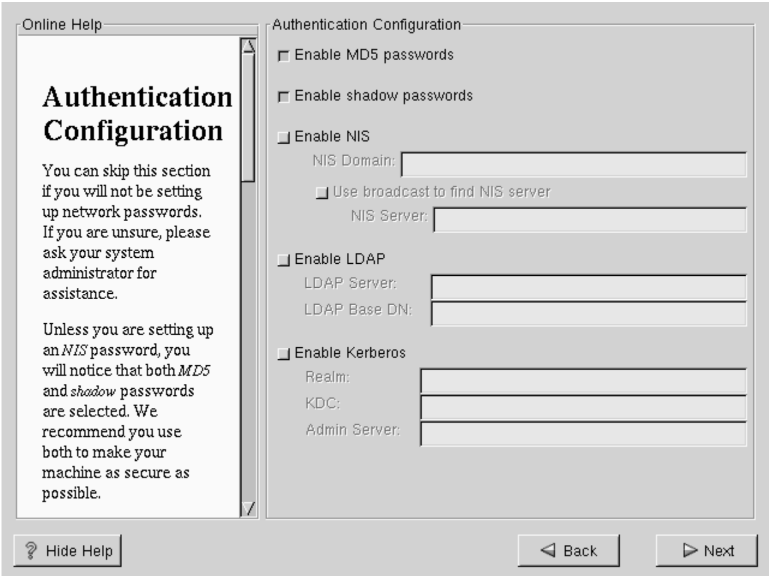
Wenn Sie eine Server-Installation durchführen, lesen Sie bitte gleich in Abschnitt 15.23, *Installation wird vorbereitet* weiter.

Sie können diesen Abschnitt überspringen, wenn Sie keine Passwörter für das Netzwerk festlegen möchten. Wenn Sie sich nicht sicher sind, welche Einstellungen Sie verwenden sollen, wenden Sie sich bitte an Ihren Systemadministrator.

Wenn Sie keine **NIS**-Authentifizierung einrichten, sind die beiden Kontrollkästchen für **MD5-** und **Shadow-**Passwörter aktiviert (siehe Abbildung 15–20, *Authentifizierung konfigurieren*). Es empfiehlt sich, beide Optionen zu verwenden, um Ihren Computer so sicher wie möglich zu machen.

Um die NIS-Option zu konfigurieren, muss Ihr Computer an ein NIS-Netzwerk angeschlossen sein. Wenn Sie sich nicht sicher sind, ob Sie mit einem NIS-Netzwerk verbunden sind, wenden Sie sich bitte an Ihren Systemadministrator.

Abbildung 15–20 Authentifizierung konfigurieren



- **MD5-Passwort** - Mit dieser Einstellung können Sie lange Passwörter (mit bis zu 256 Zeichen) statt der standardmäßigen Passwörter mit maximal acht Zeichen verwenden.
- **Shadow-Passwort** - Diese Option stellt Ihnen eine äußerst sichere Methode für das Speichern von Passwörtern zur Verfügung. Die Passwörter werden im Verzeichnis `/etc/shadow` gespeichert, auf das Sie nur als Root zugreifen können.
- **NIS aktivieren** - Eine Gruppe von Rechnern kann mit einer gemeinsamen Passwort- und Gruppendatei in derselben Network Information Service-Domäne betrieben werden. Ihnen stehen zwei Optionen zur Auswahl:
  - **NIS-Domäne** - Mit dieser Option können Sie angeben, zu welcher Domäne oder Gruppe von Computern Ihr System gehören soll.
  - **NIS Server** - Mit dieser Option kann Ihr Computer einen bestimmten NIS-Server verwenden, statt eine Broadcast-Anforderung an das lokale Netzwerk auszugeben, um nach verfügbaren Servern für das System zu fragen.
- **LDAP aktivieren** - LDAP fasst bestimmte Informationsarten innerhalb Ihrer Organisation zusammen. So können zum Beispiel alle Benutzerlisten in Ihrer Organisation in einem LDAP-Verzeichnis untergebracht werden. Weitere Informationen zu LDAP finden Sie im Kapitel 7, *Lightweight Directory Access Protocol (LDAP)*. Ihnen stehen zwei Optionen zur Auswahl:
  - **LDAP Server** - Mit dieser Option können Sie auf einen Server zugreifen, der das LDAP-Protokoll ausführt.
  - **LDAP Basis-DN** - Mit dieser Option können Sie anhand des eindeutigen Namens (*Distinguished Name*, DN) nach Benutzerinformationen suchen.
- **Kerberos aktivieren** - Bei Kerberos handelt es sich um ein sicheres System, das Authentifizierungsdienste für Netzwerke zur Verfügung stellt. Weitere Informationen zu Kerberos finden Sie in Kapitel 8, *Verwenden von Kerberos 5 in Red Hat Linux*. Ihnen stehen drei Optionen zur Auswahl:
  - **Realm** - Mit dieser Option können Sie auf ein Netzwerk zugreifen, das Kerberos verwendet und aus einem oder einigen Servern (auch als KDCs bezeichnet) sowie einer (potentiell sehr großen) Zahl von Clients besteht.

– **KDC** - Mit dieser Option können Sie auf das Key Distribution Center (KDC) zugreifen. Hierbei handelt es sich um ein Gerät, das Kerberos-Tickets ausgibt (manchmal auch als Ticket Granting Server oder TGS bezeichnet).
– **Admin-Server** - Mit dieser Option können Sie auf einen Server zugreifen, der kadmind ausführt.

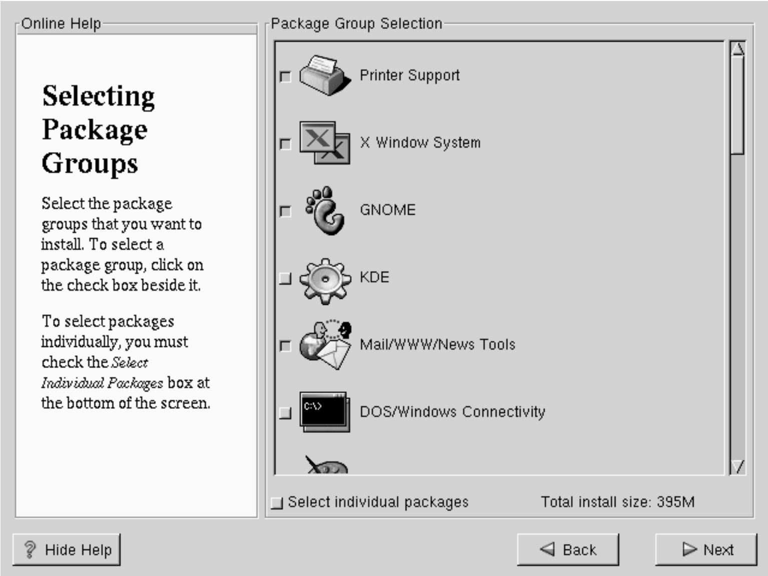
15.21 Auswählen von Paketgruppen

Nachdem Ihre Partitionen zum Formatieren ausgewählt und konfiguriert wurden, können Sie die Pakete auswählen, die Sie installieren möchten.

Sie haben die Wahl zwischen **Komponenten**, in denen Pakete nach ihrer Funktion zusammengestellt sind (z.B. `C-Programmierung`, `Workstation mit Netzwerkanbindung` oder `Webserver`), **Einzelpaketen** oder einer Kombination aus beidem.

Um eine Komponente auszuwählen, klicken Sie auf das Kontrollkästchen neben der Komponente (siehe Abbildung 15–21, *Auswählen von Paketgruppen*).

Abbildung 15–21 Auswählen von Paketgruppen



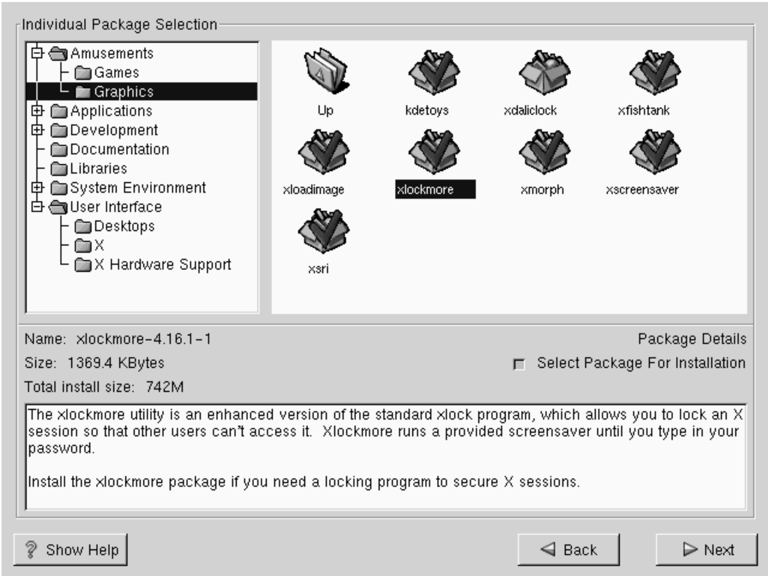
Wählen Sie alle Komponenten aus, die Sie installieren möchten. Wenn Sie die Option `Alles` wählen (die Sie am Ende der Komponentenliste finden), werden alle Pakete installiert, die zum Lieferumfang von Red Hat Linux gehören. Sie benötigen dann etwa 1,7 GB freien Festplattenspeicher.

Wenn Sie einzelne Pakete auswählen möchten, aktivieren Sie das Kontrollkästchen **Einzelne Pakete auswählen** am unteren Rand des Bildschirms.

15.21.1 Auswählen von Einzelpaketen

Nachdem Sie die Komponenten ausgewählt haben, die installiert werden sollen, können Sie einzelne Pakete aktivieren oder deaktivieren. Das Installationsprogramm zeigt eine Liste der Pakete in der Gruppe an, die Sie mit Hilfe der Maus aktivieren oder deaktivieren können (siehe Abbildung 15–22, *Auswählen von Einzelpaketen*).

Abbildung 15–22 Auswählen von Einzelpaketen



Auf der linken Bildschirmseite wird eine Verzeichnisliste der verschiedenen Paketgruppen angezeigt. Wenn Sie die Liste erweitern (doppelklicken Sie auf die Liste, um sie zu markieren) und auf ein einzelnes Verzeichnis doppelklicken, wird die Liste der zur Installation verfügbaren Pakete auf der rechten Seite angezeigt.

Um ein einzelnes Paket auszuwählen, doppelklicken Sie auf dessen Symbol. Alternativ können Sie das Paket auch durch Klicken markieren und anschließend das Kontrollkästchen **Paket für die Installation auswählen** aktivieren. Alle Pakete, die Sie für die Installation ausgewählt haben, werden jeweils durch ein rotes Häkchen gekennzeichnet.

Um vor der Installation Informationen über ein bestimmtes Paket zu erhalten, klicken Sie einmal mit der linken Maustaste auf dieses Paket, um es zu markieren. Die Informationen werden dann am unteren Bildschirmrand zusammen mit dem Namen und der Größe des Pakets angezeigt.

Bitte beachten

Einige Pakete (z.B. der Kernel und bestimmte Bibliotheken) werden für alle Red Hat Linux Systeme benötigt und können nicht abgewählt werden. Diese **Basispakete** werden standardmäßig für die Installation ausgewählt.

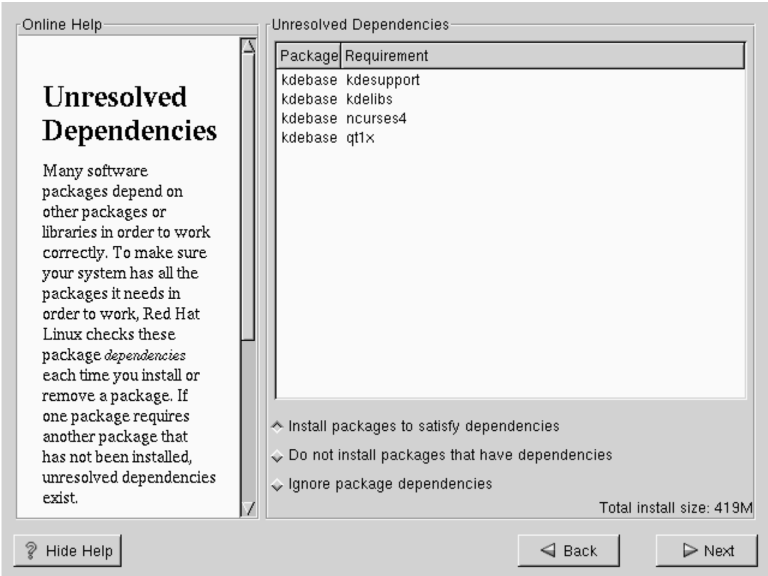
15.21.2 Ungelöste Abhängigkeiten

Viele der Software-Pakete können nur in Verbindung mit anderen Software-Paketen, die im System installiert sein müssen, korrekt ausgeführt werden. So benötigen beispielsweise viele der grafischen Tools zur Systemadministration für das Red Hat System die Pakete python und pythonlib. Um sicherzugehen, dass alle Pakete zur Verfügung stehen, die Ihr System benötigt, überprüft Red Hat Linux diese **Paketabhängigkeiten** bei jeder Installation oder Deinstallation von Software-Paketen.

Falls Pakete fehlen, die andere Pakete zur korrekten Ausführung benötigen, zeigt das Programm eine Liste dieser **ungelösten Abhängigkeiten** an und gibt Ihnen die Möglichkeit, sie zu lösen (siehe Abbildung 15–23, *Ungelöste Abhängigkeiten*).

Der Bildschirm **Ungelöste Abhängigkeiten** wird nur angezeigt, wenn bestimmte Pakete fehlen, die für die von Ihnen ausgewählten Pakete benötigt werden. Unterhalb der Liste der fehlenden Pakete befindet sich das Kontrollkästchen **Pakete installieren, um Abhängigkeiten zu erfüllen** am unteren Rand des Bildschirms. Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn Sie dieses Kontrollkästchen aktiviert lassen, löst das Installationsprogramm automatisch alle Paketabhängigkeiten, indem es alle benötigten Pakete in die Liste der ausgewählten Pakete einfügt.

Abbildung 15–23 Ungelöste Abhängigkeiten



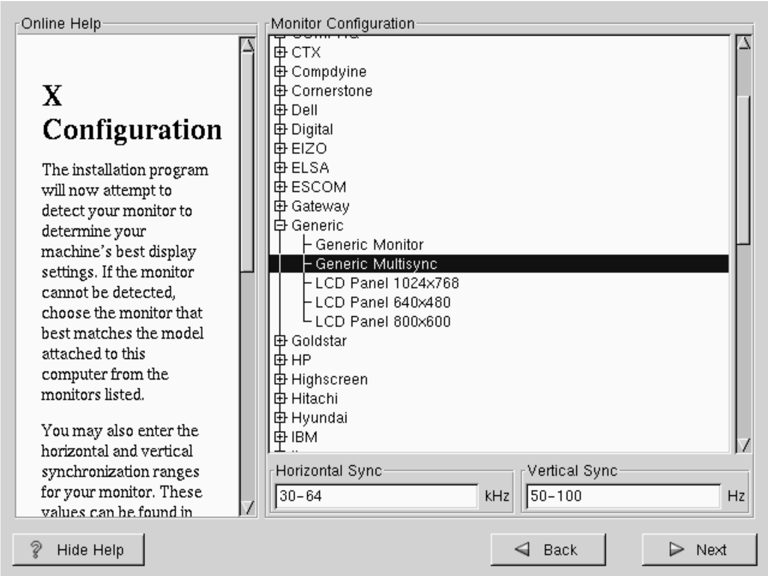
15.22 X-Konfigurationstool mit grafischer Benutzeroberfläche

Wenn Sie die Pakete für das X Window System installieren möchten, haben Sie jetzt die Gelegenheit, einen X-Server für das System zu konfigurieren. Wenn Sie diese Pakete nicht installieren wollen, fahren Sie mit Abschnitt 15.24, *Installieren der Pakete* fort.

15.22.1 Konfigurieren des Bildschirms

Xconfigurator, das Konfigurationstool für das X Window System, zeigt Ihnen zunächst eine Liste mit Bildschirmen zur Auswahl an. Sie können entweder den automatisch erkannten Bildschirm verwenden oder stattdessen selbst einen geeigneten anderen Bildschirm auswählen.

Abbildung 15–24 Auswählen des Bildschirms



Wenn Ihr Bildschirm nicht in der Liste aufgeführt wird, wählen Sie den am besten geeigneten **generischen** Bildschirm aus. Bei der Auswahl eines **generischen** Bildschirms schlägt Xconfigurator bestimmte Frequenzbereiche für die horizontale und vertikale Bildwiederholrate vor. Diese Werte werden normalerweise in der Dokumentation aufgeführt, die Ihrem Bildschirm beilag, oder sind beim Hersteller Ihres Monitors erhältlich. Um sicherzustellen, dass die korrekten Werte verwendet werden, sollten Sie in der Dokumentation zu Ihrem Bildschirm nachschlagen.

ACHTUNG

Wählen Sie keinen Bildschirm aus, der Ihrem tatsächlich verwendeten Modell *ähnlich* ist, wenn Sie nicht absolut sicher sind, dass Ihr Monitor mindestens die gleichen Wiederholraten wie der ausgewählte Monitor unterstützt. Wenn Ihr Bildschirm diese hohen Frequenzen nicht unterstützt, kann dies zu schweren Schäden an der Bildröhre führen.

In diesem Bildschirm werden auch die horizontalen und vertikalen Bildwiederholraten angezeigt, die Xconfigurator vorschlägt.

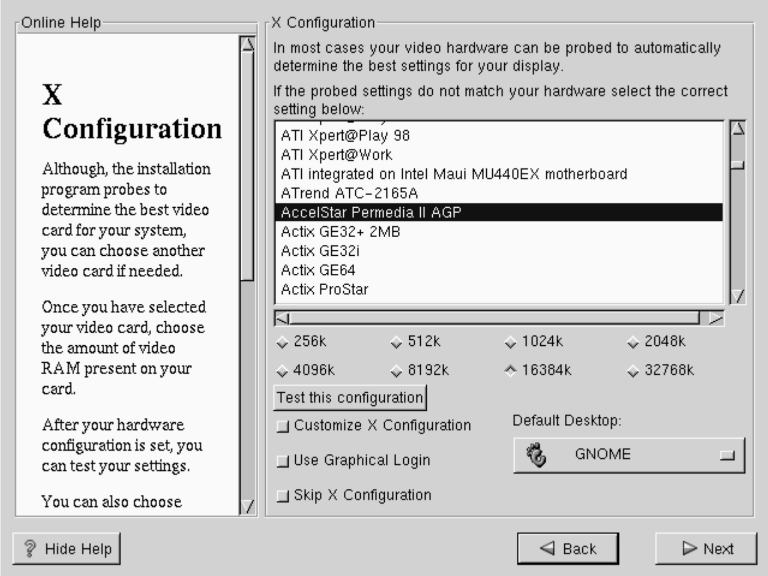
Klicken Sie auf **Weiter**, wenn Sie die Konfiguration Ihres Bildschirms abgeschlossen haben.

15.22.2 Konfigurieren der Grafik-Hardware

Als Nächstes versucht Xconfigurator, die in Ihrem System vorhandene Grafik-Hardware zu erkennen (siehe Abbildung 15–25, *Einrichten der Grafikkarte*). Wenn die Grafikkarte nicht erkannt wurde, zeigt Xconfigurator eine Liste mit Grafikkarten und Monitoren an, in der Sie eine Auswahl treffen können.

Wenn Ihre Grafikkarte nicht in der Liste enthalten ist, wird sie von **XFree86** möglicherweise nicht unterstützt. Falls Sie über technische Informationen zu Ihrer Karte verfügen, können Sie jedoch in diesem Fall die Option **Nicht aufgelistete Karte** auswählen und dann versuchen, einen für Ihren Chipsatz geeigneten X Server manuell aus der Liste mit den verfügbaren X Servern auszuwählen.

Abbildung 15–25 Einrichten der Grafikkarte



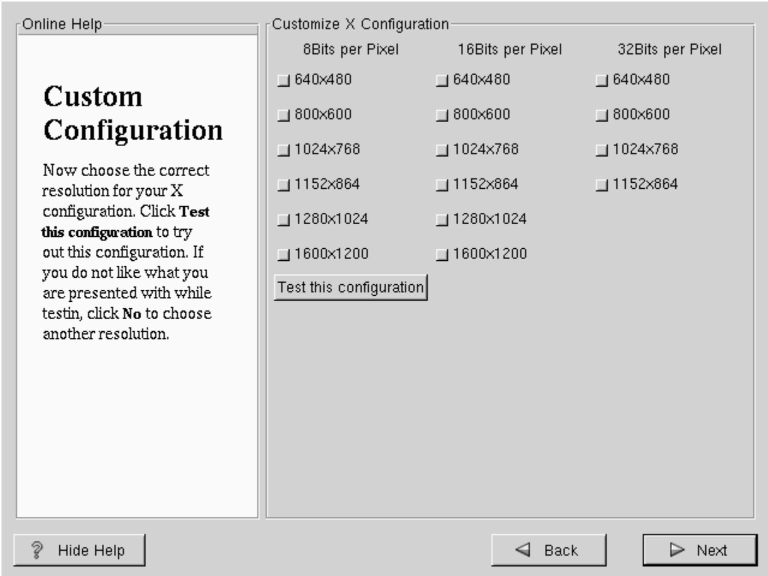
Als Nächstes fragt Xconfigurator nach der Größe des auf der Grafikkarte installierten Grafikspeichers. Falls Sie sich nicht sicher sind, ziehen Sie die Dokumentation zu Ihrer Grafikkarte heran. Sie beschädigen die Grafikkarte nicht, wenn Sie eine höhere Speichergröße als vorhanden auswählen, aber der XFree86-Server wird in diesem Fall möglicherweise nicht richtig gestartet.

Sobald die Hardware ermittelt wurde, können Sie die Konfigurationseinstellungen testen. Es empfiehlt sich, die Konfiguration zu testen, um sich zu vergewissern, dass Auflösung und Farbtiefe Ihren Wünschen entsprechen.

Wenn Sie die X-Konfiguration individuell anpassen möchten, müssen Sie das Kontrollkästchen **X-Konfiguration individuell festlegen** aktivieren. In diesem Fall wird ein weiterer Bildschirm angezeigt, in dem Sie die gewünschte Auflösung auswählen können (siehe Abbildung 15–26, *Konfigurieren von X*). Auch jetzt erhalten Sie die Möglichkeit, die Konfiguration zu testen.

Vergewissern Sie sich, dass Sie entweder GNOME oder KDE als Standard-Desktop auswählen, je nachdem, welche Benutzeroberfläche Sie installiert haben.

Abbildung 15–26 Konfigurieren von X



Wenn Sie X erst nach der Installation oder gar nicht konfigurieren möchten, können Sie das Kontrollkästchen **X-Konfiguration überspringen** aktivieren.

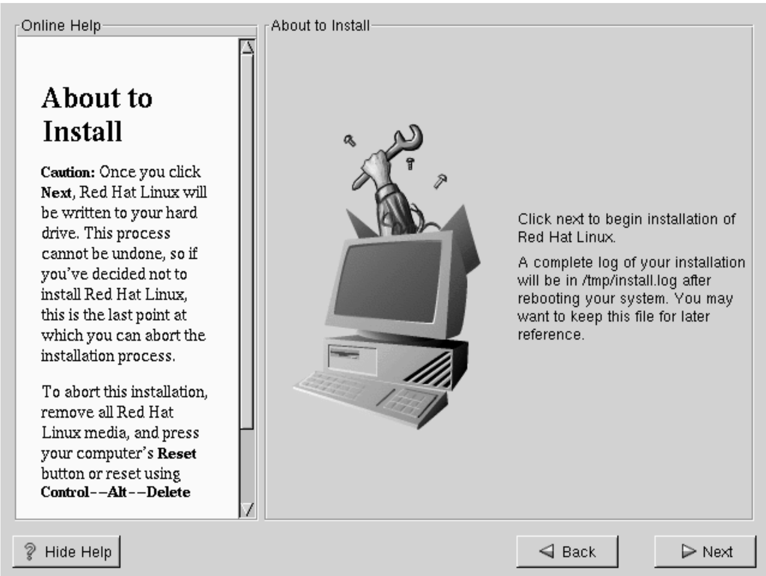
15.23 Installation wird vorbereitet

Nun wird ein Bildschirm angezeigt, der Sie darauf hinweist, dass Red Hat Linux jetzt installiert wird (siehe Abbildung 15–27, *Die Installation kann jetzt erfolgen*).

WARNUNG

Wenn Sie den Installationsvorgang nicht fortsetzen möchten, ist jetzt der letzte Zeitpunkt, zu dem Sie die Installation problemlos abbrechen und Ihren Rechner neu starten können. Sobald Sie auf den Button Weiter geklickt haben, werden die Partitionen auf die Festplatte(n) geschrieben und die Pakete installiert. Wenn Sie die Installation abbrechen möchten, sollten Sie jetzt einen Neustart durchführen, bevor die neuen Daten auf die Festplatte(n) geschrieben werden.

Abbildung 15–27 Die Installation kann jetzt erfolgen



15.24 Installieren der Pakete

Jetzt brauchen Sie nur noch so lange zu warten, bis alle Pakete installiert worden sind (siehe Abbildung 15–28, *Installieren der Pakete*). Wie lange das dauert, hängt von der Zahl der ausgewählten Pakete und der Leistung Ihres Computers ab.

Abbildung 15–28 Installieren der Pakete

15.25 Erstellen einer Bootdiskette

Wenn Sie eine Bootdiskette erstellen möchten, sollten Sie jetzt eine leere, formatierte Diskette in Ihr Diskettenlaufwerk einlegen (siehe Abbildung 15–29, *Erstellen einer Bootdiskette*).

Nach kurzer Wartezeit wird die Bootdiskette erstellt. Nehmen Sie die Diskette aus dem Diskettenlaufwerk heraus, und beschriften Sie sie eindeutig. Beachten Sie, dass Sie auch im Anschluss an die Installation eine Bootdiskette erstellen können, sofern

Sie es wünschen. Weitere Informationen finden Sie auf der man-Seite zu `mkbootdisk`. Rufen Sie diese Seite auf, indem Sie am Shell Prompt `man mkbootdisk` eingeben.

Wenn Sie das System mit der Bootdiskette (anstelle von LILO) starten, müssen Sie daran denken, eine neue Bootdiskette zu erstellen, wenn Sie Änderungen am Kernel vornehmen.

Abbildung 15–29 Erstellen einer Bootdiskette

15.26 Installation abgeschlossen

Herzlichen Glückwunsch! Die Installation von Red Hat Linux 7.0 ist jetzt abgeschlossen!

Das Installationsprogramm fordert Sie auf, das System für den Neustart vorzubereiten (siehe Abbildung 15–30, *Installation abgeschlossen*). Nehmen Sie alle Disketten und CD-ROMs aus den jeweiligen Laufwerken. Wenn Sie LILO nicht installiert haben, benötigen Sie jetzt die Bootdiskette.

Nachdem Sie Ihren Computer neu gestartet haben, sehen Sie den GUI-Prompt von LILO. Sie können nun eine der folgenden Aktionen durchführen:

- Drücken der [Eingabetaste] - Es wird ein Systemstart mit dem Standardbooteintrag von LILO durchgeführt.
- Wählen Sie eine Bootkennung aus, und drücken Sie dann die [Eingabetaste] -- LILO wird nun das Betriebssystem booten, das der Bootkennung entspricht. (Durch Drücken der Taste [?] an der LILO Texteingabe `boot:` können Sie eine Liste mit gültigen Bootkennungen anzeigen.)
- Abwarten - Nach Ablauf der Zeitüberschreitung von LILO (standardmäßig fünf Sekunden) führt LILO automatisch den Systemstart mit dem Standardbooteintrag durch.

Abbildung 15–30 Installation abgeschlossen

Führen Sie die erforderlichen Schritte aus, um Red Hat Linux zu booten. Zunächst scrollen zahlreiche Meldungen über Ihren Bildschirm. Schließlich sollte der Prompt `login:` oder ein GUI-Anmeldebildschirm angezeigt werden (sofern Sie das X Window System installiert haben und X automatisch gestartet wird).

Teil IV Anhänge

A Allgemeine Parameter und Module

Dieser Anhang soll *einige* der möglichen Parameter erklären, die von bestimmten Treibern benötigt werden. Wir weisen darauf hin, dass diese zusätzlichen Parameter in den meisten Fällen nicht notwendig sind. Darüber hinaus finden Sie in diesem Anhang eine Liste mit Netzwerk-Hardware und den von dieser Hardware benötigten Modulen.

Wenn ein Gerät, das Sie verwenden möchten, einen dieser Parameter benötigt und für dieses Gerät *keine* Unterstützung in den Kernel einkompiliert ist, kann der Parameter nicht auf die herkömmliche Weise zum LILO-Bootbefehl hinzugefügt werden. Treiber, die als Module geladen werden, benötigen die Angabe dieser Parameter beim Laden des Moduls. Das Red Hat Linux Installationsprogramm bietet Ihnen die Möglichkeit, beim Laden eines Treibers Modulparameter anzugeben.

A.1 Ein Hinweis zu Kernel-Treibern

Während der Installation von Red Hat Linux gibt es einige Einschränkungen für Dateisysteme und andere Treiber, die vom Kernel unterstützt werden. Nach der Installation werden alle unter Linux verfügbaren Dateisysteme unterstützt. Während der Installation unterstützt der modulare Kernel (E)IDE-Geräte (einschließlich ATAPI CD-ROM-Laufwerken), SCSI-Adapter und Netzwerkkarten. Des Weiteren werden alle Maustypen, SLIP, CSLIP, PPP, PLIP, FPU-Emulation, Konsolenauswahl, ELF, SysV IPC, IP-Weiterleitung, Firewalling und Benutzeraccountverwaltung, Reverse ARP, QIC-Bänder und Paralleldrucker unterstützt.

Da Red Hat Linux die Installation auf vielen verschiedenen Hardware-Typen unterstützt, sind viele Treiber (einschließlich der Treiber für SCSI -Karten, Netzwerkkarten und viele CD-ROM-Laufwerke) nicht in den Linux-Kernel integriert, der während der Installation verwendet wird. Sie sind jedoch als **Module** verfügbar und werden geladen, wenn sie während der Installation benötigt werden. Falls erforderlich, können Sie während des Ladevorgangs Optionen für diese Module festlegen. Diese Treiber ignorieren alle Optionen, die für sie am `boot:`-Prompt einstellen.

Nach Abschluss der Installation möchten Sie möglicherweise einen neuen Kernel erstellen, der Ihre Hardware-Konfiguration unterstützt. Informationen zum Erstellen eines benutzerdefinierten Kernels finden Sie in Abschnitt 2.8, *Erstellen eines benutzerdefinierten Kernels*. In den meisten Fällen ist ein solcher Kernel jedoch nicht notwendig.

A.2 CD-ROM-Modulparameter

Bitte beachten

Nicht alle aufgeführten Karten werden unterstützt. Prüfen Sie bitte die Hardware-Kompatibilitätsliste auf der Red Hat Website (http://www.redhat.com/support/docs/hardware.html), um sich zu vergewissern, dass Ihre Karte unterstützt wird.

Der relativ häufig verwendete Parameter `hdX=cdrom` *kann* am Boot-Prompt eingegeben werden, da er sich auf die in den Kernel integrierte Unterstützung von IDE/ATAPI-CD-ROMs bezieht.

Die meisten der in den folgenden Tabellen ohne Parameter aufgeführten Module können entweder automatisch die Hardware erkennen, oder Sie müssen die Einstellungen im Modulquellcode von Hand ändern und neu kompilieren.

Tabelle A–1 Hardware-Parameter

Hardware	Modul	Parameter
ATAPI/IDE CD-ROM-Laufwerke		hdX=cdrom
Aztech CD268-01A, Orchid CD-3110, Okano/Wearnes CDD110, Conrad TXC, CyCDROM CR520, CyCDROM CR540 (nicht-IDE)	`aztcd.o`	aztcd=io_port
Sony CDU 31A oder 33A CD-ROM	`cdu31a.o`	cdu31a=io_port,IRQ[,PAS] cdu31a_port=base_addr cdu31a_irq=irq
Philips/LMS CD-ROM-Laufwerk 206 mit cm260 Host Adapter-Karte	`cm206.o`	cm206=io_port,IRQ
Goldstar R420 CD-ROM	`gscd.o`	gscd=io_port
ISP16, MAD16 oder Mozart Soundkarte CD-ROM-Schnittstelle (OPTi 82C928 und OPTi 82C929) mit Sanyo/Panasonic-, Sony- oder Mitsumi-Laufwerken	`isp16.o`	isp16=io_port, IRQ, dma,drive_type isp16_cdrom_base=io_port isp16_cdrom_irq=IRQ isp16_cdrom_dma=dma isp16_cdrom_type=drive_type
Mitsumi CD-ROM, Standard	`mcd.o`	mcd=io_port,IRQ
Mitsumi CD-ROM, Experimentalversion	`mcdx.o`	mcdx=io_port_1, IRQ_1, io_port_n, IRQ_n

Hardware	Modul	Parameter
Optics storage 8000 AT-CD-ROM "Dolphin"-Laufwerk; Lasermate CR328A	`optcd.o`	optcd=io_port
SB Pro 16-kompatibel	`sbpcd.o`	sbpcd=io_port,sb_pro_Setting
Sanyo CDR-H94A	`sjcd.o`	sjcd=io_port sjcd_base=io_port
Sony CDU-535 und 531 (einige Procomm-Laufwerke)	`sonycd535.o`	sonycd535=io_port

Es folgen einige Beispiele, wie diese Module verwendet werden:

Tabelle A–2 Konfigurationsbeispiele für Hardwareparameter

Konfiguration	Beispiele
ATAPI CD-ROM, Jumpereinstellung als Master am 2. IDE-Kanal	hdc=cdrom
Mitsumi nicht-IDE-CD-ROM an Port 340, IRQ 11	mcd=0x340,11
Drei Mitsumi nicht-IDE-CD-ROM-Laufwerke mit experimentellem Treiber, E/A-Ports 300, 304 und 320 mit IRQs 5, 10 und 11	mcdx=0x300,5,0x304,10,0x320,11
Sony CDU 31 oder 33 an Port 340, kein IRQ	cdu31=0x340,0 cdu31_port=0x340 cdu31a_irq=0
Aztech CD-ROM an Port 220	aztcd=0x220
Panasonic CD-ROM an einer SoundBlaster-Schnittstelle an Port 230	sbpcd=0x230,1
Phillips/LMS cm206 und cm260 an E/A 340 und IRQ 11	cm206=0x340,11
Goldstar R420 an E/A 300	gscd=0x300

Konfiguration	Beispiele
Mitsumi-Laufwerk an einer MAD16-Soundkarte an E/A 330 und IRQ 1, DMA-Erkennung	isp16=0x330,11,0,Mitsumi
Sony CDU 531 an E/A 320	sonycd535=0x320

Bitte beachten

Die meisten neueren Sound Blaster-Karten verfügen über IDE-Schnittstellen. Für diese Karten sind keine `sbpcd`-Parameter notwendig. Verwenden Sie nur `hdx`-Parameter.

A.3 SCSI-Parameter

Tabelle A–3 SCSI-Parameter

Hardware	Modul	Parameter
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
AM53/79C974 PC-SCSI-Treiber Qlogic PCI-Basic	`AM53C974.o`	AM53C974=host-scsi-id, target-scsi-id,max-rate, max-offset
Die meisten Buslogic- (jetzt Mylex-) Karten mit "BT"-Teilenummer	`BusLogic.o`	BusLogic_Options=option,option,… (siehe `README.BusLogic` in …`drivers/scsi/`)
	`NCR53c406a.o`	ncr53c406a=io_port[, IRQ[, FASTPIO]] ncr53c406a io=io_port irq=IRQ fastpio=FASTPIO
Avansys SCSI-Karten	`avansys.o`	

Hardware	Modul	Parameter
Adaptec AHA 152x	`aha152x.o`	aha152x=io_base, IRQ, scsi_id, reconnect, parity
Adaptec AHA 1542	`aha1542.o`	aha1542=io_base,buson,busoff,dmaspeed
Adaptec AHA 1740	`aha1740.o`	
Adaptec AHA-274x, AHA-284x, AHA-29xx, AHA-394x, AHA-398x, AHA-274x, AHA-274xT, AHA-2842, AHA-2910B, AHA-2920C, AHA-2930/U/U2, AHA-2940/W/U/UW/AU/, U2W/U2/U2B/, U2BOEM, AHA-2944D/WD/UD/UWD, AHA-2950U2/W/B, AHA-3940/U/W/UW/, AUW/U2W/U2B, AHA-3950U2D, AHA-3985/U/W/UW, AIC-777x, AIC-785x, AIC-786x, AIC-787x, AIC-788x, AIC-789x, AIC-3860	`aic7xxx.o`	aic7xxx=string
Data Technology Corp DTC3180/3280	`dtc.o`	

Hardware	Modul	Parameter
DTP SCSI-Host-Adapter (EATA/DMA) PM2011B/9X ISA, PM2021A/9X ISA, PM2012A, PM2012B, PM2022A/9X EISA, PM2122A/9X, PM2322A/9X, SmartRAID PM3021, PM3222, PM3224	`eata.o`	eata=port0,port1,port2,… options eata io_port=port0,port1,port2,… option=value
DTP SCSI-Adapter PM2011, PM2021, PM2041, PM3021, PM2012B, PM2022, PM2122, PM2322, PM2042, PM3122, PM3222, PM3332, PM2024, PM2124, PM2044, PM2144, PM3224, PM3334	`eata_dma.o`	
DTP EATA-PIO-Boards	`eata_pio.o`	

Hardware	Modul	Parameter
Future Domain TMC-16x0-basierte Karten TMC-1800, TMC-18C50, TMC-18C30, TMC-36C70, Future Domain TMC-1650, TMC-1660, TMC-1670, TMC-1680, TMC-1610M/MER/MEX, TMC-3260 (PCI), Quantum ISA-200S, ISA-250MG, Adaptec AHA-2920A (PCI) (NICHT AHA-2920C)	`fdomain.o`	fdomain=io_base, IRQ[, ADAPTER_ID]
NCR5380- und NCR53c400-Karten	`g_NCR5380.o`	ncr5380=io_port,IRQ,dma ncr53c400=io_port,IRQ ncr5380 io=io_port irq=IRQ dma=dma ncr53c400 io=io_port irq=IRQ
GDT ISA/EISA/PCI Disk Array Controller	`gdth.o`	gdth=IRQ0,IRQ1,IRQ2,… options:values
IOMEGA MatchMaker SCSI-Adapter für Parallelport	`imm.o`	
Always IN2000 ISA SCSI-Karte	`in2000.o`	in2000=setup_string:value in2000 setup_string=value
Initio INI-9X00U/UW SCSI-Host-Adapter	`initio.o`	

Hardware	**Modul**	**Parameter**
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	
NCR SCSI-Controller mit den Chipsätzen 810/810A/815/ 825/825A/860/875/876/895	`ncr53c8xx.o`	ncr53c8xx=option1:value1,option2:value2,… ncr53c8xx="option1:value1 option2:value2…"
Pro Audio Spectrum/Studio 16	`pas16.o`	pas16=port,irq
IOMEGA PPA3 SCSI-Host-Adapter für Parallelport	`ppa.o`	
Perceptive Solutions PSI-240I EIDE	`psi240i.o`	
QLogic Fast SCSI FASXXX ISA/VLB/PCMCIA	`qlogicfas.o`	
QLogic ISP2100 SCSI-FCP	`qlogicfc.o`	
QLogic ISP1020 Intelligent SCSI-Karten IQ-PCI, IQ-PCI-10, IQ-PCI-D	`qlogicisp.o`	
Seagate ST01/ST02	`seagate.o`	controller_type=1 base_address=base_addr irq=irq
Future Domain TMC-885, TMC-950	`seagate.o`	controller_type=2 base_address=base_addr irq=irq

Hardware	Modul	Parameter
Karten mit dem sym53c416-Chipsatz	`sym53c416.o`	sym53c416=PORT-BASE[,IRQ] sym53c416 io=PORTBASE irq=IRQ
Trantor T128/T128F/T228 SCSI-Host-Adapter	`t128.o`	
Tekram DC390 und andere AMD53C974A-basierte PCI SCSI-Adapter	`tmscsim.o`	tmscsim=ID,SPEED
UltraStor 14F/34F SCSI-Host-Adapter (14F, 24F, 34F)	`u14-34f.o`	u14-34f=io_port1,io_port2,… io_port10 u14-34f io_port=io_port1,io_port2, … io_port10
UltraStor 14F, 24F und 34F	`ultrastor.o`	
WD7000-FASST2, WD7000-ASC, WD7000-AX/MX/EX	`wd7000.o`	wd7000=IRQ,dma,io_port wd7000 io=io_port irq=IRQ dma=dma

Es folgen einige Beispiele, wie diese Module verwendet werden:

Tabelle A–4 Konfigurationsbeispiele für SCSI-Parameter

Konfiguration	Beispiele
Adaptec AHA1522 an Port 330, IRQ 11, SCSI ID 7	aha152x=0x330,11,7
Adaptec AHA1542 an Port 330	bases=0x330
Future Domain TMC-800 an CA000, IRQ 10	controller_type=2 base_address=0xca000 irq=10

Wenn ein Parameter über Kommas verfügt, achten Sie darauf, nach einem Komma *keinen* Punkt zu setzen.

A.4 Ethernet-Parameter

Tabelle A–5 Ethernet-Modulparameter

Hardware	Modul	Parameter
3Com 3c501	`3c501.o`	3c501=io_port,IRQ
3Com 3c503 und 3c503/16	`3c503.o`	3c503=io_port,IRQ 3c503 io=io_port_1,io_port_n irq=IRQ_1,IRQ_n
3Com EtherLink Plus (3c505)	`3c505.o`	3c505=io_port,IRQ,DMA 3c505 io=io_port_1,io_port_n irq=IRQ_1,IRQ_2 dma=dma_1,dma_n
3Com EtherLink 16	`3c507.o`	3c507=io_port,IRQ 3c507 io=io_port irq=IRQ
3Com EtherLink III	`3c509.o`	3c509=IRQ
3Com ISA EtherLink XL "Corkscrew"	`3c515.o`	
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	
Apricot 680x0 VME, 82596-Chipsatz	`82596.o`	82596=IRQ 82596 irq=IRQ
Ansel Communications AC3200 EISA	`ac3200.o`	ac3200=io_port,IRQ ac3200 io=io_port_1,io_port_n irq=IRQ_1,IRQ_n

Hardware	Modul	Parameter
Alteon AceNIC Gigabit Ethernet-Treiber	`acenic.o`	acenic=trace,link acenic trace=trace link=val
Allied Telesis AT1700	`at1700.o`	at1700=io_port,IRQ at1700 io=io_port irq=IRQ
Tangent ATB-II, Novel NL-10000, Daystar Digital LT-200, Dayna DL2000, DaynaTalk PC (HL), COPS LT-95, Farallon PhoneNET PC II, III	`cops.o`	cops=io_port,IRQ cops io=io_port irq=IRQ
Modularer Treiber für die synchrone serielle COSA- oder SRP-Karte	`cosa.o`	cosa=io_port,IRQ,dma
Crystal LAN CS8900/CS8920	`cs89x0.o`	cs89x0=io_port,IRQ,MEDIA_TYPE cs89x0 io=io_port irq=IRQ media=TYPE
EtherWORKS DE425 TP/COAX EISA, DE434 TP PCI, DE435/450 TP/COAX/AUI PCI DE500 10/100 PCI Kingston, LinkSys, SMC8432, SMC9332, Znyx31[45] und Znyx346 10/100-Karten mit den Chipsätzen DC21040 (kein SROM), DC21041[A], DC21140[A], DC21142, DC21143	`de4x5.o`	de4x5=io_port de4x5 io=io_port de4x5 args='ethX[fdx] autosense=MEDIA_STRING'

Hardware	Modul	Parameter
D-Link DE-600 Ethernet Pocket Adapter	`de600.o`	
D-Link DE-620 Ethernet Pocket Adapter	`de620.o`	de620 io=io_port irq=IRQ bnc=1 utp=1
DIGITAL DEPCA & EtherWORKS DEPCA, DE100, DE101, DE200 Turbo, DE201Turbo DE202 Turbo TP/BNC, DE210, DE422 EISA	`depca.o`	depca=io_port,IRQ depca io=io_port irq=IRQ
Digi Intl. RightSwitch SE-X EISA und PCI	`dgrs.o`	
Cabletron Ethernet-Karten der Serie E2100	`e2100.o`	e2100=io_port,IRQ e2100 io=io_port irq=IRQ
Intel i82595 ISA EtherExpressPro10/10+-Treiber	`eepro.o`	eepro=io_port,IRQ,mem eepro io=io_port irq=IRQ mem=mem
Intel i82557/i82558 PCI EtherExpressPro-Treiber	`eepro100.o`	
Intel EtherExpress 16 (i82586)	`eexpress.o`	eexpress=io_port,IRQ eexpress io=io_port irq=IRQ
SMC EtherPower II 9432 PCI (Serie 83c170/175 EPIC)	`epic100.o`	
Racal-Interlan ES3210 EISA Network Adapter	`es3210.o`	es3210=io_port,IRQ,mem es3210 io=io_port irq=IRQ mem=mem

Hardware	**Modul**	**Parameter**
ICL EtherTeam 16i/32	`eth16i.o`	eth16i=io_port,mediatype eth16i ioaddr=io_port mediatype=type
EtherWORKS 3 (DE203, DE204 und DE205)	`ewrk3.o`	ewrk=io_port,IRQ ewrk io=io_port irq=IRQ
Fujitsu FMV-181/182/183/184	`fmv18x.o`	fmv18x=io_port,IRQ fmv18x io=io_port irq=IRQ
Modularer Treiber für den Comtrol Hostess SV11	`hostess_sv11.o`	hostess_sv11=io_port, IRQ, DMABIT hostess_sv11 io=io_port irq=IRQ dma=DMABIT
HP PCLAN/plus	`hp-plus.o`	hp-plus=io_port,IRQ hp-plus io=io_port irq=IRQ
HP LAN Ethernet	`hp.o`	hp=io_port,IRQ hp io=io_port irq=IRQ
100VG-AnyLan Network Adapter HP J2585B, J2585A, J2970, J2973, J2573 Compex ReadyLink ENET100-VG4, FreedomLine 100/VG	`hp100.o`	hp100=io_port,name hp100 hp100_port=io_port hp100_name=name
IBM Token Ring 16/4	`ibmtr.o`	ibmtr=io_port,IRQ,mem ibmtr io=io_port irq=IRQ mem=mem

Hardware	**Modul**	**Parameter**
AMD LANCE/PCnet Allied Telesis AT1500, HP J2405A, NE2100, NE2500	`lance.o`	lance=io_port,IRQ,dma lance io=io_port_1,io_port_n irq=IRQ_1,IRQ_2 dma=dma_1,dma_n
Mylex LNE390 EISA-Karten (LNE390A, LNE390B)	`lne390.o`	lne390=io_port,IRQ,mem lne390 io=io_port irq=IRQ mem=mem
	`ltpc.o`	ltpc=io_port,IRQ ltpc io=io_port irq=IRQ
NE1000 / NE2000 (kein PCI)	`ne.o`	ne=io_port,IRQ ne io=io_port irq=IRQ
PCI NE2000-Karten RealTEk RTL-8029, Winbond 89C940, Compex RL2000, KTI ET32P2, NetVin, NV5000SC, Via 82C926, SureCom NE34	`ne2k-pci.o`	
Novell NE3210 EISA Network Adapter	`ne3210.o`	ne3210=io_port,IRQ,mem ne3210 io=io_port irq=IRQ mem=mem
MiCom-Interlan NI5010 Ethernet-Karte	`ni5010.o`	ni5010=io_port,IRQ ni5010 io=io_port irq=IRQ
NI5210-Karte (i82586 Ethernet-Chip)	`ni52.o`	ni52=io_port,IRQ ni52 io=io_port irq=IRQ
NI6510, ni6510 EtherBlaster	`ni65.o`	ni65=io_port,IRQ,dma ni65 io=io_port irq=IRQ dma=dma

Hardware	Modul	Parameter
AMD PCnet32 und AMD PCnetPCI	`pcnet32.o`	
RedCreek Communications PCI	`rcpci.o`	
RealTek-Karten mit dem Chipsatz RTL8129 oder RTL8139 Fast Ethernet	`rtl8139.o`	
Sangoma S502/S508 Multi-Protokoll FR	`sdla.o`	
Sangoma S502A, ES502A, S502E, S503, S507, S508, S509	`sdladrv.o`	
SysKonnect Token Ring ISA/PCI Adapter, TR4/16(+) ISA oder PCI, TR4/16 PCI und ältere SK NET TR4/16 ISA-Karten	`sktr.o`	sktr=io_port,IRQ,mem sktr io=io_port irq=IRQ mem=mem
SMC Ultra und SMC EtherEZ ISA-Ethernet-Karte (8K, 83c790)	`smc-ultra.o`	smc-ultra=io_port,IRQ smc-ultra io=io_port irq=IRQ
SMC Ultra32 EISA Ethernet-Karte (32K)	`smc-ultra32.o`	
Ethernet-Karten der Serie SMC 9000	`smc9194.o`	smc9194=io_port,IRQ smc9194 io=io_port irq=IRQ ifport=[0,1,2]

Hardware	Modul	Parameter
Compaq Netelligent 10/100 TX PCI UTP Compaq Netelligent 10 T PCI UTP Compaq Integrated NetFlex 3/P Compaq Netelligent Dual 10/100 TX PCI UTP Compaq Netelligent Integrated 10/100 TX UTP Compaq Netelligent 10/100 TX Embedded UTP Compaq Netelligent 10 T/2 PCI UTP/Coax Compaq Netelligent 10/100 TX UTP Compaq NetFlex 3/P Olicom OC-2325, OC-2183, OC-2326	`tlan.o`	tlan=io_port,IRQ,aui,debug tlan io=io_port irq=IRQ Weitere Moduloptionen: speed=10Mbs,100Mbs debug=0x0[1,2,4,8] aui=1 duplex=[1,2]
Digital 21x4x Tulip PCI Ethernet-Karten SMC EtherPower 10 PCI(8432T/8432BT) SMC EtherPower 10/100 PCI(9332DST) DEC EtherWorks 100/10 PCI(DE500-XA) DEC EtherWorks 10 PCI(DE450) DEC QSILVER's, Znyx 312 Etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	

Hardware	Modul	Parameter
VIA Rhine PCI Fast Ethernet-Karten entweder mit VIA VT86c100A Rhine-II PCI oder 3043 Rhine-I D-Link DFE-930-TX PCI 10/100	`via-rhine.o`	
AT&T GIS (früher NCR) WaveLan ISA-Karte	`wavelan.o`	wave-lan=[IRQ,0],io_port,NWID
WD8003 und WD8013-"kompatible" Ethernet-Karten	`wd.o`	wd=io_port, IRQ, mem,mem_end wd io=io_port irq=IRQ mem=mem mem_end=end
Packet Engines Yellowfin	`yellowfin.o`	
G-NIC PCI Gigabit Ethernet-Adapter		
Z8530-basierte HDLC-Karten für AX.25	`z85230.o`	

Es folgen einige Beispiele, wie diese Module verwendet werden:

Tabelle A–6 Konfigurationsbeispiele für Ethernet-Parameter

Konfiguration	Beispiele
NE2000 ISA-Karte an E/A 300 und IRQ 11	ne=0x300,11 ether=0x300,11,eth0
Wavelan-Karte an E/A 390, automatische IRQ-Erkennung und Verwendung der NWID bis 0x4321	wavelan=0,0x390,0x4321 ether=0,0x390,0x4321,eth0

A.4.1 Verwenden mehrerer Ethernet-Karten

Sie können in einem Computer mehrere Ethernet-Karten verwenden. Wenn die Karten mit unterschiedlichen Treibern arbeiten (z.B. 3c509 und DE425), müssen Sie lediglich der Datei `/etc/conf.modules` für jede Karte eine `alias`-Zeile (und eventuell eine `options`-Zeile) hinzufügen. Weitere Informationen finden Sie in Abschnitt 3.2.2, *Laden von Kernelmodulen*.

Wenn zwei Ethernet-Karten denselben Treiber verwenden (z.B. zwei 3c509 oder eine 3c595 und eine 3c905), müssen Sie den beiden Karten entweder in der options-Zeile des Treibers Adressen zuweisen (bei ISA-Karten), oder Sie fügen einfach für jede Karte eine `alias`-Zeile hinzu (bei PCI-Karten).

http://metalab.unc.edu/LDP/HOWTO/Ethernet-HOWTO.html Weitere Informationen über die Verwendung mehrerer Ethernet-Karten finden Sie im *Linux Ethernet-HOWTO* unter http://metalab.unc.edu/LDP/HOWTO/Ethernet-HOWTO.html. Wenn Sie bei der Installation von Red Hat Linux das `howto`-Paket installiert haben, finden Sie die entsprechenden Informationen in der Datei `/usr/share/doc/HOWTO/Ethernet-HOWTO`.

B Eine Einführung in Festplattenpartitionen

Festplattenpartitionen bilden einen grundlegenden Bestandteil der PC-Welt, und das nicht erst seit gestern. Da jedoch viele Computer mit vorinstalliertem Betriebssystem gekauft werden, wissen relativ wenige Benutzer, wie Partitionen wirklich funktionieren. In diesem Kapitel wollen wir die Funktionsweise von Festplattenpartitionen erklären, damit Ihnen die Red Hat Linux Installation so leicht wie möglich fällt.

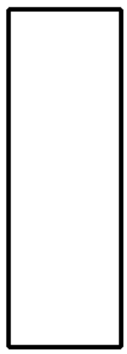
Wenn Sie mit Festplattenpartitionen bereits vertraut sind, fahren Sie fort mit Abschnitt B.1.4, *Verfügbarmachen von Festplattenspeicher für Red Hat Linux*. Hier erfahren Sie, wie Sie als Vorbereitung für eine Red Hat Linux Installation Festplattenspeicher freigeben. In diesem Abschnitt werden auch verwandte Themen wie das von Linux-Systemen verwendete Namensschema für Partitionen oder die gemeinsame Nutzung von Festplattenspeicher mit anderen Betriebssystemen behandelt.

B.1 Grundlagenwissen zu Festplatten

Festplatten haben eine sehr einfache Funktion - sie speichern Daten und rufen sie auf Befehl wieder ab.

Das Thema Festplattenpartitionierung erfordert auch, dass man sich etwas mit der zugrunde liegenden Hardware auskennt. Leider kann man sich dabei leicht in Einzelheiten verlieren. Lassen Sie uns daher eine vereinfachte Darstellung einer Festplatte betrachten, um zu verstehen, was "unter der Oberfläche" vor sich geht. Abbildung B–1, *Eine unformatierte Festplatte* zeigt eine neue, unbenutzte Festplatte.

Abbildung B–1 Eine unformatierte Festplatte

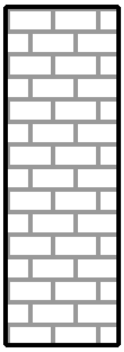


Es ist nicht gerade viel zu sehen, aber für eine einfache Erklärung von Festplatten reicht es aus. Angenommen, wir möchten Daten auf diesem Laufwerk speichern. So wie die Festplatte im Moment aussieht, kann das nicht funktionieren. Wir müssen zuerst noch etwas tun…

B.1.1 Nicht was Sie schreiben ist wichtig, sondern wie Sie es schreiben

Die Erfahreneren unter den Lesern haben es wahrscheinlich gleich erraten. Wir müssen die Festplatte zuerst **formatieren**. Beim Formatieren (im Linux-Sprachgebrauch auch als "Erstellen eines **Dateisystems**" bezeichnet) werden Informationen auf die Festplatte geschrieben, die Ordnung in den leeren Speicherplatz einer unformatierten Festplatte bringen.

Abbildung B–2 Festplatte mit Dateisystem



Wie Abbildung B–2, *Festplatte mit Dateisystem* andeutet, erfordert die von einem Dateisystem hergestellte Ordnung einige Zugeständnisse:

- Ein kleiner Prozentsatz des Platzes auf der Festplatte wird zum Speichern von dateisystembezogenen Daten verwendet (Overhead).
- Ein Dateisystem teilt den verbleibenden Platz in kleine Segmente gleicher Größe ein. In der Linux-Welt werden diese Segmente als **Blöcke** bezeichnet. [1]

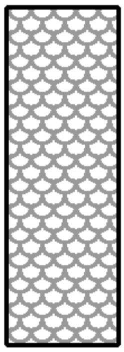
In Anbetracht der Tatsache, dass Dateisysteme Verzeichnisse und Dateien erst möglich machen, fallen diese kleinen Abweichungen nicht allzu sehr ins Gewicht.

Es gibt übrigens nicht nur ein einziges, universelles Dateisystem. Wie Abbildung B–3, *Festplatte mit einem anderen Dateisystem* zeigt, gibt es verschiedene Dateisysteme für Festplatten. Wie Sie sich vorstellen können, sind verschiedene Dateisysteme

[1] Blöcke *haben* im Gegensatz zu unseren Abbildungen immer die gleiche Größe. Beachten Sie auch, dass eine durchschnittliche Festplatte Tausende von Blöcken enthält. Für unsere Betrachtung sollen solche unwesentlichen Diskrepanzen aber keine Rolle spielen.

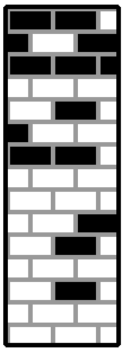
oftmals untereinander nicht kompatibel, d.h. ein Betriebssystem, das ein Dateisystem unterstützt (oder mehrere verwandte Dateisystemtypen), unterstützt ein anderes Dateisystem möglicherweise nicht. Die letzte Aussage gilt jedoch nicht immer. Red Hat Linux unterstützt z.B. eine Vielzahl von Dateisystemen (darunter viele Dateisysteme anderer Betriebssysteme). Das erleichtert den Datenaustausch.

Abbildung B–3 Festplatte mit einem anderen Dateisystem



Natürlich ist das Schreiben eines Dateisystems auf die Festplatte nur der Anfang. Ziel ist es, Daten *zu speichern* und *abzurufen*. Schauen wir uns die Festplatte an, nachdem einige Daten darauf geschrieben worden sind.

Abbildung B–4 Mit Daten beschriebene Festplatte



Wie Abbildung B–4, *Mit Daten beschriebene Festplatte* zeigt, enthalten jetzt 14 der zuvor leeren Blöcke Daten. Wir können keine Aussage darüber machen, wie viele Dateien auf der Festplatte gespeichert sind. Es kann nur eine sein, es können aber auch 14 sein, denn alle Dateien verwenden mindestens einen Block. Ein weiterer wichtiger Punkt ist, dass die verwendeten Blöcke nicht unmittelbar hintereinander liegen müssen. Verwendete und nicht verwendete Blöcke können auf der Festplatte verstreut sein. Dies wird als **Fragmentierung** bezeichnet. Die Fragmentierung muss bei der Änderung der Größe einer Partition berücksichtigt werden.

Wie die meisten Technologien im Computerbereich wurden auch Festplatten ständig weiter entwickelt. Insbesondere in einer Hinsicht - sie wurden immer größer. Nicht was ihre Abmessungen betrifft, sondern ihre Kapazität. Das führte zu Änderungen beim Einsatz von Festplatten.

B.1.2 Partitionen - aus einer Festplatte werden mehrere

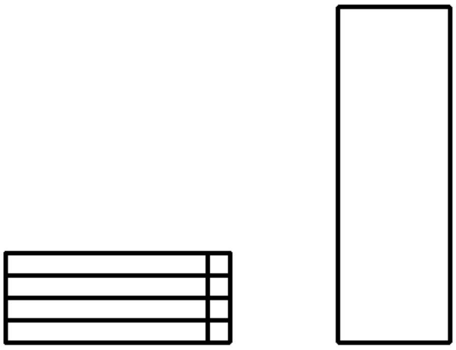
Als die Kapazitäten der Festplatten immer größer wurden, fragte sich so mancher, ob es wirklich sinnvoll ist, mit so einem großen Festplattenspeicher in einem Stück zu arbeiten. Dieser Gedanke war sowohl in organisatorischen als auch in technischen Fragen begründet. Was die Organisation angeht, so schien es, dass ab einer bestimmten Größe der zusätzliche Speicherplatz größerer Festplatten nur noch für mehr Unordnung sorgte. Rein technisch gesehen waren manche Dateisysteme für die Unterstützung größerer Festplatten einfach nicht ausgelegt. Manche Dateisysteme *unterstützten* zwar größere Festplatten, aber ein übermäßiger Verwaltungsaufwand war die Folge.

Die Lösung des Problems war, die Festplatten in **Partitionen** aufzuteilen. Auf jede Partition kann wie auf eine separate Festplatte zugegriffen werden. Dies wird durch das Hinzufügen von **Partitionstabellen** ermöglicht.

Bitte beachten

In den Abbildungen dieses Kapitels wird die Partitionstabelle getrennt von der eigentlichen Festplatte dargestellt. Das ist nicht ganz richtig. In Wirklichkeit wird die Partitionstabelle ganz am Anfang der Festplatte gespeichert (vor dem Dateisystem und den Benutzerdaten). Nur der Übersicht wegen wurde für unsere Abbildungen die getrennte Darstellung gewählt.

Abbildung B–5 Festplatte mit Partitionstabelle



Wie Abbildung B–5, *Festplatte mit Partitionstabelle* zeigt, ist die Partitionstabelle in vier Abschnitte eingeteilt. Jeder Abschnitt kann die für die Definition einer Partition notwendigen Informationen aufnehmen, d.h. die Partitionstabelle kann nicht mehr als vier Partitionen definieren.

Jeder Eintrag in der Partitionstabelle enthält mehrere wichtige Angaben über die Partition:

- Die Punkte auf der Festplatte, wo die Partition beginnt und endet
- Ob die Partition "aktiv" ist
- Den Partitionstyp

Wir wollen uns die Angaben zur Partition etwas näher anschauen. Die Start- und Endpunkte definieren die Größe und Lage der Partition auf der Festplatte. Das "aktiv"-Flag wird von Bootloadern einiger Betriebssysteme verwendet, d.h. es wird das Betriebssystem von der Partition gestartet, das als "aktiv" markiert ist.

Die Angabe des Partitionstyps kann etwas verwirren. Der Typ besteht aus einer Zahl, die die beabsichtigte Verwendung der Partition angibt. Wenn diese Angabe etwas verschwommen wirkt, so ist das darin begründet, dass nicht exakt festgelegt ist, was ein Partitionstyp eigentlich ist. Manche Betriebssysteme kennzeichnen mit dem Partitionstyp, dass es sich um einen speziellen Dateisystemtyp handelt, dass die Partition mit einem bestimmten Betriebssystem verknüpft ist, dass die Partition ein startfähiges Betriebssystem enthält, oder eine Kombination aus diesen drei Punkten.

Tabelle B–1, *Partitionstypen* enthält eine Liste mit einigen weitverbreiteten (sowie weniger bekannten) Partitionstypen einschließlich ihrer Zahlenwerte.

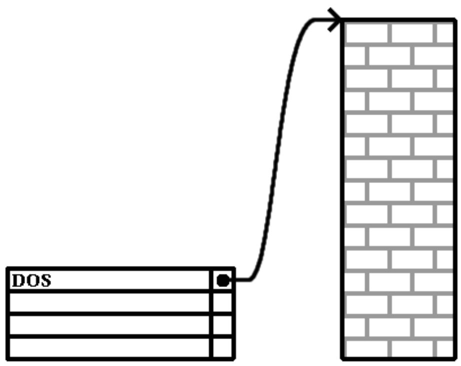
Tabelle B–1 Partitionstypen

Partitionstyp	Wert	Partitionstyp	Wert
leer	00	Novell Netware 386	65
DOS 12-Bit FAT	01	PIC/IX	75
XENIX root	02	Old MINIX	80
XENIX usr	03	Linux/MINUX	81
DOS 16-Bit <=32 MB	04	Linux swap	82
Extended	05	Linux native	83
DOS 16-Bit >=32 MB	06	Linux extended	85
OS/2 HPFS	07	Amoeba	93
AIX	08	Amoeba BBT	94
AIX bootable	09	BSD/386	a5
OS/2 Boot Manager	0a	OpenBSD	a6
Win95 FAT32	0b	NEXTSTEP	a7
Win95 FAT32 (LBA)	0c	BSDI fs	b7
Win95 FAT16 (LBA)	0e	BSDI swap	b8
Win95 Extended (LBA)	0f	Syrinx	c7

Partitionstyp	Wert	Partitionstyp	Wert
Venix 80286	40	CP/M	db
Novell?	51	DOS access	e1
Microport	52	DOS R/O	e3
GNU HURD	63	DOS secondary	f2
Novell Netware 286	64	BBT	ff

Sie fragen sich jetzt vielleicht, wie diese zusätzlichen komplexen Zusammenhänge üblicherweise in der Praxis aussehen. Abbildung B–6, *Festplatte mit einer Partition* zeigt ein Beispiel.

Abbildung B–6 Festplatte mit einer Partition



In vielen Fällen gibt es nur eine einzige Partition für die ganze Festplatte (also im Grunde so wie früher, als es noch keine Partitionen gab). Die Partitionstabelle enthält nur einen Eintrag, der auf den Anfang der Partition zeigt.

Wir haben für diese Partition den Typ "DOS" gewählt. Wie Sie aus Tabelle B–1, *Partitionstypen* entnehmen können, ist diese Darstellungsweise etwas vereinfacht, aber für unsere Betrachtung ausreichend. Dies ist eine typische Partitionsvariante, wie sie bei den meisten neu gekauften Computern mit vorinstalliertem Windows zu finden ist.

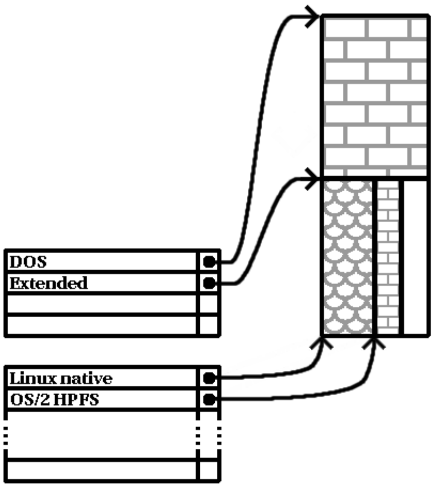
B.1.3 Partitionen innerhalb von Partitionen - ein Überblick über erweiterte Partitionen

Mit der Zeit wurde natürlich klar, dass vier Partitionen nicht ausreichen. Mit zunehmender Kapazität der Festplatten wuchs die Wahrscheinlichkeit, dass vier Partitionen in üblicher Größe konfiguriert werden konnten und immer noch Platz auf der Festplatte frei war. Es musste ein Weg gefunden werden, mehr Partitionen zu erstellen.

Hier kommt die erweiterte Partition ins Spiel. Vielleicht ist Ihnen in Tabelle B–1, *Partitionstypen* aufgefallen, dass es einen Partitionstyp "Extended" (Erweitert) gibt. Genau dieser Partitionstyp wird für erweiterte Partitionen verwendet. Das funktioniert so:

Wenn eine Partition erstellt und als Typ "Extended" (Erweitert) eingestellt wird, wird eine erweiterte Partitionstabelle angelegt. Die erweiterte Partition ist im Prinzip eine Festplatte innerhalb der Festplatte - sie verfügt über eine Partitionstabelle, die auf eine oder mehrere Partitionen zeigt (jetzt **logische Partitionen** genannt, im Gegensatz zu den vier **primären Partitionen**), die vollständig innerhalb der erweiterten Partition liegen. Abbildung B–7, *Festplatte mit erweiterter Partition* zeigt eine Festplatte mit einer primären Partition und einer erweiterten Partition, die zwei logische Partitionen enthält (neben einer geringen Menge von nicht partitioniertem Speicherplatz).

Abbildung B–7 Festplatte mit erweiterter Partition



Wie in der Abbildung zu sehen ist, unterscheiden sich primäre und logische Partitionen - es kann nur vier primäre Partitionen geben, aber die Anzahl der logischen Partitionen ist nicht begrenzt. (In der Praxis sollten jedoch nicht mehr als 12 logische Laufwerke auf einer Festplatte angelegt werden.)

Nachdem Partitionen im Allgemeinen besprochen wurden, soll betrachtet werden, wie diese Kenntnisse für die Installation von Red Hat Linux genutzt werden können.

B.1.4 Verfügbarmachen von Festplattenspeicher für Red Hat Linux

Sie können beim Versuch, die Festplatte neu zu partitionieren, drei mögliche Szenarien vorfinden:

- Nicht partitionierter freier Festplattenspeicher ist verfügbar.
- Eine unbenutzte Partition ist verfügbar.
- Auf einer aktiv genutzten Partition ist noch freier Festplattenspeicher verfügbar.

Sehen wir uns die Szenarien der Reihe nach an.

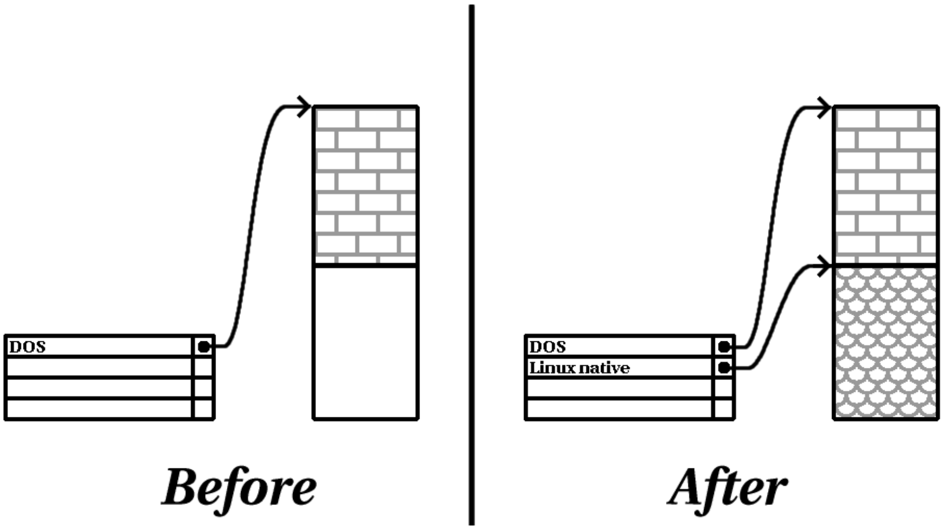
Bitte beachten

Die Abbildungen in diesem Abschnitt wurden der Klarheit wegen vereinfacht und geben nicht die genaue Partitionsaufteilung wieder, die Sie bei der tatsächlichen Installation von Red Hat Linux vorfinden.

Nicht partitionierter freier Festplattenspeicher

In diesem Fall belegen die bereits definierten Partitionen nicht die gesamte Festplatte, so dass noch nicht zugewiesener Speicher vorhanden ist, der nicht Teil einer definierten Partition ist. Abbildung B–8, *Festplatte mit nicht partitioniertem freien Platz* zeigt, wie dies aussehen könnte.

Abbildung B–8 Festplatte mit nicht partitioniertem freien Platz



Genau genommen fällt eine nicht verwendete Festplatte ebenfalls in diese Kategorie. Der einzige Unterschied besteht darin, dass der *gesamte* Festplattenspeicher nicht Teil einer definierten Partition ist.

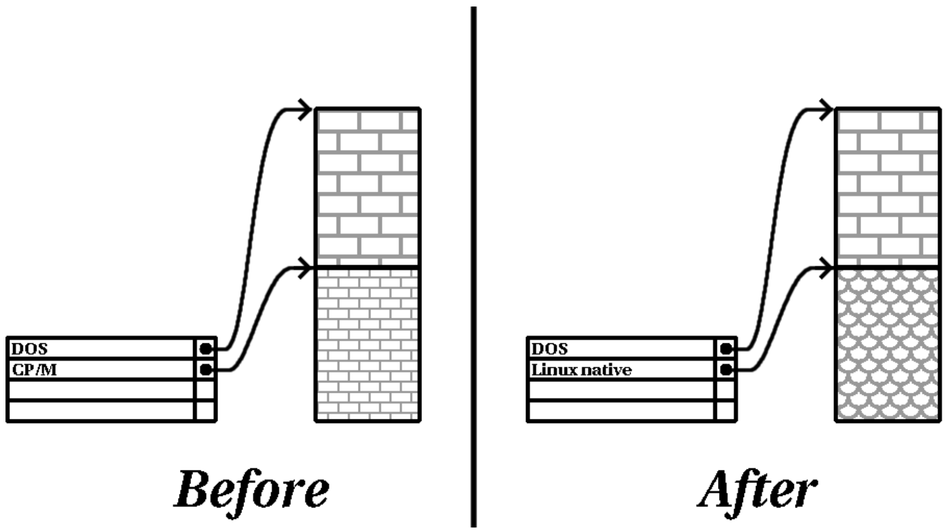
Auf jeden Fall können Sie einfach die notwendigen Partitionen auf dem unbenutzten Festplattenspeicher erstellen. Leider ist es sehr unwahrscheinlich, dass Sie dieses sehr einfache Szenario vorfinden (es sei denn, Sie haben extra für Red Hat Linux eine neue Festplatte gekauft).

Weiter geht's mit einer etwas alltäglicheren Situation.

Festplattenspeicher auf einer unbenutzten Partition

In diesem Fall sind möglicherweise eine oder mehrere Partitionen vorhanden, die nicht mehr gebraucht werden. Vielleicht haben Sie vorher ein anderes Betriebssystem ausprobiert, und Sie benötigen die diesem System zugewiesenen Partitionen nicht mehr. Abbildung B–9, *Festplatte mit einer unbenutzten Partition* zeigt eine solche Situation.

Abbildung B–9 Festplatte mit einer unbenutzten Partition



Wenn diese Situation vorliegt, können Sie den Platz verwenden, der der nicht benutzten Partition zugewiesen ist. Sie müssen zunächst die Partition löschen und stattdessen dann die geeignete(n) Linux-Partition(en) erstellen. Entweder löschen Sie die Partition mit dem DOS-Befehl `fdisk`, oder Sie benutzen dazu die während einer benutzerdefinierten Installation angebotene Option.

Freier Festplattenspeicher auf einer aktiven Partition

Diese Situation kommt am häufigsten vor. Leider ist sie auch die schwierigste. Selbst wenn genügend freier Festplattenspeicher vorhanden ist, besteht das Hauptproblem darin, dass dieser bereits einer Partition zugewiesen ist, die genutzt wird. Wenn Sie einen Computer mit vorinstallierter Software kaufen, befindet sich auf der Festplatte sehr wahrscheinlich eine große Partition, in der das Betriebssystem und alle Dateien enthalten sind.

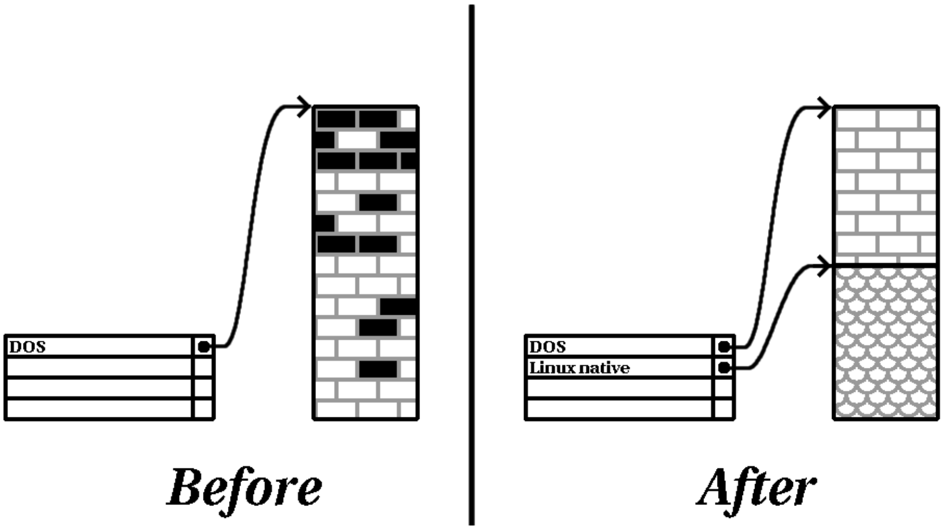
Sofern Sie keine neue Festplatte in das System einbauen, stehen Ihnen zwei Möglichkeiten zur Verfügung:

Neupartitionieren mit Datenverlust

Im Wesentlichen löschen Sie eine große Partition und erstellen mehrere kleinere. Wie Sie sich möglicherweise vorstellen können, werden dabei alle Daten, die in der ursprünglichen Partition vorhanden sind, zerstört. Das bedeutet, dass zuvor eine komplette Sicherungskopie erstellt werden muss. Erstellen Sie zur Sicherheit zwei Sicherungskopien, führen Sie eine Prüfung auf Übereinstimmung durch (falls Ihre Backup-Software über eine CRC-Prüfung verfügt), und prüfen Sie zunächst, ob sich die Daten von der Sicherungskopie lesen lassen, *bevor* Sie die Partition löschen. Wenn auf dieser Partition ein Betriebssystem installiert war, beachten Sie bitte auch, dass dieses später ebenfalls erneut installiert werden muss.

Nach dem Erstellen einer kleineren Partition für die vorhandene Software können Sie alle Programme neu installieren, die Daten wiederherstellen und die Installation von Red Hat Linux fortsetzen. Abbildung B–10, *Festplatte, mit Datenverlust neu partitioniert* zeigt diesen Vorgang.

Abbildung B–10 Festplatte, mit Datenverlust neu partitioniert



ACHTUNG

Wie aus Abbildung B–10, *Festplatte, mit Datenverlust neu partitioniert* ersichtlich ist, gehen alle in der ursprünglichen Partition vorhandenen Daten ohne ordnungsgemäßes Backup verloren!

Neupartitionieren ohne Datenverlust

Dabei wird ein Programm ausgeführt, das scheinbar Unmögliches vollbringt: es verkleinert eine große Partition, ohne dass dabei Dateien verloren gehen, die in dieser Partition gespeichert sind. Diese Methode hat sich für viele als zuverlässig und fehlerfrei erwiesen. Für das Festplattenmanagement sind verschiedene Software-Produkte erhältlich. Erkundigen Sie sich bitte danach, und finden Sie das für Ihre Situation geeignete Programm heraus.

Auch wenn der Neupartitionierungsvorgang ohne Datenverlust ziemlich geradlinig verläuft, setzt er sich doch aus einigen Teilschritten zusammen:

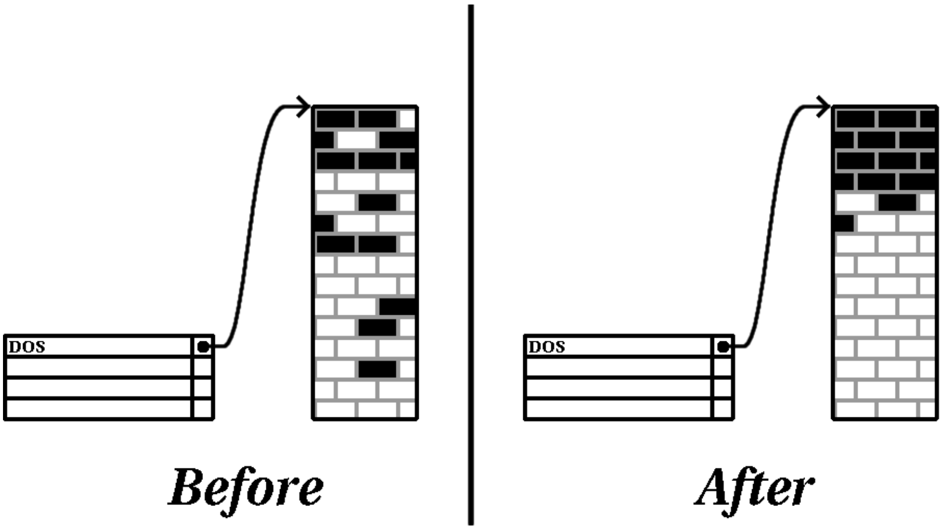
- Komprimieren vorhandener Daten
- Ändern der Partitionsgröße
- Erstellen neuer Partition(en)

Betrachten wir die einzelnen Schritte einmal näher.

Komprimieren vorhandener Daten

Wie Abbildung B–11, *Festplatte, komprimiert* zeigt, besteht der erste Schritt darin, die Daten in der vorhandenen Partition zu komprimieren. Auf diese Weise werden die Daten neu angeordnet, so dass der verfügbare freie Festplattenspeicher am "Ende" der Partition maximale Größe erreicht.

Abbildung B–11 Festplatte, komprimiert



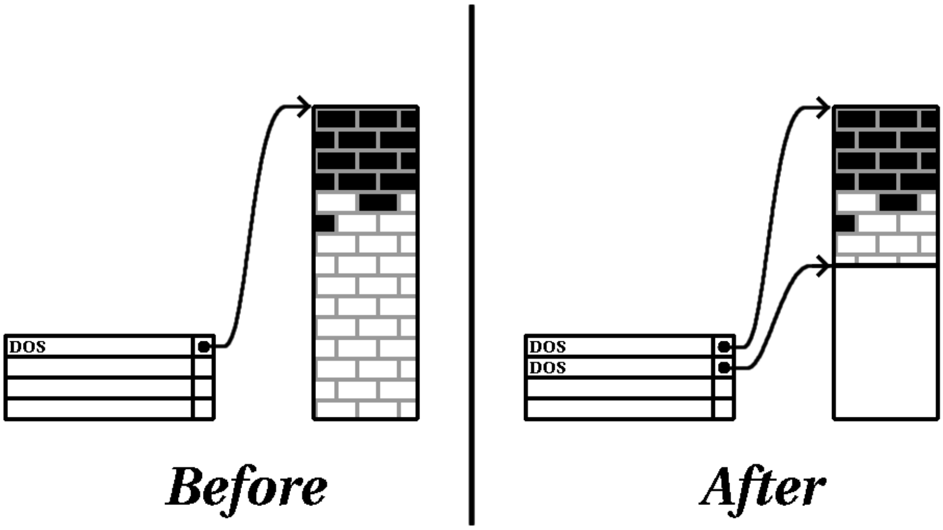
Dieser Schritt ist entscheidend. Wenn er ausgelassen wird, kann die Position der Daten verhindern, dass die Partition auf die gewünschte Größe gebracht werden kann. Beachten Sie auch, dass, aus welchen Gründen auch immer, manche Daten nicht verschoben werden können. Wenn dies der Fall ist (und dadurch die Größe der neuen

Partition(en) eingeschränkt wird), müssen Sie möglicherweise die Festplatte mit Datenverlust neu partitionieren.

Ändern der Partitionsgröße

Abbildung B–12, *Festplatte mit geänderter Partitionsgröße* zeigt den tatsächlichen Größenänderungsvorgang. Während das Ergebnis der Größenänderung je nach verwendeter Software variiert, wird in den meisten Fällen der freigegebene Platz zum Erstellen einer nicht formatierten Partition des gleichen Typs wie die ursprüngliche Partition verwendet.

Abbildung B–12 Festplatte mit geänderter Partitionsgröße

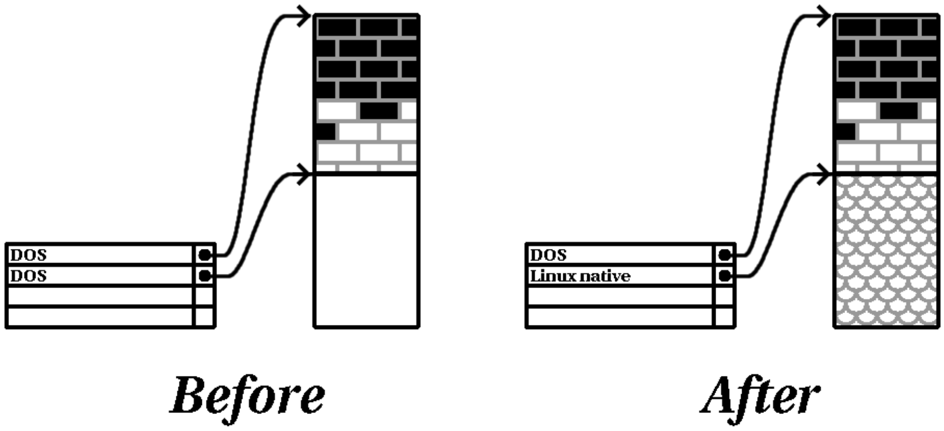


Wichtig ist, dass Sie verstehen, was die Größenänderungs-Software mit dem freigegebenen Platz macht, damit Sie die geeigneten Schritte durchführen können. In dem dargestellten Fall wäre es das Beste, die neue DOS-Partition zu löschen und (eine) geeignete Linux-Partition(en) zu erstellen.

Erstellen neuer Partition(en)

Nach dem vorherigen Schritt kann es notwendig sein, neue Partitionen zu erstellen. Wenn die Größenänderungs-Software Linux nicht berücksichtigt, müssen Sie wahrscheinlich die Partition, die während der Größenänderung erstellt wurde, löschen. Abbildung B–13, *Festplatte mit endgültiger Partitionskonfiguration* zeigt diesen Vorgang.

Abbildung B–13 Festplatte mit endgültiger Partitionskonfiguration



Intel

Die folgenden Informationen gelten nur für Intel-basierte Computer.

Um unseren Kunden die Arbeit zu erleichtern, bieten wir das Dienstprogramm `fips` an. Dieses frei verfügbare Programm kann die Größe von FAT (File Allocation Table)-Partitionen ändern. Sie finden es auf der Red Hat Linux/Intel CD-ROM im Verzeichnis `dosutils`.

Bitte beachten

Viele haben `fips` bereits erfolgreich zum Neupartitionieren von Festplatten verwendet. Wegen der Art der von `fips` ausgeführten Vorgänge und der Vielfalt der Hardware- und Software-Konfigurationen, unter denen das Programm laufen muss, kann Red Hat nicht garantieren, dass `fips` auf Ihrem System korrekt arbeitet. Deshalb gibt es für `fips` keinerlei Installationsunterstützung. Sie benutzen das Programm auf eigenes Risiko.

Wenn Sie sich trotzdem entschließen, Ihre Festplatte mit `fips` neu zu partitionieren, müssen Sie *unbedingt* zwei Dinge beachten:

- Erstellen Sie ein Backup - Erstellen Sie zwei Kopien von allen wichtigen Daten auf Ihrem Computer. Diese Kopien sollten auf Wechseldatenträgern (z.B. Band oder Disketten) gespeichert werden. Überprüfen Sie, ob die Datenträger lesbar sind, bevor Sie fortfahren.
- Lesen Sie die Dokumentation - Lesen Sie bitte die Dokumentation zu `fips`, die sich auf der Red Hat Linux/Intel CD 1 im Unterverzeichnis `/dosutils/fipsdocs` befindet.

Sollten Sie sich dazu entschließen, `fips` zu verwenden, beachten Sie bitte, dass nach der Ausführung von `fips` *zwei* Partitionen vorhanden sind: eine mit einer geänderten Größe und eine, die von `fips` auf dem verfügbar gemachten Festplattenspeicher erstellt wurde. Wenn Sie diesen Platz für die Installation von Red Hat Linux verwenden möchten, müssen Sie die neu erstellte Partition löschen. Verwenden Sie dazu `fdisk` unter dem aktuellen Betriebssystem, oder nutzen Sie die entsprechende Option beim Einrichten von Partitionen während einer benutzerdefinierten Installation.

B.1.5 Benennen von Partitionen

Linux bezeichnet Festplattenpartitionen unter Verwendung einer Kombination aus Buchstaben und Ziffern. Wenn Sie gewöhnt sind, Festplatten und deren Partitionen als "C-Laufwerk" usw. zu bezeichnen, kann dies verwirrend für Sie sein. In der DOS/Windows-Welt werden Partitionen folgendermaßen benannt:

- Jeder Partitionstyp wird überprüft, um festzustellen, ob er von DOS/Windows gelesen werden kann.
- Wenn der Partitionstyp kompatibel ist, erhält er einen "Laufwerksbuchstaben". Der erste Laufwerksbuchstabe lautet stets "C".
- Der Laufwerksbuchstabe kann dann dazu verwendet werden, um auf diese Partition sowie das Dateisystem, das in dieser Partition enthalten ist, zu verweisen.

Red Hat Linux arbeitet mit einem flexibleren Namensschema, das mehr Informationen enthält als das von anderen Betriebssystemen. Das Namensschema ist dateiorientiert, mit Dateinamen der Form:

```
/dev/xxyN
```

So entschlüsseln Sie das Namensschema für Partitionen:

`/dev/`

Diese Zeichenkette ist der Name des Verzeichnisses, in dem alle Gerätedateien abgelegt sind. Da sich Partitionen auf Festplatten befinden und Festplatten Geräte sind, befinden sich die Dateien für alle möglichen Partitionen in `/dev/`.

`xx`

Die ersten beiden Buchstaben des Partitionsnamens kennzeichnen den Typ des Geräts, auf dem sich die Partition befindet. Sie sehen normalerweise `hd` (für IDE-Laufwerke) oder `sd` (für SCSI-Laufwerke).

`y`

Dieser Buchstabe kennzeichnet, auf welchem Gerät sich die Partition befindet. Zum Beispiel `/dev/hda` (auf der ersten IDE-Festplatte) oder `/dev/sdb` (auf dem zweiten SCSI-Laufwerk).

N

Die Endziffer kennzeichnet die Partition. Die ersten vier (primären oder erweiterten) Partitionen sind von `1` bis `4` durchnummeriert. Logische Partitionen beginnen bei `5`. Beispielsweise ist `/dev/hda3` die dritte primäre oder erweiterte Partition auf der ersten IDE-Festplatte. `/dev/sdb6` ist die zweite logische Partition auf der zweiten SCSI-Festplatte.

Bitte beachten

Kein Teil dieser Namenskonvention basiert auf dem Partitionstyp. Im Gegensatz zu DOS/Windows können unter Red Hat Linux *alle* Partitionen erkannt werden. Das heißt nicht, dass Red Hat Linux auf die Daten aller Partitionstypen zugreifen kann. Aber in vielen Fällen ist es möglich, auf Daten zuzugreifen, die sich in einer Partition befinden, die von einem anderen Betriebssystem verwendet wird.

Behalten Sie diese Informationen im Hinterkopf. Sie erleichtern das Verständnis, wenn Sie die für Red Hat Linux erforderlichen Partitionen einrichten.

B.1.6 Festplattenpartitionen und andere Betriebssysteme

Wenn Ihre Red Hat Linux Partitionen eine Festplatte mit von anderen Betriebssystemen verwendeten Partitionen gemeinsam nutzen, gibt es in der Regel keine Schwierigkeiten. Es gibt jedoch bestimmte Kombinationen aus Linux und anderen Betriebssystemen, die zusätzliche Sorgfalt erfordern. Informationen zum Erstellen von Festplattenpartitionen, die mit anderen Betriebssystemen kompatibel sind, finden Sie in mehreren HOWTOs und Mini-HOWTOs, die auf der Red Hat Linux CD-ROM in den Verzeichnissen `doc/HOWTO` und `doc/HOWTO/mini` zu finden sind. Insbesondere sind die Mini-HOWTOs, deren Namen mit `Linux+` beginnen, recht hilfreich.

Intel

Wenn Red Hat Linux/Intel zusammen mit OS/2 auf Ihrem Computer verwendet werden soll, müssen Sie die Festplattenpartitionen mit der Partitionierungs-Software von OS/2 erstellen - sonst erkennt OS/2 möglicherweise die Partitionen nicht. Während der Installation erstellen Sie keine neuen Partitionen, sondern Sie stellen die richtigen Partitionstypen für Ihre Linux-Partitionen mit Hilfe von Linux `fdisk` ein.

B.1.7 Festplattenpartitionen und Mount-Points

Was Linux-Anfänger immer wieder verwirrt, ist die Tatsache, wie Partitionen vom Betriebssystem Linux verwendet werden und wie der Zugriff darauf erfolgt. Unter DOS/Windows ist das relativ einfach: Wenn mehr als eine Partition vorhanden ist, erhält jede Partition ihren eigenen "Laufwerksbuchstaben". Mit diesem Laufwerksbuchstaben können Sie dann Dateien und Verzeichnisse auf einer bestimmten Partition ansprechen.

Red Hat Linux geht völlig anders mit Partitionen - und Plattenspeicher im Allgemeinen - um. Der Hauptunterschied besteht darin, dass jede Partition dazu verwendet wird, einen Teilbereich des Speichers zu bilden, der für die Aufnahme einer Gruppe von Dateien und Verzeichnissen benötigt wird. Dies geschieht durch Zuordnung einer Partition zu einem Verzeichnis mit Hilfe eines Prozesses, der als **Mounten** bezeichnet wird. Durch das Mounten einer Partition wird deren Speicher über das angegebene Verzeichnis (bekannt als **Mount-Point**) verfügbar.

Wenn zum Beispiel die Partition `/dev/hda5` in `/usr` eingebunden (gemountet) wird, bedeutet das, dass alle Dateien und Verzeichnisse unter `/usr` physikalisch in `/dev/hda5` abgelegt sind. So wäre die Datei `/usr/share/doc/FAQ/txt/Linux-FAQ` in `/dev/hda5` gespeichert, nicht jedoch die Datei `/etc/X11/gdm/Sessions/Gnome`.

Setzen wir das Beispiel fort: Es wäre auch möglich, dass ein oder mehrere Verzeichnisse unter `/usr` Mount-Points für andere Partitionen sind. Beispielsweise könnte eine Partition (z.B. `/dev/hda7`) in `/usr/local` eingebunden werden. Das bedeutet, dass z.B. `/usr/local/man/whatis` dann in `/dev/hda7` zu finden wäre und nicht in `/dev/hda5`.

B.1.8 Anzahl der Partitionen

An dieser Stelle der Vorbereitungen für die Installation von Red Hat Linux sollten Sie einige Überlegungen zu Anzahl und Größe der Partitionen für Ihr neues Betriebssystem anstellen. Über die Frage nach der "richtigen Anzahl der Partitionen" wird in der Linux-Gemeinschaft heftig gestritten, und ohne dass ein Ende dieser Auseinandersetzung abzusehen wäre, kann mit Sicherheit behauptet werden, dass es sicherlich genauso viele Partitionsaufteilungen gibt wie Beiträge zu diesem Thema.

Vor diesem Hintergrund empfiehlt es sich, sofern kein Grund für eine andere Vorgehensweise vorliegt, die folgenden Partitionen zu erstellen:

- Eine Swap-Partition — Swap-Partitionen dienen zur Unterstützung von virtuellem Speicher. Mit anderen Worten: Daten werden in den Swap-Speicher geschrieben, wenn der RAM-Speicher für die von Ihrem System verarbeiteten Daten nicht ausreicht. Wenn Ihr Computer mit 16 MB RAM oder weniger ausgestattet ist, *müssen* Sie eine Swap-Partition erstellen. Auch wenn Sie mehr Speicher zur Verfügung haben, empfiehlt sich eine Swap-Partition. Die Mindestgröße der Swap-Partition sollte der Größe des RAMs oder 16 MB entsprechen (je nachdem, was größer ist).
- Eine `/boot`-Partition — Die Partition, die in `/boot` gemountet ist, enthält den Betriebssystem-Kernel (der den Start von Red Hat Linux ermöglicht) und einige andere Dateien, die während des Bootens benötigt werden. Wegen der Einschränkungen der meisten PC-BIOS-Versionen sollten Sie zur Aufnahme dieser Dateien nur eine kleine Partition erstellen. Sie sollte nicht größer als 16 MB sein.

Bitte beachten

Lesen Sie bitte Abschnitt B.1.9, *Verwenden von LILO* — Die dort angegebenen Informationen gelten für die `/boot`-Partition.

- Eine Root-Partition (/) — In der Root-Partition befindet sich `/` (das Root-Verzeichnis). In dieser Partitionsaufteilung befinden sich bis auf die Dateien, die in `/boot` gespeichert sind, alle Dateien in der Root-Partition. Deshalb sollten Sie die Root-Partition so groß wie möglich ansetzen. Eine Root-Partition von 900 MB erlaubt den Umfang einer Workstation-Installation (mit *sehr* wenig freiem Festplattenspeicher), während Sie in einer Root-Partition von 1,7 GB alle Pakete installieren können.

B.1.9 Verwenden von LILO

LILO (der LInux LOader) ist die am häufigsten eingesetzte Methode zum Starten von Red Hat Linux auf Intel-basierten Systemen. Als Betriebssystemloader arbeitet LILO "außerhalb" von Betriebssystemen und verwendet nur das in den Computer integrierte elementare E/A-System (Basic Input/Output System, BIOS). Dieser Abschnitt beschreibt die Interaktionen zwischen LILO und dem PC-BIOS und gilt nur für Intel-basierte Computer.

BIOS-Einschränkungen, die sich auf LILO auswirken

LILO ist einigen Einschränkungen unterworfen, die durch das BIOS der meisten Intel-basierten Computern auferlegt werden. Für die meisten BIOS-Versionen ist vor allem der Zugriff auf mehr als zwei Festplatten sowie auf Daten, die auf Festplattenbereichen oberhalb von Zylinder 1023 gespeichert sind, nicht möglich. Beachten Sie, dass einige neuere BIOS-Versionen diese Einschränkung nicht mehr kennen, aber das ist leider noch die Ausnahme.

Alle Daten, auf die LILO während des Systemstarts zugreifen muss (einschließlich Linux-Kernel), befinden sich im Verzeichnis `/boot`. Wenn Sie die oben empfohlene Partitionsaufteilung vornehmen oder wenn Sie eine Workstation- oder Server-Installation durchführen, befindet sich das `/boot`-Verzeichnis in einer kleinen separaten

Partition. Andernfalls ist es in der Root-Partition angeordnet. Wenn Sie Ihr Red Hat Linux System mit LILO starten möchten, muss die Partition, in der sich `/boot` befindet, in beiden Fällen den folgenden Richtlinien entsprechen:

Auf einem der beiden ersten IDE-Laufwerke

Wenn Sie 2 IDE- (oder EIDE)-Laufwerke haben, muss `/boot` auf einem dieser Laufwerke vorhanden sein. Beachten Sie, dass diese Einschränkung auch alle IDE-CD-ROM-Laufwerke, die am primären IDE-Controller angeschlossen sind, einschließt. Wenn Ihr Computer also über eine IDE-Festplatte und ein IDE-CD-ROM-Laufwerk am primären Controller verfügt, *muss* sich `/boot` auf der ersten Festplatte befinden, selbst wenn am zweiten IDE-Controller weitere Festplatten angeschlossen sind.

Auf dem ersten IDE- oder SCSI-Laufwerk

Wenn Sie ein IDE- (oder EIDE)-Laufwerk und ein oder mehrere SCSI-Laufwerke haben, muss `/boot` entweder auf dem IDE-Laufwerk oder dem SCSI-Laufwerk mit der ID 0 liegen. Ein Laufwerk mit anderer SCSI-ID ist nicht zulässig.

Auf den ersten beiden SCSI-Laufwerken

Wenn Sie nur SCSI-Festplatten haben, muss `/boot` auf einem Laufwerk mit der ID 0 oder ID 1 liegen. Ein Laufwerk mit anderer SCSI-ID ist nicht zulässig.

Partition *vollständig* unterhalb Zylinder 1023

Unabhängig von den oben genannten Konfigurationen muss die Partition, die `/boot` enthält, vollständig unterhalb von Zylinder 1023 liegen. Wenn die Partition mit `/boot` teils unter, teils über Zylinder 1023 liegt, kann es vorkommen, dass LILO anfänglich funktioniert (da alle wichtigen Informationen unterhalb Zylinder 1023 liegen), bis ein neuer Kernel geladen werden muss, der sich oberhalb dieses Zylinders befindet.

Wie bereits zuvor erwähnt wurde, erlauben einige der neueren BIOS-Versionen LILO den Betrieb mit Konfigurationen, die nicht unseren Richtlinien entsprechen. Ähnlich können auch ausgefallenere Funktionsmerkmale von LILO dazu verwendet werden, ein Linux-System zum Laufen zu bringen, selbst wenn die Konfiguration nicht unseren Richtlinien entspricht. Wegen der Vielzahl der damit verbundenen Unbekannten kann Red Hat solche außergewöhnlichen Systeme nicht unterstützen.

Bitte beachten

Das Partitionierungstool Disk Druid sowie die Workstation- und Server-Installation berücksichtigen diese BIOS-bedingten Einschränkungen.

C Treiberdisketten

C.1 Wozu werden Treiberdisketten benötigt?

Während das Red Hat Linux Installationsprogramm geladen wird, werden Sie möglicherweise in einem Bildschirm nach einer Treiberdiskette gefragt. Die Treiberdiskette wird am häufigsten in drei Szenarien benötigt:

- Wenn Sie das Installationsprogramm im `Expertenmodus` ausführen.
- Wenn Sie das Installationsprogramm durch Eingeben von `linux dd` am `boot:`-Prompt ausführen.
- Wenn Sie das Installationsprogramm auf einem Computer ausführen, der keine PCI-Geräte enthält.

C.1.1 Was ist eine Treiberdiskette?

Durch eine Treiberdiskette kann Unterstützung für Hardware hinzugefügt werden, die nicht vom Installationsprogramm unterstützt wird. Die Treiberdiskette kann von Red Hat oder von Ihnen erstellt worden sein oder von einem Hardware-Händler mit einem Gerät mitgeliefert werden.

Eine Treiberdiskette wird nur dann benötigt, wenn Sie für die Installation von Red Hat Linux ein spezielles Gerät benötigen. Im Allgemeinen wird es sich dabei um Treiberdisketten für SCSI-Adapter und Netzwerkkarten handeln, da dies die einzigen Geräte bei der Installation sind, für die möglicherweise eine Treiberdiskette benötigt wird. Wenn für die Installation von Red Hat Linux kein nichtunterstütztes Gerät benötigt wird, fahren Sie mit der normalen Installation fort, und fügen Sie die Unterstützung für das neue Gerät im Anschluss an die Installation hinzu.

C.1.2 Wie sind Treiberdisketten erhältlich?

Informationen zu Treiberdisketten finden Sie auf der Red Hat Website unter http://www.redhat.com/support/errata/ im Abschnitt **Bug Fixes**.

Erstellen Sie eine Bootdiskette unter Verwendung der jeweiligen Datei mit der allgemeinen Bezeichnung *`Dateiname`*`.img`, wenn Sie eine Treiberdiskette gefunden haben, die den Anforderungen Ihrer Geräte entspricht. Hinweise zum Erstellen einer Bootdiskette finden Sie im *Offiziellen Red Hat Linux Installationshandbuch* im Abschnitt *Erstellen von Installationsdisketten*.

Sobald Sie Ihre Treiberdiskette erstellt haben, müssen Sie das System booten. Verwenden Sie Ihre Diskette hierzu als Bootdiskette und geben Sie entweder `linux expert` oder `linux dd` am `boot:`-Prompt ein.

Bitte beachten

Einige der Treiberdisketten-Images sind auch im Verzeichnis mit Images Ihrer Red Hat Linux CD zu finden.

D Einrichten eines Dual-Boot-Systems

Dieses Dokument beschreibt, wie Sie Red Hat Linux auf einem Computer installieren können, auf dem bereits ein anderes Betriebssystem installiert ist. Außerdem beschreibt es die Einrichtung einer Dual-Boot-Umgebung.

D.1 Wenn auf Ihrem Computer bereits ein Betriebssystem installiert ist ...

Wenn auf dem Computer, auf dem Sie Red Hat Linux installieren wollen, bereits Windows oder ein anderes Betriebssystem installiert ist, müssen Sie eine wichtige Entscheidung treffen. Sie haben folgende Möglichkeiten:

- Sie möchten Red Hat Linux installieren, scheuen jedoch das Partitionieren der Festplatte? Sie haben die Möglichkeit, Red Hat Linux auf Ihrem System zu installieren, ohne Linux-Partitionen zu erstellen. In diesem Fall führen Sie einfach eine **partitionslose** Installation aus. Das Installationsprogramm kann Red Hat Linux auf einer vorhandenen formatierten Windows-Partition installieren. Lediglich die Erstellung einer Boot-Diskette ist erforderlich, um Red Hat Linux auf Ihrem System zu booten.

  Diese Methode ist sehr gut geeignet, wenn Sie Red Hat Linux nicht als primäres Betriebssystem oder als Dual-Boot-Betriebssystem installieren wollen. Auf diese Weise können Sie Red Hat Linux ausprobieren, ohne auf Ihrem System Linux-Partitionen einrichten zu müssen.

  Wenn Sie sich für diese Installationsart entscheiden, finden Sie die entsprechende Anleitung im *Offiziellen Red Hat Linux Installationshandbuch*, *Anhang B. Installation ohne Partitionieren*.

- Sie möchten Red Hat Linux installieren und die Möglichkeit haben, entweder Red Hat Linux oder Ihr anderes Betriebssystem zu starten? Bei einer Workstation- bzw. benutzerdefinierten Installation wird Red Hat Linux auf Ihrem System installiert, ohne dass das andere Betriebssystem davon beeinflusst wird. Bei einer Workstation-Installation ist das die Standardvorgabe. Bei einer benutzerdefinierten Installation müssen Sie LILO (LInux LOader) im MBR (Master Boot Record) installieren - es sei denn, Ihr zweites Betriebssystem ist Windows NT oder Sie verwenden bereits einen anderen Bootloader. Informationen zur Installation und Konfiguration von LILO finden Sie im *Offiziellen Red Hat Linux Installationshandbuch*. Im Anschluss an die Installation müssen Sie bei jedem Systemstart angeben, ob Sie Red Hat Linux oder das andere Betriebssystem starten wollen.

WARNUNG

Wenn das zweite Betriebssystem auf der Festplatte Windows NT ist, dürfen Sie keine Workstation-Installation durchführen, da Windows NT sonst nicht mehr gestartet werden kann. LILO überschreibt den Bootloader von NT. Das Starten von Windows NT wäre anschließend nicht mehr möglich. Sie müssen eine benutzerdefinierte Installation durchführen und LILO so konfigurieren, dass dieser nicht im MBR installiert wird.

Bei der Einrichtung einer Dual-Boot-Umgebung auf einem System, auf dem NT installiert ist, müssen Sie LILO statt im MBR im ersten Sektor der Root-Partition installieren. Sie müssen in diesem Fall unbedingt eine Bootdiskette erstellen. In diesem Fall müssen Sie zum Starten von Linux entweder eine Bootdiskette verwenden oder den Loader von Windows NT so konfigurieren, dass LILO vom ersten Sektor der Root-Partition gestartet wird. Weitere Informationen zum Einrichten von LILO und NT finden Sie unter http://www.linuxdoc.org/HOWTO/mini/Linux+NT-Loader.html. Bitte lesen Sie sich diese Informationen sorgfältig durch.

Wenn Sie sich für diese Installationsart entscheiden, finden Sie weitere Informationen unter Abschnitt D.2, *Einrichten einer Dual-Boot-Umgebung*

- Sie möchten Red Hat Linux als einziges Betriebssystem auf Ihrem Computer installieren? Das Installationsprogramm von Red Hat Linux löscht die anderen Betriebssysteme und alle Daten, die mit diesen Betriebssystemen erstellt wurden.

Bitte beachten

Die Installation von Red Hat Linux bei gleichzeitigem Beibehalten eines weiteren Betriebssystems erfordert genügend Platz für Red Hat Linux auf der Festplatte. Andernfalls werden das aktuelle Betriebssystem und vorhandene Dateien von Red Hat Linux überschrieben. Wenn Sie Ihre Festplatte nicht so partitioniert haben, dass genügend Speicherplatz für Red Hat Linux vorhanden ist oder nicht genügend unpartitionierten Speicherplatz für Ihre Installation frei gehalten haben, wird Red Hat Linux standardmäßig über die vorhandenen Daten installiert. Dasselbe gilt für eine Server-Installation. (Beachten Sie, dass bei einer Serverinstallation das X Window System nicht installiert wird und somit keine grafische Benutzeroberfläche vorhanden ist [1]). Eine Dual-Boot-Umgebung kann daher bei dieser Installationsart nicht eingerichtet werden.

Wenn Sie sich für diese Installationsart entscheiden, sollten Sie zuerst alle wichtigen Daten auf Ihrem Computer sichern (oder eine vollständige Sicherung aller Daten durchführen, wenn Sie eventuell die ursprüngliche Konfiguration Ihres Systems wiederherstellen möchten). Fahren Sie dann mit der Installation fort, wie im *Offiziellen Red Hat Linux Installationshandbuch* beschrieben.

1 Eine Server-Installation ist am besten geeignet, wenn Ihr System als Linux-basierter Server verwendet werden soll, ohne dass Sie sich im Detail mit der Systemkonfiguration befassen möchten.

D.2 Einrichten einer Dual-Boot-Umgebung

Die Installation von zwei Betriebssystemen auf einem Computer erfordert eine Dual-Boot-Umgebung. Sie können immer nur mit einem der beiden Betriebssysteme arbeiten, nicht mit beiden gleichzeitig. Jedes Betriebssystem bootet von seinen eigenen Festplatten bzw. Festplattenpartitionen (eine Partition ist ein physikalischer Abschnitt auf einer Festplatte).

Im Folgenden wollen wir davon ausgehen, dass das andere Betriebssystem Windows ist. Die allgemeinen Abläufe sind allerdings bei anderen Betriebssystemen ähnlich.

Bitte beachten

Wenn Red Hat Linux gemeinsam mit OS/2 auf Ihrem System installiert werden soll, müssen Sie die Festplattenpartitionen mit der Partitionssoftware von OS/2 erstellen - andernfalls kann OS/2 möglicherweise die Festplattenpartitionen nicht erkennen. Während der Installation dürfen keine neuen Partitionen erstellt werden. Die richtigen Partitionstypen für Ihre Linux-Partition werden jedoch während der Installation mit `fdisk` eingestellt.

Bevor Sie das Installationsprogramm starten, müssen Sie zuerst Platz für Red Hat Linux schaffen. Sie haben folgende Möglichkeiten:

- Hinzufügen einer neuen Festplatte
- Verwenden einer vorhandenen Festplatte oder Partition
- Erstellen einer neuen Partition

D.2.1 Hinzufügen einer neuen Festplatte

Am einfachsten kann Platz für Red Hat Linux durch Hinzufügen einer neuen Festplatte geschaffen werden. Anschließend wird Red Hat Linux auf diesem Laufwerk installiert. Wenn Sie zum Beispiel eine zweite IDE-Festplatte hinzufügen, erkennt das Installationsprogramm von Red Hat Linux die zweite Festplatte als `hdb` und die vorhandene Festplatte (mit installiertem Windows) als `hda`. (Bei SCSI-Festplatten würde die neu installierte Festplatte als `sdb` und die andere Festplatte als `sda`erkannt werden.)

Wenn Sie sich für den Einbau einer neuen Festplatte für Linux entscheiden, brauchen Sie nicht weiterzulesen. Sie müssen nach dem Start des Installationsprogramms von Red Hat Linux nur angeben, dass Linux auf der neu eingebauten Festplatte (`hdb`, `sdb`) installiert werden soll, und nicht auf der von Windows genutzten Festplatte.

D.2.2 Verwenden einer vorhandenen Festplatte oder Partition

Die zweiteinfachste Möglichkeit, für Linux Platz zu schaffen, ist die Verwendung einer Festplatte oder Festplattenpartition, die zurzeit von Windows verwendet wird. Angenommen, im Windows-Explorer werden zwei Festplatten angezeigt, `C:` und `D:`. Das kann bedeuten, dass im Computer entweder zwei Festplatten eingebaut sind oder eine Festplatte in zwei Partitionen aufgeteilt ist. In beiden Fällen (vorausgesetzt, die Größe reicht aus) können Sie Red Hat Linux auf der Festplatte oder der Festplattenpartition installieren, die von Windows als `D:` erkannt wird.

Diese Installationsart wird nur angezeigt, wenn der Computer über mindestens zwei Festplatten oder Festplattenpartitionen verfügt.

Bitte beachten

Windows verwendet sowohl für austauschbare Datenträger (z.B. ein ZIP-Laufwerk) und Netzlaufwerke (virtuelle Laufwerke) als auch für lokalen Festplattenspeicher Buchstaben. Linux kann jedoch nicht auf Wechsel- oder Netzwerklaufwerken installiert werden.

Wenn eine lokale Windows-Partition zur Verfügung steht, in der Linux installiert werden soll, brauchen Sie nicht weiterzulesen. Führen Sie die folgenden Schritte aus:

1. Kopieren Sie alle zu sichernden Daten von der ausgewählten Festplatte oder Partition (in diesem Beispiel `D:`) auf ein anderes Laufwerk bzw. eine andere Partition.
2. Starten Sie das Installationsprogramm von Red Hat Linux, und geben Sie das Laufwerk oder die Partition für die Linux-Installation an - in diesem Beispiel die Festplatte oder die Partition, die von Windows als `D:` bezeichnet wird. Beachten Sie, dass Linux zwischen Festplatten und Festplattenpartitionen unterscheidet. Folglich:
   - Wenn sich `C:` und `D:` auf zwei verschiedene Festplatten beziehen, werden diese vom Installationsprogramm als `hda` und `hdb` (IDE) bzw. `sda` und `sdb` (SCSI) erkannt. Geben Sie an, dass `hdb` bzw. `sdb` verwendet werden soll.
   - Wenn sich `C:` und `D:` auf Partitionen auf einer einzige Festplatte beziehen, werden diese vom Installationsprogramm als `hda1` und `hda2` (bzw. `sda1` und `sda2`) erkannt. Während der Partitionierungsphase der Linux-Installation löschen Sie die zweite Partition (`hda2` bzw. `sda2`) und partitionieren dann den nicht zugewiesenen freien Speicherplatz für Linux. (Die zweite Partition muss nicht vor der Linux-Partitionierung gelöscht werden. Wenn sie jedoch nicht gelöscht wird, gibt Windows bei jedem Systemstart eine Fehlermeldung aus, dass von `Laufwerk D` nicht gelesen werden kann. Außerdem würde beim versehentlichen Formatieren von Laufwerk `D` Ihr Linux-System zerstört werden.)

D.2.3 Erstellen einer neuen Partition

Die dritte Möglichkeit, Platz für Linux zu schaffen, ist die Erstellung einer neuen Partition für Red Hat Linux auf der Festplatte, die von dem anderen Betriebssystem verwendet wird. Wenn vom Windows-Explorer nur eine Festplatte angezeigt wird (`C:`), und keine neue Festplatte eingebaut werden soll, müssen Sie die vorhandene Festplatte partitionieren. Nach dem Partitionieren zeigt der Windows-Explorer weniger Speicherplatz für das Laufwerk `C:` an. Der Rest der Festplatte wird vom Red Hat Linux Installationsprogramm für Linux partitioniert.

Sie können zum Unterteilen der Festplatte ein Partitionierungsprogramm verwenden, das die vorhandenen Daten löscht, z.B. fdisk. Dann muss allerdings Windows neu installiert werden (und somit ist das wahrscheinlich nicht die beste Lösung...).

Für das Betriebssystem Windows wird von Drittanbietern eine Reihe von Partitionierungsprogrammen angeboten, die bei der Partitionierung keine Daten löschen. Wenn Sie sich für eines dieser Programme entscheiden, sollten Sie die entsprechende Dokumentation lesen.

Informationen zum Partitionieren mit FIPS (auf der Red Hat Linux CD-ROM enthalten) finden Sie in Abschnitt D.3, *Partitionieren mit* FIPS.

D.3 Partitionieren mit FIPS

Um unseren Kunden die Arbeit zu erleichtern, wird von uns das Dienstprogramm FIPS mitgeliefert. Dieses frei verfügbare Programm kann die Größe von FAT (File Allocation Table)-Partitionen ändern. Sie finden es auf der Red Hat Linux CD-ROM im Verzeichnis `dosutils`.

Bitte beachten

Viele haben FIPS bereits erfolgreich zum Neupartitionieren von Festplatten verwendet. Aufgrund der Komplexität der von FIPS vorgenommenen Aktionen und der großen Vielfalt der Hardware- und Softwarekonfigurationen, unter denen das Programm ausgeführt wird, kann Red Hat jedoch nicht garantieren, dass FIPS auf Ihrem System einwandfrei funktioniert. Deshalb ist für FIPS keinerlei Installations-Support verfügbar. Sie benutzen das Programm auf eigenes Risiko.

Wenn Sie sich trotzdem entschließen, Ihre Festplatte mit FIPS neu zu partitionieren, müssen Sie unbedingt zwei Dinge beachten:

- `Erstellen Sie ein Backup` - Erstellen Sie zwei Kopien von allen wichtigen Daten auf Ihrem Computer. Diese Kopien sollten auf Wechseldatenträgern (z.B. Band oder Disketten) gespeichert werden. Überprüfen Sie, ob die Datenträger lesbar sind, bevor Sie fortfahren.

- `Lesen Sie die Dokumentation` - Lesen Sie die gesamte Dokumentation zu FIPS. Sie finden sie im Verzeichnis FIPS auf der Red Hat Linux CD-ROM.

Beachten Sie, dass bei der Verwendung von FIPS nach dem Ausführen von FIPS zwei Partitionen existieren: eine verkleinerte Partition und eine mit FIPS aus dem neu zugeteilten Speicherplatz erstellte Partition. Wenn Sie diesen Speicherplatz zur Installation von Red Hat Linux nutzen wollen, müssen Sie die neu erstellte Partition entweder mit fdisk unter Ihrem aktuellen Betriebssystem oder beim Einrichten der Partitionen während der benutzerdefinierten Installation löschen.

Die folgenden Anweisungen sind eine vereinfachte Version der FIPS-Dokumentationsdatei (`fips.doc`), die Sie im FIPS-Verzeichnis (`/dosutils/fips20/*`) finden können. Diese Anweisungen sollten für die meisten Anwendungsfälle Gültigkeit haben. Wenn Sie Probleme haben, finden Sie entsprechende Informationen in der Dokumentationsdatei.

1. In Windows:
   - Führen Sie eine vollständige Datensicherung durch.
   - Führen Sie scandisk aus, um die Festplatte auf fehlerhafte Cluster zu überprüfen.
   - Entscheiden Sie, wie Sie den auf der Festplatte verfügbaren Speicherplatz auf die Betriebssysteme aufteilen wollen. Bestimmen Sie mit dem Windows-Explorer den freien Speicherplatz auf der Festplatte. Notieren Sie den Speicherplatz (in Megabyte), der jedem Betriebssystem zugeteilt werden soll.
   - Erstellen Sie eine DOS-Bootdiskette, falls Sie noch keine haben.

     Starten Sie dazu Ihren Rechner unter DOS.

     Legen Sie dann eine leere, formatierte Diskette in das Diskettenlaufwerk ein.

     Geben Sie auf der Befehlszeile den folgenden Befehl ein, und drücken Sie die [Eingabetaste]:

     ```
     FORMAT A: /S
     ```

Unter Windows 95 legen Sie zuerst eine leere, formatierte Diskette in das Diskettenlaufwerk ein. Klicken Sie dann auf **Start**/**Ausführen**, und geben Sie Folgendes ein:

```
FORMAT A: /S
```

Die Diskette wird formatiert, und die Datei `COMMAND.COM` wird zusammen mit den verknüpften zugehörigen Dateien (`IO.SYS`, `MSDOS.SYS` und `BDLSAPCE.BIN`) auf die Diskette kopiert.

- Kopieren Sie die folgenden Dateien von der Red Hat Linux CD-ROM auf die DOS-Bootdiskette.

```
/mnt/cdrom/dosutils/fips20/fips.exe
/mnt/cdrom/dosutils/fips20/restorrb.exe
/mnt/cdrom/dosutils/fips20/errors.txt
/mnt/cdrom/dosutils/fips20/fips.doc
/mnt/cdrom/dosutils/fips20/fips.faq
```

- Defragmentieren Sie die Festplatte.

2. Legen Sie die DOS-Bootdiskette in das Diskettenlaufwerk, und starten Sie das System neu.
3. Starten Sie FIPS (geben Sie am Prompt `fips` ein).

   Nach dem Start von FIPS wird ein Begrüßungsbildschirm ähnlich dem Folgenden angezeigt:

Abbildung D–1 FIPS-Begrüßungsbildschirm

```
FIPS version 2.0, Copyright (C) 1993/4 Arno Schaefer
FAT32 Support, Copyright (C) 1997 Gordon Chaffee

DO NOT use FIPS in a multitasking environment like Windows, OS/2, Desqview,
Novell Task manager or the Linux DOS emulator; boot from a DOS boot disk first.

If you use OS/2 or a disk compressor, read the relevant sections in FIPS.DOC.
```

```
FIPS comes with ABSOLUTELY NO WARRANTY, see file COPYING for details.

This is free software, and you are welcome to redistribute it
under certain conditions; again, see file COPYING for details.

Press any key.
```

Nachdem Sie eine Taste gedrückt haben, wird ein Root-Partitionsbildschirm ähnlich dem Folgenden geöffnet. (Beachten Sie, dass Sie auswählen müssen, welche Festplatte partitioniert werden soll, wenn der Computer über mehrere Festplatten verfügt.)

Abbildung D–2 FIPS-Root-Partitionierungsbildschirm

```
Partition table:
     |        |     Start      |      |      End       | Start  |Number of|
Part.|bootable|Head Cyl. Sector|System|Head Cyl. Sector| Sector |Sectors  |  MB
-----+--------+----------------+------+----------------+--------+---------+----
1    |    yes |   0  148      1|   83h|  15  295     63|  149184|   149184|  72
2    |     no |   1    0      1|   06h|  15  139     63|      63|   141057|  68
3    |     no |   0  140      1|   06h|  15  147     63|  141120|     8064|   3
4    |     no |   0    0      0|   00h|   0    0      0|       0|        0|   0

Checking root sector ... OK

Press any key.
```

Nachdem Sie eine Taste gedrückt haben, werden Details über die Festplatte wie die folgenden Informationen angezeigt.

Abbildung D–3 FIPS-Bootsektorbildschirm

```
Boot sector:
Bytes per sector: 512
Sectors per cluster: 8
Reserved sectors: 1
Number of FATs: 2
Number of rootdirectory entries: 512
Number of sectors (short): 0
Media descriptor byte: f8h
Sectors per FAT: 145
Sectors per track: 63
```

```
Drive heads: 16
Hidden sectors: 63
Number of sectors (long): 141057
Physical drive number: 80h
Signature: 29h

Checking boot sector ... OK
Checking FAT ... OK
Searching for free space ... OK

Do you want to make a backup copy of your root and boot sector before
proceeding? (y/n)
```

Geben Sie **y** für `yes (ja)` ein, um eine Sicherungskopie von Ihrem Root- und Bootsektor anfertigen zu lassen, bevor Sie in FIPS fortfahren.

Als Nächstes wird folgende Meldung angezeigt:

```
Do you have a bootable floppy disk in drive A: as described in the
documentation? (y/n)
```

Überprüfen Sie, ob eine DOS-Bootdiskette im Diskettenlaufwerk eingelegt ist, und geben Sie **y** für `yes (ja)` ein. Ein Bildschirm ähnlich dem Folgenden wird angezeigt. Hier können Sie die Größe der Partition ändern.

Abbildung D–4 Bildschirm zur Änderung der Partitionsgröße

```
Writing file a:\rootboot:000

Enter start cylinder for new partition (33-526)

Use the cursor keys to choose the cylinder, <enter> to continue

Old partition           Cylinder             New partition
 258.9 MB                  33                  3835.8 MB
```

Durch die vorgegebenen Anfangswerte wird der neuen Partition der *gesamte* freie Speicherplatz zugewiesen. Diese Einstellung muss geändert werden, denn so würde kein freier Speicherplatz auf Ihrer Windows-Partition verbleiben. Drücken Sie die [Nach-rechts-Taste], um die Größe der Windows-Partition zu erhöhen und die Größe der neuen (Linux-) Partition zu verringern. Drücken Sie die

[Nach-links-Taste], um die Größe der Windows-Partition zu verringern und die Größe der Linux-Partition zu erhöhen. Drücken Sie die [Eingabetaste], wenn die richtige Größe eingestellt ist. Ein Kontrollbildschirm ähnlich dem Folgenden wird angezeigt:

Abbildung D–5 FIPS-Kontrollbildschirm

```
First Cluster: 17442
Last Cluster: 65511

Testing if empty ... OK

New partition table:

     |        |     Start       |      |      End        | Start  |Number of|
Part.|bootable|Head Cyl. Sector|System|Head Cyl. Sector| Sector |Sectors  | MB
-----+--------+----------------+------+----------------+--------+---------+---
1    |    yes |   0  148      1|   83h|  15  295     63|  149184|   149184| 1090
2    |     no |   0  139      1|   06h| 254  521     63| 2233035|  6152995| 3084
3    |     no |   0  140      1|   06h|  15  147     63|  141120|     8064|  3
4    |     no |   0    0      0|   00h|   0    0      0|       0|        0|  0

Checking root sector ... OK

Do you want to continue or reedit the partition table (c/r)?
```

Wenn Sie **r** eingeben (zum erneuten Ändern der Partitionstabellen), wird *Abbildung 4* angezeigt. Hier können Sie die Partitionsgrößen ändern. Wenn Sie **c** eingeben, wird ein Bestätigungsbildschirm (*Abbildung 6*) angezeigt:

Abbildung D–6 FIPS-Bestätigungsbildschirm

```
New boot sector:

Boot sector:
Bytes per sector: 512
Sectors per cluster: 8
Reserved sectors: 1
Number of FATs: 2
Number of rootdirectory entries: 512
Number of sectors (short): 0
Media descriptor byte: f8h
```

```
Sectors per FAT: 145
Sectors per track: 63
Drive heads: 16
Hidden sectors: 63
Number of sectors (long): 141057
Physical drive number: 80h
Signature: 29h

Checking boot sector ... OK

Ready to write new partition scheme to disk
Do you want to proceed (y/n)?
```

Geben Sie **`y`** ein, um die Größenänderung abzuschließen. Möglicherweise erscheint eine harmlose Fehlermeldung, die im Prinzip anzeigt, dass FIPS das System nicht neu starten kann.

Nach der erfolgreichen Durchführung dieser Schritte ist die Festplatte in zwei Partitionen eingeteilt. Die erste Partition (`hda1` bzw. `sda1`) wird für Windows verwendet. Wir empfehlen, Windows zu starten (denken Sie daran, die Bootdiskette aus dem Laufwerk `A:` zu entfernen) und das Laufwerk `C:` mit scandisk zu überprüfen.

Wenn Probleme auftreten (z.B. Windows lässt sich nicht starten), können Sie die mit FIPS durchgeführte Größenänderung mit dem von Ihnen auf die DOS-Bootdiskette kopierten Programm restorrb.exe wieder rückgängig machen. Falls Fehler auftreten, finden Sie entsprechende Hinweise in den FIPS-Dokumentationsdateien (`fips.doc` und `fips.faq`). Dort sind zahlreiche Faktoren aufgeführt, die Probleme bei der Größenänderung verursachen können. Im schlimmsten Fall können Sie mit Hilfe der angefertigten Sicherungskopie Windows wiederherstellen.

Die zweite Partition (`hda2` bzw. `sda2`) umfasst den vom Red Hat Linux Installationsprogramm verwendeten Speicherplatz. Wenn während der Installation der Bildschirm von Disk Druid geöffnet wird, löschen Sie diese Partition (Vorgehensweise siehe Installationshandbuch), und fahren Sie dann mit der Linux-Partitionierung fort.

E Redundant Array of Independent Disks (RAID)

E.1 Was verbirgt sich hinter RAID?

Die grundlegende Idee hinter RAID (Redundant Array of Independent Disks) besteht darin, mehrere kleine, preiswerte Festplatten zu einer Festplattengruppe zu kombinieren und dadurch eine höhere Leistung zu erreichen als mit einer großen und teuren Festplatte. Diese Festplattengruppe wird durch den Computer wie eine einzige logische Speichereinheit oder Festplatte angesprochen.

Bei dieser Methode werden Daten auf mehrere Festplatten unter Verwendungen von Techniken wie **Disk Striping** (RAID Level 0) und **Disk Mirroring** (RAID Level 1) verteilt, um Redundanz, geringere Latenzzeit und/oder größere Bandbreite zum Lesen und/oder Schreiben sowie die Möglichkeit zur Wiederherstellung der Datei nach dem Ausfall einer Festplatte zu gewinnen.

Das grundlegende Konzept von RAID ist, dass Daten auf jedes Laufwerk innerhalb der Laufwerkgruppe auf einheitliche Art und Weise verteilt werden können. Dazu müssen die Daten zuerst in "Blöcke" einheitlicher Größe aufgeteilt werden (oft 32 oder 64 KB groß, andere Größen sind möglich). Jeder Block wird dann abwechselnd auf jedes Laufwerk geschrieben. Wenn die Daten gelesen werden sollen, wird der Prozess umgekehrt. Dadurch entsteht der Eindruck, dass mehrere Laufwerke ein großes Laufwerk sind.

E.1.1 Wer sollte RAID verwenden?

Wer mit großen Datenmengen umgeht (z.B. ein typischer Administrator), kann von der RAID-Technologie profitieren. Zu den Hauptgründen für die Verwendung von RAID gehören:

- Höhere Geschwindigkeit
- Größere Speicherkapazität (und wirtschaftlicher)
- Bessere Effizienz beim Wiederherstellen von Daten nach einem Plattenausfall

E.1.2 RAID: Hardware- oder Software-Lösung

Es gibt zwei mögliche Ansätze für RAID: Hardware-RAID und Software-RAID.

Hardware-RAID

Das Hardware-basierte System verwaltet das RAID-Teilsystem unabhängig vom Rechner und stellt für den Rechner nur eine einzige Festplatte pro RAID-Array dar.

Ein Beispiel für ein Hardware-RAID-Gerät wäre eine Einheit, die an einen SCSI-Controller angeschlossen ist und deren RAID-Array wie ein einziges SCSI-Laufwerk angesprochen wird. Ein externes RAID-System verlagert alle RAID-Steuerungsprozesse in einen Controller, der sich im externen Festplattenteilsystem befindet. Das ganze Teilsystem wird über einen normalen SCSI-Controller an den Rechner angeschlossen und erscheint für diesen als "ganz normale" Festplatte.

RAID-Controller werden auch in Form von Karten angeboten, die für das Betriebssystem wie ein SCSI-Controller *agieren*, jedoch die gesamte Kommunikation mit den RAID-Laufwerken übernehmen. In diesen Fällen werden die Laufwerke genauso an den RAID-Controller angeschlossen wie an einen SCSI-Controller. Danach werden sie in die Konfiguration des RAID-Controllers eingetragen, so dass das Betriebssystem den Unterschied zu herkömmlichen Laufwerken nicht mehr erkennt.

Software-RAID

Beim Software-RAID sind die verschiedenen RAID-Levels im Kernel-Disk-(Blockgeräte-) Code implementiert. Dieser Ansatz ist die preiswerteste Lösung: Es werden keine teuren Festplattencontroller oder Hot-Swap-Chassis benötigt [1], und Software-RAID funktioniert mit billigeren IDE-Festplatten ebenso wie mit SCSI-Festplatten. Mit den heutigen schnellen CPUs übertrifft die Leistung von Software-RAID-Systemen sogar die von Hardware-RAID-Systemen.

Der MD-Treiber im Linux-Kernel ist ein Beispiel für eine RAID-Lösung, die vollkommen hardwareunabhängig ist. Die Leistung eines Software-basierten Arrays ist sehr stark abhängig von Leistung und Auslastung der Server-CPU.

[1] Ein Hot-Swap-Chassis ermöglicht es, ein Festplattenlaufwerk zu entfernen, ohne das System ausschalten zu müssen.

E.1.3 Einige Funktionsmerkmale von RAID

Für alle, die sich für Software-RAID interessieren, geben wir hier eine kurze Liste einiger der Funktionsmerkmale an:

- Wiederherstellungs-Prozess mit Threads
- Vollständig Kernel-basierte Konfiguration
- Portabilität von Arrays zwischen Linux-Rechnern ohne Reorganisation
- Reorganisation von Arrays erfolgt im Hintergrund unter Verwendung ungenutzter Systemressourcen
- Unterstützung von Hotswap-fähigen Laufwerken
- Automatische CPU-Erkennung, um bestimmte CPU-Optimierungen voll auszunutzen

Levels und lineare Unterstützung

RAID bietet außerdem die Level 0, 1, 4, 5 und lineare Unterstützung. Diese RAID-Typen funktionieren folgendermaßen:

- *Level 0* - RAID Level 0, oftmals als "Striping" bezeichnet, ist eine leistungsorientierte Datenzuordnungstechnik. Das heißt, die in das Array zu schreibenden Daten werden zerlegt und auf die einzelnen Festplatten des Arrays verteilt. Dies ermöglicht eine hohe E/A-Leistung bei geringen zusätzlichen Kosten, bietet jedoch keine Redundanz. Die Speicherkapazität des Arrays entspricht der Gesamtkapazität aller Festplatten des Arrays.
- *Level 1* - RAID Level 1, oder "Mirroring", wird bereits länger als alle anderen RAID-Formen eingesetzt. Level 1 gewährleistet Redundanz, indem die gleichen Daten auf jede einzelne Festplatte des Arrays geschrieben werden, so dass auf jeder Festplatte eine "gespiegelte" Kopie vorliegt. Diese Vorgehensweise bleibt wegen ihrer Einfachheit und hohen Datenverfügbarkeit weiterhin populär. Sie funktioniert mit zwei oder mehreren Festplatten, die für hohe Datenübertragungsgeschwindigkeiten mit parallelem Zugriff lesen können, aber normalerweise für hohe E/A-Transaktionsraten unabhängig voneinander arbeiten. Level 1 bietet

sehr gute Datensicherheit und verbessert die Leistung für leseintensive Anwendungen, jedoch bei relativ hohen Kosten. [2]Wenn Sie identische Festplattenlaufwerke verwenden, dann entspricht die Kapazität des Arrays der Kapazität einer einzelnen Festplatte im Array.

- *Level 4* - Level 4 verwendet Prüfbits [3]die zum Datenschutz auf einer einzigen Festplatte konzentriert sind. Dieses Verfahren eignet sich eher für E/A-Vorgänge als für die Übertragung großer Dateien. Da die eigens für Prüfbits bestimmte Festplatte einen Engpass darstellt, wird Level 4 selten ohne unterstützende Techniken wie Write Back Caching verwendet. Obwohl RAID Level 4 für einige RAID-Partitionsvarianten verwendet werden kann, ist es für Red Hat Linux RAID-Installationen nicht zugelassen. [4]Die Kapazität des Arrays entspricht der Kapazität der Festplatten im Array minus der Kapazität einer Festplatte, falls Sie identische Festplattenlaufwerke verwenden.
- *Level 5* - Der am weitesten verbreitete RAID-Typ. Durch Verteilen der Prüfbits auf einige oder alle Array-Laufwerke wird der Schreibengpass von Level 4 eliminiert. Den einzigen Engpass bildet jetzt die Prüfsummenbildung, was jedoch mit modernen CPUs und Software-RAID kein nennenswertes Problem ist. Wie bei Level 4 ist das Ergebnis ein asymmetrisches Leistungsverhalten, wobei Lesevorgänge erheblich schneller ablaufen als Schreibvorgänge. Um diese Asymmetrie zu verringern, wird Level 5 häufig zusammen mit Write-back verwendet. Die Kapazität des Arrays entspricht der Kapazität der Festplatten im Array minus der Kapazität einer Festplatte, falls Sie identische Festplattenlaufwerke verwenden.
- *Lineares RAID* - Lineares RAID ist die einfache Zusammenschaltung von Festplatten, um so zu einer größeren virtuellen Festplatte zu gelangen. Beim linearen

[2] RAID Level 1 ist teuer, weil alle Informationen auf alle Festplatten des Arrays geschrieben werden. Dadurch wird Speicherplatz verschwendet. Wenn zum Beispiel RAID Level 1 so eingerichtet ist, dass die Root ("/")-Partition über zwei 4 GB-Festplattenlaufwerke verteilt ist, sind insgesamt 8 GB im Einsatz, wobei Sie aber nur auf 4 GB dieser 8 GB zugreifen können. Die anderen 4 GB werden als eine Art Spiegel der ersten 4 GB verwendet.

[3] Die Prüfbitinformationen werden auf der Grundlage des Inhalts der restlichen Festplatten des Arrays berechnet. Diese Informationen können dann für die Rekonstruktion von Daten verwendet werden, wenn eine Festplatte des Arrays ausfällt. Mit den rekonstruierten Daten können E/A-Anforderungen an die ausgefallene Festplatte beantwortet und die Festplatte nach der Reparatur oder dem Austausch neu beschrieben werden.

[4] RAID Level 4 benötigt etwa denselben Speicherplatz wie RAID Level 5. Level 5 bietet allerdings im Gegensatz zu Level 4 eine Vielzahl von Vorteilen. Aus diesem Grund wird Level 4 nicht unterstützt.

RAID werden die Blöcke jeweils auf die nächste Festplatte geschrieben, wenn die vorhergehende Festplatte voll ist. Diese Gruppierung bringt keinen Leistungsvorteil, da es unwahrscheinlich ist, dass E/A-Operationen zwischen verschiedenen Festplatten aufgeteilt werden. Lineares RAID bietet auch keine Redundanz und reduziert sogar die Zuverlässigkeit - wenn eine der Festplatten ausfällt, funktioniert das gesamte Array nicht mehr. Die Kapazität berechnet sich aus der Summe der Kapazitäten aller Festplatten.

E.1.4 Erstellen von RAID-Partitionen

RAID ist sowohl bei Verwendung der grafischen Oberfläche als auch im Kickstart-Installationsmodus verfügbar. Ihre RAID-Konfiguration können Sie mit fdisk oder Disk Druid erstellen. Diese Anleitung konzentriert sich jedoch hauptsächlich auf die Verwendung von Disk Druid für diese Aufgabe.

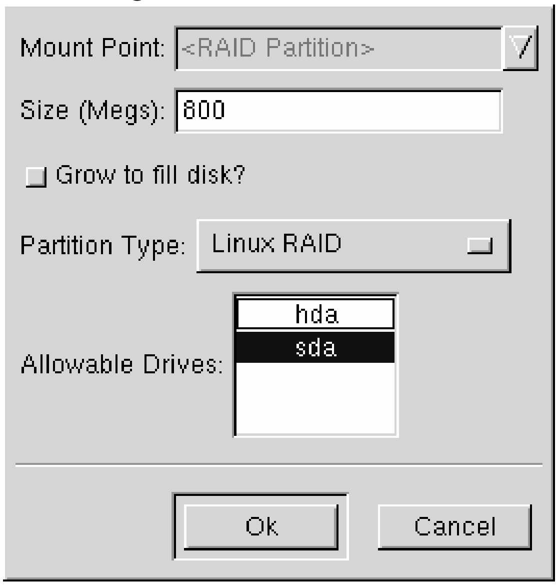
Bevor Sie ein RAID-Gerät erstellen können, müssen zuerst RAID-Partitionen erstellt werden. Gehen Sie dabei nach der folgenden Schritt-für-Schritt-Anweisung vor.

Tipp: Verwendung von fdisk

Wenn Sie fdisk zum Erstellen einer RAID-Partition verwenden, ist Folgendes zu beachten: Sie müssen statt einer Partition vom Typ `83` (= Linux Native) eine Partition vom Typ `fd` (Linux RAID) erstellen. Die beste Leistung erzielen Sie außerdem, wenn die Partitionen innerhalb eines festgelegten RAID-Arrays auf den Laufwerken identische Zylinder umfassen.

- Erstellen Sie eine Partition. In Disk Druid müssen Sie **Hinzufügen** wählen, um eine neue Partition zu erstellen (siehe Abbildung E–1, *Erstellen einer neuen RAID-Partition*).

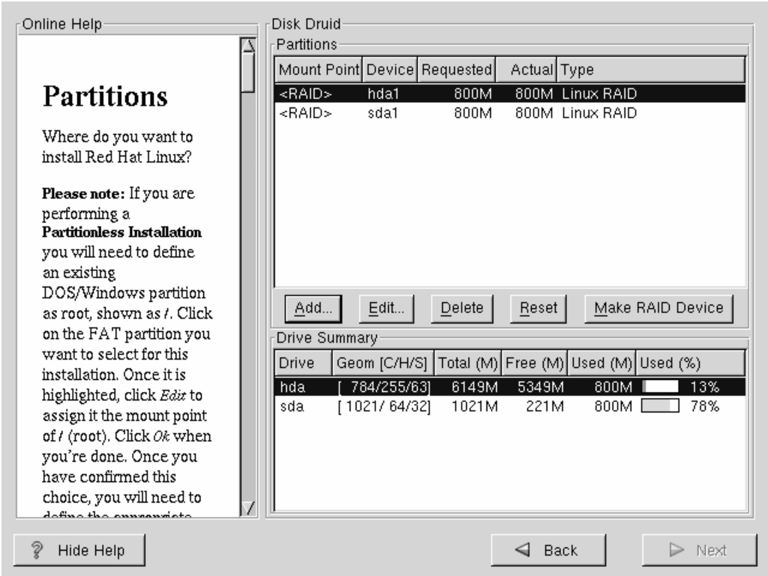
Abbildung E–1 Erstellen einer neuen RAID-Partition



- Sie können dabei noch keinen Mount-Point eingeben. (Das können Sie erst, wenn Sie Ihr RAID-Gerät erstellt haben.)
- Geben Sie die Größe der Partition ein.
- Aktivieren Sie das Kontrollkästchen **An Kapazität der Festplatte anpassen**, wenn Sie die Partition so anpassen wollen, dass sie die gesamte Festplatte einnimmt. Ihre Größe ist variabel und hängt davon ab, wie Sie die anderen Partitionen festlegen. Wenn Sie mehr als eine anpassbare Partition erstellen, dann werden die verschiedenen Partitionen um den verfügbaren freien Festplattenplatz konkurrieren.
- Geben Sie RAID als Partitionstyp an.
- Wählen Sie schließlich unter **Verfügbare Laufwerke** das RAID-Laufwerk aus. Wenn Sie über mehrere Laufwerke verfügen, werden hier alle Laufwerke aktiviert. Sie müssen diejenigen Laufwerke deaktivieren, auf denen *kein* RAID-Array erstellt werden soll.

Fahren Sie auf diese Weise fort, und erstellen Sie so viele Partitionen, wie für das RAID-Array benötigt werden.

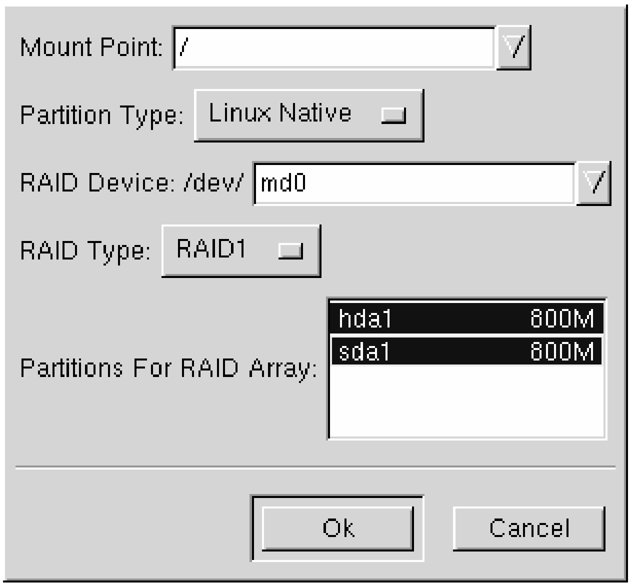
Abbildung E–2 RAID-Partitionen



Wenn Sie alle RAID-Partitionen erstellt haben, wählen Sie die Schaltfläche **RAID-Gerät erstellen** im Hauptpartitionierungsbildschirm von Disk Druid (siehe Abbildung E–2, *RAID-Partitionen*).

Dann erscheint Abbildung E–3, *Erstellen eines RAID-Gerätes*. Hier können Sie ein RAID-Gerät erstellen.

Abbildung E–3 Erstellen eines RAID-Gerätes



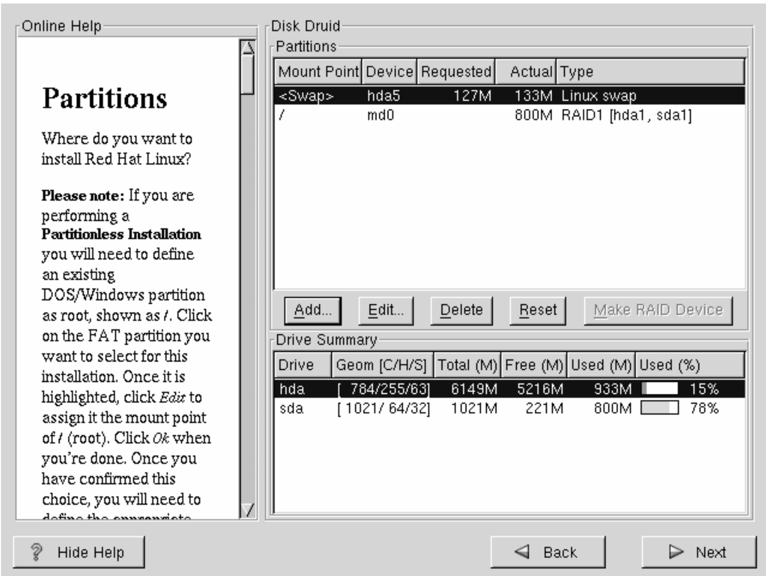
- Geben Sie zuerst einen Mount-Point an.
- Überprüfen Sie dann, ob der Partitionstyp auf **Linux Native** eingestellt ist (Standardvorgabe).
- Wählen Sie Ihr RAID-Gerät aus. Wählen Sie für das erste Gerät `md0`, für das zweite Gerät `md1` usw., es sei denn es liegt ein wichtiger Grund vor, andere Bezeichnungen für die Geräte auszuwählen. Für RAID-Geräte können die Bezeichnungen md0 bis md7 und jede nur einmal verwendet werden.
- Wählen Sie den RAID-Typ aus. Sie können zwischen **RAID 0**, **RAID 1** und **RAID 5** wählen.

Bitte beachten

Wenn Sie eine RAID-Partition von `/boot` erstellen, müssen Sie RAID Level 1 auswählen. Zudem muss eines der ersten beiden Laufwerke (IDE als erstes, SCSI als zweites) verwendet werden. Wenn Sie keine RAID-Partition von `/boot`, sondern von `/` erstellen, müssen Sie ebenfalls RAID Level 1 auswählen. Auch in diesem Fall muss eines der beiden ersten Laufwerke (IDE als erstes, SCSI als zweites) verwendet werden.

- Wählen Sie schließlich die Partitionen aus, die zum RAID-Array gehören sollen (siehe Abbildung E–4, *Erstellen eines RAID-Arrays*), und klicken Sie auf **Weiter**.

Abbildung E–4 Erstellen eines RAID-Arrays



- Ab hier können Sie mit dem Installationsprozess fortfahren. Weitere Informationen finden Sie im *Offiziellen Red Hat Linux Installationshandbuch*.

F Kickstart-Installationen

F.1 Was sind Kickstart-Installationen?

Da die Nachfrage nach automatisierten Installationen wächst, hat Red Hat die Installationsart "Kickstart" entwickelt. Der Systemadministrator kann dabei alle Informationen, die während einer typischen Installation von Red Hat Linux abgefragt werden, in einer einzigen Datei zusammenstellen.

Die Kickstart-Dateien werden auf einem einzelnen Server-System bereitgestellt und können von dort während der Installation von den einzelnen Computern gelesen werden. Diese Methode ist so leistungsfähig, dass oft eine einzige Kickstart-Datei genügt, um Red Hat Linux auf mehreren Maschinen zu installieren. Dadurch ist sie ideal für Netzwerk- und Systemadministratoren geeignet.

Kickstart ermöglicht die Automatisierung des größten Teils der Red Hat Linux-Installation. Dazu gehören:

- Auswählen der Sprache
- Netzwerk-Konfiguration
- Tastaturauswahl
- Bootloaderinstallation (LILO)
- Partitionieren der Festplatte
- Auswählen der Maus
- X Window Systemkonfiguration

F.2 So führen Sie Kickstart-Installationen durch

Kickstart-Installationen können mit Hilfe einer lokalen CD-ROM, eines lokalen Festplattenlaufwerks oder mit Hilfe von Installationsarten wie NFS, FTP oder HTTP durchgeführt werden.

Zunächst müssen Sie eine Kickstart-Datei (`ks.cfg`) erstellen und dem Red Hat Linux Installationsprogramm zugänglich machen.

F.2.1 Speicherort der Kickstart-Datei

Eine Kickstartdatei muss an einem der folgenden zwei Orte vorliegen:

- auf einer Bootdiskette
- auf einem Netzwerk

Normalerweise wird die Kickstart-Datei auf die Bootdiskette kopiert oder im Netzwerk bereitgestellt. Gewöhnlich wird die Verwendung des Netzwerks bevorzugt, da die meisten Kickstart-Installationen auf vernetzten Computern durchgeführt werden.

Im Folgenden wird genauer erläutert, wo die Kickstart-Datei gespeichert werden kann.

Bei einer diskettenbasierten Kickstart-Installation hat die Kickstart-Datei den Namen `ks.cfg` und befindet sich im Hauptverzeichnis der Bootdiskette. Beachten Sie, dass die Bootdisketten für Red Hat Linux im MS-DOS-Format vorliegen, was das Kopieren der Kickstart-Datei unter Linux mit dem Befehl `mcopy` vereinfacht:

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

(stattdessen können Sie auch Windows verwenden). Sie können auch die MS-DOS-Bootdiskette mounten und die Datei mit `cp` kopieren. Die meisten diskettenbasierten Kickstart-Installationen von Red Hat Linux werden von CD-ROM ausgeführt, auch wenn es keine technischen Gründe dafür gibt.

Netzwerkbasierte Kickstart-Installationen kommen recht häufig vor und sind empfehlenswerter als diskettenbasierte Installationen, weil sie Systemadministratoren in die Lage versetzen, die Installation auf mehreren miteinander vernetzten Computern schnell und einfach zu automatisieren. In der Regel hat der Systemadministrator im lokalen Netzwerk sowohl einen BOOTP/DHCP- als auch einen NFS-Server eingerichtet. Der BOOTP/DHCP-Server liefert dem Client-System die notwendigen Informationen zur Einrichtung der Netzwerk-Software, und der NFS-Server stellt die tatsächlich für die Installation benötigten Dateien bereit. Die beiden Serverprozesse werden oft auf derselben Maschine ausgeführt, was jedoch nicht unbedingt notwendig ist.

Um eine netzwerkbasierte Kickstart-Installation durchzuführen, benötigen Sie einen in Ihr Netzwerk eingebundenen BOOTP/DHCP-Server, der die Konfigurationsinformationen für den Rechner enthält, auf dem Red Hat Linux installiert werden soll. Der BOOTP/DHCP-Server liefert den Clients die Informationen für deren Netzwerkkonfiguration sowie den Speicherort der Kickstart-Datei.

Wenn der BOOTP/DHCP-Server eine Kickstart-Datei angibt, versucht das Client-System, den Pfad über NFS einzubinden, und kopiert die angegebene Datei auf das lokale System. Die genauen Einstellungen hängen vom verwendeten BOOTP/DHCP-Server ab.

Hier ein Beispiel für eine Zeile aus der Datei `dhcpd.conf` für den DHCP-Server, der mit Red Hat Linux geliefert wird:

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

Beachten Sie, dass die Zeile `filename` für den Namen der Kickstart-Datei (oder den Pfad zur Kickstart-Datei) zu verwenden ist und die Zeile `next-server` für den Namen des NFS-Servers.

Wenn der vom BOOTP/DHCP-Server ausgegebene Dateiname mit einem Schrägstrich ("/") endet, wird er lediglich als Pfad interpretiert. In diesem Fall bindet das Client-System den Pfad über NFS in das eigene Dateisystem ein und sucht nach einer Datei mit dem Namen:

```
<IP-Adresse>-kickstart
```

Der `<IP-Adresse>` -Teil des Dateinamens ist durch die IP-Adresse des Client zu ersetzen. Die IP-Adresse wird in durch Punkt getrennten Dezimalzahlen angegeben. Der Dateiname für einen Computer mit der IP-Adresse 10.10.0.1 würde beispielsweise `10.10.0.1-kickstart` lauten.

Wenn Sie keinen NFS-Server angeben, versucht das Client-System, den Server als NFS-Server zu verwenden, der auf die BOOTP/DHCP-Anfrage geantwortet hat.

Wenn Sie keinen Pfad oder Dateinamen angeben, wird das Client-System versuchen, `/kickstart` vom BOOTP/DHCP-Server zu mounten und - wie oben beschrieben - die Kickstart-Datei unter Verwendung desselben `<IP-Adresse>-kickstart`-Dateinamens aufzufinden.

F.3 Starten einer Kickstart-Installation

Booten Sie zunächst das System von einer Red Hat Linux Bootdiskette, und geben Sie am Boot-Prompt den entsprechenden Bootbefehl ein. Wenn sich die Kickstart-Datei auf der Bootdiskette befindet, lautet der entsprechende Bootbefehl folgendermaßen:

```
boot: linux ks=floppy
```

Wenn sich die Kickstart-Datei auf einem Server befindet, lautet der entsprechende Bootbefehl folgendermaßen:

```
boot: linux ks
```

Anaconda sucht nach einer Kickstart-Datei, wenn das Befehlszeilenargument `ks` an den Kernel übergeben wird. Das kann auf verschiedene Weise geschehen:

`ks=floppy`

Das Installationsprogramm sucht nach der Datei `ks.cfg` in einem VFAT-Dateisystem auf der Diskette im Laufwerk /dev/fd0.

`ks=hd:<Gerät>/<Datei>`

Das Installationsprogramm mountet das Dateisystem auf *<Gerät>* (muss VFAT oder ext2 sein) und sucht nach der Kickstart-Konfigurationsdatei *<Datei>* in diesem Dateisystem (z.B. `ks=hd:sda3/mydir/ks.cfg`).

`ks=file:/<Datei>`

Das Installationsprogramm versucht, die Datei *<Datei>* im Dateisystem zu lesen. Es werden keine Mounts vorgenommen. So wird normalerweise vorgegangen, wenn sich die Kickstart-Datei bereits auf dem `initrd`-Image befindet.

`ks=nfs:`*`<Server:>/<Pfad>`*

Das Installationsprogramm sucht nach der Kickstart-Datei auf dem NFS-Server *<Server>* als Datei *<Pfad>*. Das Installationsprogramm verwendet DHCP zur Konfiguration der Ethernet-Karte.

`ks=cdrom:`*`/<Pfad>`*

Das Installationsprogramm sucht nach der Kickstart-Datei auf der CD-ROM als Datei *<Pfad>*.

`ks`

Wenn `ks` ohne weitere Informationen eingegeben wird, konfiguriert das Installationsprogramm die Ethernet-Karte im System mit DHCP. Das System verwendet den "Bootserver" gemäß der DHCP-Rückmeldung als NFS-Server, von dem die Kickstart-Datei gelesen wird (die Standardeinstellung ist dieselbe wie für den DHCP-Server). Der Name der Kickstart-Datei wird wie folgt vergeben:

- Wenn DHCP angegeben ist und die "Bootdatei" mit einem `/` beginnt, wird diese Datei auf dem NFS-Server gesucht.
- Wenn DHCP angegeben ist und die "Bootdatei" nicht mit einem `/` beginnt, wird im Verzeichnis `/kickstart` auf dem NFS-Server nach dieser Datei gesucht.
- Wenn DCHP keine "Bootdatei" angegeben hat, versucht das Installationsprogramm, die Datei `/kickstart/1.2.3.4-kickstart` zu lesen, wobei *1.2.3.4* die nummerische IP-Adresse des Rechners ist, auf dem die Installation vorgenommen wird.

F.4 Die Kickstart-Datei

Nachdem Sie einige Hintergrundinformationen zur Kickstart-Installation erhalten haben, wird im Folgenden die Kickstart-Datei selbst näher beschrieben. Es handelt sich dabei um eine einfache Textdatei, die mehrere jeweils durch Schlüsselwörter gekennzeichnete Einträge enthält. Sie können diese Datei entweder durch Bearbeiten einer

Kopie der im Verzeichnis `/doc` der Red Hat Linux CD-ROM gespeicherten Datei `sample.ks` erstellen oder ganz neu anlegen. Die Datei kann mit einem beliebigen Texteditor oder Textverarbeitungsprogramm bearbeitet werden, falls mit diesem Programm das Speichern der Dateien als ASCII-Text möglich ist.

Zunächst ein paar prinzipielle Regeln, die bei der Erstellung der Kickstart-Datei berücksichtigt werden müssen:

- Die *Reihenfolge* der Einträge ist vorgeschrieben. Die Reihenfolge lautet:

  ```
  <Abschnitt mit Befehlen>
  <beliebige Kombination aus %pre, %post, %packages>
  <Installationsklasse>
  ```

- Nicht erforderliche Einträge können weggelassen werden.
- Falls erforderliche Einträge fehlen, wird der Benutzer wie beim herkömmlichen Installationsprozess aufgefordert, die nötigen Angaben zu machen. Danach wird die Installation im automatischen Modus fortgesetzt.
- Zeilen, die mit einem Gatter-Zeichen ("#") beginnen, werden als Kommentar interpretiert und ignoriert.
- Bei *Upgrades* mit der Kickstart-Methode sind die folgenden Einträge erforderlich:
  - Sprache
  - Installationsart
  - Geräteangabe (wenn das Gerät für die Installation erforderlich ist)
  - Tastaturkonfiguration
  - Schlüsselwort `upgrade`
  - LILO-Konfiguration

  Andere eingetragene Informationen werden bei einer Aktualisierung ignoriert (dies gilt auch für ausgewählte Pakete).

- Kickstart-Dateien sind in drei Abschnitte unterteilt: Befehle, Paketliste und Skripten. Die Datei muss folgende Form haben:
  - *<Kickstart-Befehle>*
  - %packages
  - *<Paketliste>*
  - %post
  - *<Skripten, die nach der Installation ausgeführt werden sollen>*

Die Reihenfolge muss genau eingehalten werden. Der Abschnitt post muss sich am Ende der Datei befinden und bildet gleichzeitig die Endmarkierung für die Datei.

F.5 Kickstart-Befehle

Die folgenden Befehle können in einer Kickstart-Datei verwendet werden.

F.5.1 `auth` - Authentifizierungsoptionen

`auth` (obligatorisch)

Richtet die Authentifizierungsoptionen für das System ein. Dieser Befehl ähnelt dem Befehl `authconfig`, der nach der Installation ausgeführt werden kann. Standardmäßig wird statt Shadow-Passwörtern die normale Verschlüsselung verwendet.

`--enablemd5`

Verwenden von MD5-Verschlüsselung für die Benutzerpasswörter.

`--enablenis`

Aktiviert die NIS-Unterstützung. Standardmäßig verwendet `--enablenis` die nächste Domäne, die im Netzwerk gefunden wird. Eine Domäne sollte fast immer manuell eingestellt werden (über `--nisdomain`).

--nisdomain

NIS-Domänenname für NIS-Dienste.

--nisserver

Server für NIS-Dienste (Standardvorgabe ist Broadcast).

--useshadow

Shadow-Passwörter verwenden.

--enableldap

Aktiviert die LDAP Unterstützung in `/etc/nsswitch.conf` und ermöglicht es Ihrem System, Informationen über Benutzer (UIDs, Home-Verzeichnis, Shells etc.) aus einem LDAP-Verzeichnis abzufragen. Um diese Option verwenden zu können, muss das Paket `nss_ldap` installiert sein. Außerdem müssen Sie einen Server und einen Basis-DN angeben.

--enableldapauth

Verwenden Sie LDAP als Methode zur Authentifizierung. Dadurch wird das Modul `pam_ldap` in die Lage versetzt, Authentifizierungen und Passwortänderungen unter Verwendung eines LDAP-Verzeichnisses vorzunehmen. Um diese Option verwenden zu können, muss das Paket `nss_ldap` installiert sein. Außerdem müssen Sie einen Server und einen Basis-DN angeben.

--ldapserver=

Der Name des verwendeten LDAP-Servers, wenn Sie entweder --enableldap oder --enableldapauth angegeben haben. Diese Option wird in der Datei `/etc/ldap.conf` eingerichtet.

--ldapbasedn=

Der eindeutige Name (Distinguished Name, DN) in Ihrem LDAP-Verzeichnisbaum, unter dem die Benutzerinformationen gespeichert sind. Diese Option wird in der Datei `/etc/ldap.conf` eingerichtet.

--enablekrb5

Verwenden Sie Kerberos 5 zur Überprüfung von Benutzern. Kerberos selbst kann keine Informationen über Home-Verzeichnisse, UIDs oder Shells abrufen. Das bedeutet: Wenn Sie Kerberos aktivieren, müssen Sie auch weiterhin noch LDAP, NIS oder Hesiod aktivieren, falls Sie es vermeiden möchten, den Befehl `/usr/sbin/useradd` zu verwenden, um Informationen zu Accounts dieser Workstation zu übergeben. Um diese Option verwenden zu können, muss das Paket `pam_krb5` installiert sein.

--krb5realm

Der Kerberos 5 Realm, zu dem Ihre Workstation gehört.

--krb5kdc

KDC (Key Distribution Center) oder KDCs, die Anfragen für den Realm (d.h. Gültigkeitsbereich) bearbeiten. Falls sich mehrere KDCs in Ihrem Realm befinden, müssen Sie ihre Namen durch Komma trennen ([,]).

--krb5adminserver

Das KDC in Ihrem Realm, das ebenfalls kadmind ausführt. Dieser Server, der (falls Sie über mehr als ein KDC verfügen) nur auf dem Master-KDC ausgeführt werden kann, bearbeitet Passwortänderungen und andere Verwaltungsanforderungen.

--enablehesiod

Aktivieren Sie die Hesiod-Unterstützung, um Home-Verzeichnisse von Benutzern, UIDs und Shells anzuzeigen. Weitere Informationen dazu, wie Sie Hesiod in Ihrem Netzwerk einrichten und verwenden, finden Sie in der Datei `/usr/share/doc/glibc-2.x.x/README.hesiod`, die im Lieferumfang des Paketes `glibc` enthalten ist. Hesiod ist eine Erweiterung des DNS und verwendet DNS-Datensätze, um Informationen über Benutzer, Gruppen und andere Objekte zu speichern.

--hesiodlhs

Die Option Hesiod LHS ("left-hand side", linke Seite), die in `/etc/hesiod.conf` eingerichtet wird. Diese Option wird von der Hesiod-Bibliothek verwendet, um den Namen zu bestimmen, nach dem im DNS bei der Abfrage von Informationen gesucht werden soll. Die Funktionsweise ähnelt der Art, wie LDAP einen Basis-DN verwendet.

--hesiodrhs

Die Option Hesiod RHS ("right-hand side", rechte Seite), die in `/etc/hesiod.conf` eingerichtet wird. Diese Option wird von der Hesiod-Bibliothek verwendet, um den Namen zu bestimmen, nach dem im DNS bei der Abfrage von Informationen gesucht werden soll. Die Funktionsweise ähnelt der Art, wie LDAP einen Basis-DN verwendet.

Tipp

Um z.B. Benutzerinformationen zu "jim" anzuzeigen, sucht die Hesiod-Bibliothek nach *jim.passwd<LHS><RHS>*. Das Suchergebnis wäre dann ein TXT-Eintrag, der dem Passworteintrag des Benutzers "Jim" entspricht (`jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`). Dieselbe Vorgehensweise gilt auch für Gruppen, mit dem einzigen Unterschied, dass hier *jim.group<LHS><RHS>* verwendet würde.

Es kann auch anhand von Nummern nach Benutzern und Gruppen gesucht werden. Dazu muss "501.uid" als CNAME für "jim.passwd" und "501.gid" als CNAME für "jim.group" angegeben werden. Bitte beachten Sie, dass keine Punkte [.] vor LHS und RHS gesetzt werden, wenn die Bibliothek den zu suchenden Namen bestimmt, obwohl LHS und RHS meist mit Punkten beginnen.

F.5.2 `clearpart` - Löschen von Partitionen auf Basis des Partitionstyps

`clearpart` (optional)

Enfernt Partitionen, bevor neue Partitionen erstellt werden. Standardmäßig werden keine Partitionen entfernt.

`--linux`

Löscht Linux-Partitionen (Typ 0x82, 0x83 und 0xfd [RAID]).

--all

Löscht alle Partitionen vom System.

F.5.3 device --opts

device (optional)

Auf den meisten PCI-Systemen erkennt das Installationsprogramm automatisch die meisten Ethernet- und SCSI-Karten ordnungsgemäß. Auf älteren Systemen und einigen PCI-Systemen muss Kickstart jedoch beim Finden der richtigen Geräte unterstützt werden. Der Befehl device weist Anaconda an, Zusatzmodule zu installieren. Die Befehlssyntax ist wie folgt:

```
device <Typ>
<Modulname> --opts
<Optionen>
```

Als <Typ> sollte "scsi" oder "eth" angegeben werden, und der *<Modulname>* ist der Name des Kernel-Moduls, das installiert sein sollte.

--opts

Optionen, die an das Kernelmodul übergeben werden sollen. Beachten Sie, dass durch das Einschließen in Anführungszeichen mehrere Optionen übergeben werden können. Beispiel:

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

F.5.4 driverdisk

driverdisk (optional)

Beim Kickstart können Treiberdisketten verwendet werden. Kopieren Sie dazu den Inhalt einer Treiberdiskette in das Root-Verzeichnis einer Partition auf der Festplatte des Systems, und verwenden Sie dann den Befehl `driverdisk`, um das Installationsprogramm anzuweisen, wo es danach suchen soll.

```
driverdisk <Partition> [--type
<FS-Typ>]
```

<Partition> ist die Partition, in der sich die Treiberdiskette befindet.

`--type`

Dateisystemtyp (z.B. VFAT oder ext2).

F.5.5 `install`

`install` (optional)

Weist das System an, ein neues System zu installieren, anstatt ein vorhandenes System zu aktualisieren. Dies ist der Standardmodus.

F.5.6 Installationsarten

Sie müssen einen dieser vier Befehle verwenden, um anzugeben, welche Art von Kickstart ausgeführt werden soll:

NFS

Installation vom NFS-Server.

- --server *<Server>*

  Server, von dem aus die Installation vorgenommen werden soll (Rechnername oder IP).

- --dir *<Verzeichnis>*

  Verzeichnis mit dem Red Hat Installationsverzeichnisbaum.

Beispiel:

```
nfs --server <Server> --dir
<Verzeichnis>
```

CD-ROM

Installation vom ersten CD-ROM-Laufwerk des Systems.

Beispiel:

```
cdrom
```

harddrive

Installation von einem Red Hat Installationsverzeichnisbaum auf einem lokalen Laufwerk (VFAT oder ext2).

- --partition <*Partition*>

  Partition, von der installiert werden soll (z.B. sdb2).

- --dir <*Verzeichnis*>

  Verzeichnis mit dem Red Hat Installationsverzeichnisbaum.

Beispiel:

```
harddrive --partition <Partition> --dir <Verzeichnis>
```

URL

Installation von einem Red Hat Installationsverzeichnisbau auf einem Remote-Server über FTP oder HTTP.

Beispiel:

```
url --ulr http://<Server>/<Verzeichnis>
```

F.5.7 `keyboard`

`keyboard` (obligatorisch)

Zur Angabe des Typs der Systemtastatur. Hier die Liste der verfügbaren Tastaturen auf i386- und Alpha-Rechnern:

```
azerty, be-latin1, be2-latin1, fr-latin0, fr-latin1, fr-pc, fr,
wangbe, ANSI-dvorak, dvorak-l, dvorak-r, dvorak, pc-dvorak-latin1,
tr_f-latin5, trf, bg, cf, cz-lat2-prog, cz-lat2, defkeymap,
defkeymap_V1.0, dk-latin1, dk. emacs, emacs2, es, fi-latin1, fi,
gr-pc, gr, hebrew, hu101, is-latin1, it-ibm, it, it2, jp106,
la-latin1, lt, lt.l4, nl, no-latin1, no, pc110, pl, pt-latin1,
pt-old, ro, ru-cp1251, ru-ms, ru-yawerty, ru, ru1, ru2, ru_win,
se-latin1, sk-prog-qwerty, sk-prog, sk-qwerty, tr_q-latin5, tralt,
```

```
trf, trq, ua, uk, us, croat, cz-us-qwertz, de-latin1-nodeadkeys,
de-latin1, de, fr_CH-latin1, fr_CH, hu, sg-latin1-lk450,
sg-latin1, sg, sk-prog-qwertz, sk-qwertz, slovene
```

Hier die Liste für SPARC-Rechner:

```
sun-pl-altgraph, sun-pl, sundvorak, sunkeymap, sunt4-es,
sunt4-no-latin1, sunt5-cz-us, sunt5-de-latin1, sunt5-es,
sunt5-fi-latin1, sunt5-fr-latin1, sunt5-ru, sunt5-uk, sunt5-us-cz
```

F.5.8 `Sprache`

`lang` (obligatorisch)

Gibt die Standardsprache für das installierte System an. Die angegebene Sprache wird während der Installation und zur Konfiguration aller sprachspezifischen Aspekte des installierten Systems verwendet. Wenn Sie zum Beispiel die Sprache Deutsch einrichten möchten, lautet der entsprechende Eintrag in der Kickstart-Datei:

```
lang de_DE
```

Gültige Sprachcodes sind:

```
cs_CZ, en_US, fr_FR, de_DE, hu_HU, is_IS, id_ID, it_IT,
ja_JP.ujis, no_NO, pl_PL, ro_RO, sk_SK, sl_SI, es_ES,
ru_RU.KOI8-R, uk_UA
```

F.5.9 `lilo`

`lilo` (obligatorisch)

Gibt an, wie der Bootloader auf dem System installiert werden soll. Standardmäßig wird LILO in den MBR der ersten Festplatte installiert. Wenn eine DOS-Partition gefunden wird, wird ein Dual-Boot-System installiert. (Das DOS/Windows-System wird gebootet, wenn am `LILO:`-Prompt **`dos`** durch den Benutzer eingegeben wird.)

`--append` <***Parameter***>

Angabe von Kernelparametern.

`--linear`

Verwendung der `linearen` LILO-Option. Dies dient nur der Abwärtskompatibilität. (Linear wird inzwischen als Standardeinstellung verwendet.)

`--location`

Gibt an, wo der LILO-Booteintrag gespeichert wird. Gültige Werte sind **`mbr`** (Standardvorgabe), **`partition`** (installiert den Bootloader in den ersten Sektor der Partition, in der sich der Kernel befindet) oder none, wodurch keine Bootloader installiert wird.

F.5.10 `lilocheck`

`lilocheck` (optional)

Wenn diese Angabe vorhanden ist, prüft das Installationsprogramm, ob sich LILO im MBR der ersten Festplatte befindet und startet das System neu, falls dies zutrifft - in diesem Fall wird keine Installation durchgeführt. Dadurch kann verhindert werden, dass Kickstart ein bereits installiertes System nochmals installiert.

F.5.11 `mouse`

`mouse` (obligatorisch)

Konfiguriert die Maus für das System, sowohl für den grafischen Modus als auch für den Textmodus. Optionen:

`--device` <***Gerät***>

Das Gerät, an dem die Maus angeschlossen ist (z.B. --device ttyS0).

--emulthree

Wenn das X Window System installiert ist, werden die linke und die rechte Maustaste zum Emulieren einer dritten Maustaste verwendet (bei Zwei-Tasten-Mäusen).

Nach den Optionen kann einer der folgenden Maustypen angegeben werden:

```
alpsps/2, ascii, asciips/2, atibm, generic, generic3,
genericps/2, generic3ps/2, geniusnm, geniusnmps/2,
geniusnsps/2, thinking, thinkingps/2, logitech,
logitechcc, logibm, logimman, logimmanps/2, logimman+,
logimman+ps/2, microsoft, msnew, msintelli, msintellips/2,
msbm, mousesystems, mmseries, mmhittab, sun, none
```

Wenn der Befehl mouse ohne Argumente angegeben oder weggelassen wird, versucht das Installationsprogramm, die Maus selbst zu erkennen (funktioniert bei den meisten neueren Mäusen).

F.5.12 `network`

`network` (optional)

Konfiguriert Netzwerkinformationen für das System. Wenn diese Option nicht angegeben ist und die Kickstart-Installation keine Netzwerkfunktion erfordert (also keine Installation über NFS), wird keine Netzwerkfunktionalität für das System konfiguriert. Wenn die Installation Netzwerkfunktionalität erfordert, geht Anaconda davon aus, dass über eth0 und eine dynamische IP-Adresse (BOOTP/DHCP) installiert werden soll, und konfiguriert das fertig installierte System so, dass seine IP-Adresse automatisch bestimmt wird. Der Befehl network konfiguriert die Netzwerkinformationen für Netzwerk-Kickstart-Installationen und für das fertig installierte System.

--bootproto

Eine der folgenden Angaben: **dhcp**, **bootp**, oder **static** (Standardvorgabe DHCP, **dhcp** und **bootp** werden gleich behandelt). **static** muss angegeben werden, wenn statische IP-Informationen verwendet werden sollen.

--device ***<Gerät>***

Wird verwendet, um ein spezifisches Ethernet-Gerät für die Installation auszuwählen. Bitte beachten Sie: Der Befehl `--device` *<Gerät>* wird erst dann wirksam, wenn es sich bei der Kickstart-Datei um eine lokale Datei handelt (z.B. ks=floppy), da das Installationsprogramm das Netzwerk für das Auffinden der Kickstart-Datei konfiguriert. Beispiel:

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

--ip

IP-Adresse des zu installierenden Rechners.

--gateway

Standard-Gateway als IP-Adresse.

--nameserver

Primärer Nameserver als IP-Adresse.

--netmask

Netzmaske für das installierte System.

--hostname

Rechnername für das installierte System.

Es gibt drei Möglichkeiten zur Netzwerkkonfiguration:

- DHCP
- BOOTP
- statisch

Bei der DHCP-Methode bezieht das System die Informationen zur Netzwerkkonfiguration von einem DHCP-Serversystem. Die BOOTP-Methode benötigt entsprechend einen BOOTP-Server, der die Informationen zur Netzwerkkonfiguration liefert.

Bei der statischen Methode müssen Sie selbst alle erforderlichen Informationen zum Netzwerk in die Kickstart-Datei eintragen. Diese Informationen sind statisch, d.h. sie werden während der Installation und auch nach der Installation verwendet.

Mit der folgenden Zeile weisen Sie ein System an, die Netzwerkkonfiguration über DHCP zu beziehen:

```
network --bootproto dhcp
```

Entsprechend bestimmt die nächste Zeile für diese Aufgabe einen BOOTP-Server:

```
network --bootproto bootp
```

Wenn Sie die statische Methode gewählt haben, ist die Zeile etwas komplexer, da Sie alle Konfigurationsinformationen in einer Zeile angeben müssen. Die folgenden Angaben sind obligatorisch:

- IP-Adresse
- Netzmaske
- IP-Adresse des Gateways
- IP-Adresse des Nameservers

Hier ein Beispiel für eine statische Zeile:

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

Bitte beachten

Die gesamte `Netzwerkkonfiguration` *muss* in einer Zeile untergebracht werden. Nur aus Gründen der besseren Lesbarkeit haben wir in diesem Beispiel Zeilenumbrüche eingefügt.

Beachten Sie bitte die folgenden Einschränkungen, die für die statische Methode gelten:

- Alle statischen Informationen zur Netzwerkkonfiguration müssen in *einer* Zeile angegeben werden. Es ist nicht möglich, Zeilen z.B. mit Hilfe eines umgekehrten Schrägstrichs umzubrechen.
- Sie können hier nur einen Nameserver angeben. Im Abschnitt `%post` der Kickstart-Datei (beschrieben in Abschnitt F.5.24, *`%post` - Konfigurieren nach der Installation*) können Sie jedoch bei Bedarf weitere Nameserver hinzufügen.

F.5.13 `partition`

`part` (obligatorisch für Installationen, bei Aktualisierungen ignoriert)

Erstellt auf dem System eine Partition. Die Partitionsvorgaben haben die Form:

```
part <Mountpoint> --size
<Größe> [--grow] [--onpart
<Partition>] [--ondisk
<Laufwerk>] [--onprimary
<N>] [--asprimary <N>]
```

Am <*Mountpoint*> ist die Partition gemountet. Die Angaben müssen mit einer der folgenden Methoden gemacht werden:

/<Mountpoint>

(z.B. **`/`**, **`/usr`**, **`/home`**)

swap

Die Partition wird als Swap-Bereich verwendet.

raid.<*id*>

Die Partition wird für Software-RAID verwendet (siehe Befehl `raid` weiter unten).

--size <*Größe*>

Legt die Mindestgröße der Partition fest

--grow

Weist die Partition an, sich an den verfügbaren Platz (falls vorhanden) anzupassen oder die maximale Größe anzunehmen.

--maxsize <*Größe*>

Richtet die maximale Partitionsgröße ein, wenn die Partition angewiesen wurde, ihre Größe anzupassen.

--noformat

Weist das Installationsprogramm an, die Partition nicht zu formatieren, damit sie für die Verwendung mit dem Befehl `--onpart` zur Verfügung steht.

--onpart <*Partition*> oder --usepart <*Partition*>

Weist das Installationsprogramm an, die Partition auf dem *bereits vorhandenen* Gerät <*Partition*> anzulegen. `partition /home --onpart hda1` legt zum Beispiel `/home` auf Gerät `/dev/hda1` an, das bereits vorhanden sein muss.

--ondisk <*Laufwerk*>

Erzwingt die Erstellung der Partition auf einer speziellen Festplatte. `--ondisk sdb` legt die Partition zum Beispiel auf der zweiten Systemfestplatte an.

--onprimary <*N*>

Erzwingt die Erstellung der Partition auf der primären Partition <*N*> oder ein Fehlschlagen der Partitionserstellung. <*N*> kann die Werte 1 bis 4 annehmen.

--asprimary <*N*>

Erzwingt die automatische Zuweisung als primäre Partition <*N*> oder ein Fehlschlagen der Zuweisung. <*N*> kann die Werte 1 bis 4 annehmen.

--bytes-per-inode=<*N*>

<*N*> steht für die Anzahl Byte pro Inode im Dateisystem, während dieses erstellt wird. Der Wert muss im Dezimalformat angegeben werden. Diese Option ist besonders bei Anwendungen nützlich, bei denen Sie die Anzahl der Inodes im Dateisystem erhöhen möchten.

--type=<*X*>

Stellt den Partitionstyp auf <*X*> ein, wobei <*X*> für einen nummerischen Wert steht.

Alle erstellten Partitionen werden während des Installationsvorgangs formatiert, es sei denn, Sie verwenden die Befehle `--noformat` und `--onpart`.

Bitte beachten

Falls der Befehl `--clearpart` in der Datei `ks.cfg` verwendet wird, dann kann `--onpart` nicht für eine logische Partition verwendet werden.

Bitte beachten

Falls die Partitionierung aus irgendeinem Grund nicht vorgenommen werden kann, werden auf VC3 Diagnosemeldungen angezeigt.

F.5.14 `raid`

`raid` (optional)

Erstellt ein Software-RAID-Gerät. Dieser Befehl hat die Form:

```
raid <Mountpoint> --level
<Level> --device
<RAID-Gerät><Partitionen*>
```

Am <*Mountpoint*> wird das RAID-Dateisystem gemountet. Bei `/` muss RAID Level 1 verwendet werden, es sei denn, es ist eine Boot-Partition vorhanden (`/boot`). In diesem Fall muss die `/boot`-Partition vom Typ Level 1 sein. Für den Typ der Root (`/`)-Partition kann jeder der verfügbaren Typen festgelegt werden. <*Partitionen**> (* deutet an, dass mehrere Partitionen aufgeführt werden können) gibt die RAID-Bezeichnungen an, die zum RAID-Array hinzugefügt werden sollen.

--level <*Level*>

Zu verwendender RAID-Level (0, 1 oder 5).

--device <*RAID-Gerät*>

Bezeichnung des zu verwendenden RAID-Gerätes (z.B. md0 oder m1). Für RAID-Geräte können die Bezeichnungen md0 bis md7 (und jede nur einmal) verwendet werden.

Im Folgenden sehen Sie ein Beispiel dafür, wie eine Partition vom Typ RAID Level 1 für `/` und eine Partition vom Typ RAID Level 5 für `/usr` erstellt wird. In diesem Beispiel wird davon ausgegangen, dass im System drei SCSI-Platten vorhanden sind. Es werden außerdem drei Swap-Partitionen erstellt, auf jedem Laufwerk eine.

```
part raid.01 --size 60 --ondisk sda
part raid.02 --size 60 --ondisk sdb
part raid.03 --size 60 --ondisk sdc


part swap --size 128 --ondisk sda
part swap --size 128 --ondisk sdb
```

```
part swap --size 128 --ondisk sdc

part raid.11 --size 1 --grow --ondisk sda
part raid.12 --size 1 --grow --ondisk sdb
part raid.13 --size 1 --grow --ondisk sdc

raid / --level 1 --device md0 raid.01 raid.02 raid.03 raid /usr
--level 5 --device md1 raid.11 raid.12 raid.13
```

F.5.15 `reboot`

`reboot` (optional)

Neustart nach fertig gestellter Installation (keine Argumente). Normalerweise zeigt Kickstart eine Meldung an und wartet darauf, dass der Benutzer zum Neustart eine Taste betätigt.

F.5.16 `rootpw`

`rootpw` (obligatorisch)

Verwendung: rootpw [--iscrypted] <*Passwort*>

Setzt das Root-Passwort auf das als Argument angegebene <*Passwort*>.

--iscrypted

Wenn diese Angabe vorhanden ist, wird davon ausgegangen, dass das Passwort-Argument bereits verschlüsselt ist.

F.5.17 `skipx`

`skipx` (optional)

Wenn diese Angabe vorhanden ist, wird auf dem installierten System X nicht konfiguriert.

F.5.18 `timezone`

`timezone` (obligatorisch)

timezone [--utc] <*Zeitzone*>

Die System-Zeitzone wird auf <*Zeitzone*> eingestellt. Es kann jede der in "timeconfig" aufgeführten Zeitzonen angegeben werden.

--utc

Wenn diese Angabe vorhanden ist, geht das System davon aus, dass die Hardware-Uhr auf UTC (Greenwich Mean)-Zeit eingestellt ist.

F.5.19 `upgrade`

`upgrade` (optional)

Weist das System an, ein vorhandenes System zu aktualisieren, statt ein neues System zu installieren.

F.5.20 `xconfig`

`xconfig` (optional)

Konfiguriert das X Window System. Wenn diese Option nicht angegeben wird, muss X während der Installation vom Benutzer manuell konfiguriert werden, falls X installiert wurde. Diese Option sollte nur verwendet werden, wenn X auf dem Endsystem installiert ist.

--noprobe

Keine Monitor-Erkennung.

--card <*Karte*>

Verwendung von Karte <*Karte*>. Der Kartenname muss in der Kartenliste in Xconfigurator enthalten sein. Wenn dieses Argument nicht angegeben wird, fragt Anaconda den PCI-Bus nach der Karte ab.

--monitor <*Monitor*>

Verwendung des Monitors <*Monitor*>. Der Monitorname muss in der Monitorliste in Xconfigurator enthalten sein. Diese Angabe wird ignoriert, wenn **`--hsync`** oder **`--vsync`** angegeben ist. Wenn keine Monitorinformationen angegeben sind, wird die Monitorerkennung über Plug-and-Play durchgeführt.

--hsync <*Monitorfrequenz*>

Gibt die Horizontalfrequenz des Monitors an.

--vsync <*Monitorfrequenz*>

Gibt die Bildwiederholrate des Monitors an.

--defaultdesktop=(*GNOME* oder *KDE*)

Stellt als Standard-Desktop entweder GNOME oder KDE ein (und geht davon aus, dass GNOME und/oder KDE durch `%packages` installiert wurde).

--startxonboot

Verwendung eines grafischen Dialogfelds für die Anmeldung (Runlevel 5) für das installierte System.

F.5.21 `zerombr` - Initialisieren der Partitionstabelle

`zerombr` **(optional)**

Wenn "zerombr" angegeben wird und "yes" das einzige Argument ist, werden alle auf den Festplatten gefundenen ungültigen Partitionstabellen initialisiert. Dadurch wird der gesamte Inhalt der Festplatten mit ungültigen Partitionstabellen gelöscht. Verwendung:

```
zerombr yes
```

Es ist kein anderes Format möglich.

F.5.22 `%packages` - Auswählen der Pakete

Der Befehl `%packages` steht am Beginn eines Kickstart-Dateiabschnitts, in dem die zu installierenden Pakete aufgeführt sind (nur für Installationen, die Paketauswahl bei Aktualisierungen wird nicht unterstützt).

Pakete können als Komponenten oder als einzelne Paketnamen angegeben werden. Das Installationsprogramm definiert verschiedene Komponenten, in denen Pakete mit ähnlichen Funktionen zusammengefasst sind. Eine Liste der Komponenten finden Sie in der Datei `RedHat/base/comps` auf jeder Red Hat Linux CD-ROM. Die Zeilen zur Angabe von Komponenten beginnen mit einer Zahl, gefolgt von einem Leerzeichen und dem Namen der Komponente. In dieser Komponente sind die einzelnen Komponenten Zeile für Zeile aufgelistet. Einzelpaketen ist keine Zahl vorangestellt.

Zusätzlich gibt es drei weitere Zeilentypen in der Datei `comps`:

Architekturspezifisch (alpha:, i386: und sparc64:)

Wenn ein Paketname mit einem Architekturtyp beginnt, muss nur der Paketname eingegeben zu werden, nicht der Architekturname. Beispiel:

Für `i386: netscape-common`. Es muss nur der Teil `netscape-common` angegeben werden, damit dieses Paket installiert wird.

Zeilen mit vorangestelltem ?

Zeilen, die mit `?` beginnen, gelten nur für das Installationsprogramm. Diese Zeilentypen brauchen Sie nicht zu beachten.

Zeilen, mit vorangestelltem `--hide`

Wenn ein Paketname mit `--hide` beginnt, muss nur der Paketname ohne `--hide` angegeben werden. Beispiel:

Bei `--hide KDE Workstation` muss nur der Teil `KDE Workstation` angegeben werden, um dieses Paket zu installieren.

Normalerweise reicht es aus, wenn Sie nur die gewünschten Komponenten und nicht die einzelnen Pakete angeben. Bitte beachten Sie, dass standardmäßig immer die

`Basis-` Komponente ausgewählt wird. Es ist daher nicht notwendig, sie im Abschnitt `%packages` anzugeben.

Hier ein Beispiel für eine `%packages`-Auswahl:

```
%packages
@ Networked Workstation
@ C Development
@ Web Server
@ X Window System
bsd-games
```

Wie das Beispiel zeigt, werden die Komponenten zeilenweise angegeben. Die Zeilen werden mit dem Zeichen `@` eingeleitet, gefolgt von einem Leerzeichen und dem vollständigen Namen der Komponente (aus der Datei `comps`). Einzelne Pakete werden ohne zusätzliche Zeichen eingetragen (im obigen Beispiel steht die Zeile `bsd-games` für ein einzelnes Paket).

Bitte beachten

Sie können die Kickstart-Installation auch anweisen, die Workstation- und Server-Installationen zu verwenden. (Sie können auch die vollständige Installation auswählen, um alle Pakete zu installieren.) Fügen Sie hierzu einfach *eine* der folgenden Zeilen in den Abschnitt `%packages` ein:

```
@ Gnome Workstation
@ KDE Workstation
@ Server
@ Everything
```

F.5.23 `%pre` -- Konfigurieren vor der Installation

Sie können Befehle hinzufügen, die direkt nach der Analyse von `ks.cfg` im System ausgeführt werden. Dieser Abschnitt muss sich am Ende der Kickstart-Datei befinden (nach den Befehlen) und mit dem Befehl `%pre` beginnen. Bitte beachten Sie, dass Sie im Abschnitt `%pre` auf das Netzwerk zugreifen können. Allerdings wurde

name service bisher noch nicht konfiguriert, so dass nur IP-Adressen funktionieren. Im Folgenden sehen Sie ein Beispiel für den Abschnitt `%pre`:

```
%pre

# Kommentar zu /etc/motd hinzufügen
echo "Kickstart-Installation Red Hat Linux ‘/bin/date‘" > /etc/motd

# einen weiteren Nameserver hinzufügen
echo "nameserver 10.10.0.2" >> /etc/resolv.conf
```

Diese Abschnitt erstellt eine Message-of-the-day-Datei, die das Datum der Kickstart-Installation enthält und die Beschränkung des Befehls `network` auf "nur einen Nameserver" dadurch umgeht, dass ein weiterer Nameserver zu `/etc/resolv.conf` hinzugefügt wird.

Bitte beachten

Das pre-Installationsskript wird nicht in der chroot-Umgebung ausgeführt.

F.5.24 `%post` - Konfigurieren nach der Installation

Sie können Befehle hinzufügen, die nach der abgeschlossenen Installation auf dem System ausgeführt werden. Dieser Abschnitt muss sich am Ende der Kickstart-Datei befinden und mit dem Befehl `%post` beginnen. Bitte beachten Sie, dass Sie im Abschnitt `%post` auf das Netzwerk zugreifen können. Allerdings wurde bisher kein **name service** konfiguriert, so dass nur IP-Adressen funktionieren. Hier ein Beispiel für einen `%post`-Abschnitt:

```
%post

# Kommentar zu /etc/motd hinzufügen
echo "Red Hat Linux Kickstart-Installation ‘/bin/date‘"  > /etc/motd

# einen weiteren Nameserver hinzufügen
echo "nameserver 10.10.0.2" >> /etc/resolv.conf
```

Diese Abschnitt erstellt eine Message-of-the-day-Datei, die das Datum der Kickstart-Installation enthält und die Beschränkung des Befehls `network` auf "nur einen Nameserver" dadurch umgeht, dass ein weiterer Nameserver zu `/etc/resolv.conf` hinzugefügt wird.

Bitte beachten

Die nach der Installation ausgeführten Skripten werden in einer chroot-Umgebung ausgeführt. Daher ist zum Beispiel das Kopieren von Skripten oder RPMs vom Installationsmedium nicht möglich.

--nochroot

Damit können Befehle angegeben werden, die außerhalb der chroot-Umgebung ausgeführt werden sollen.

--interpreter ***/usr/bin/perl***

Ermöglicht es Ihnen, eine andere Skript-Sprache wie z.B. perl anzugeben.

Index

A

B

K

L

R

S

T

U

Z