Red Hat Linux 7.1

Das Offizielle Red Hat Linux Referenzhandbuch

ISBN: N/A


Red Hat, Inc.

2600 Meridian Parkway
Durham , NC 27713 USA

Research Triangle Park, NC 27709 USA

rhl-rg(DE)-7.1-Print-RHI (2001-02-21T10:50-0500)

Printed in Canada, Ireland und Japan

Inhalt

Red Hat Linux 7.1

Einführung

Willkommen im *Offiziellen Red Hat Linux Referenzhandbuch*.

Das *Offizielle Red Hat Linux Referenzhandbuch* enthält nützliche Informationen über Ihr Red Hat Linux System. Für grundlegende Konzepte wie die Struktur des Red Hat Linux Systems bis hin zu den Details wie die Festplattenpartitionierung und Authentifizierungskontrolle, hoffen wir, dass dieses Buch zu einem wertvollen Nachschlagwerk für Sie wird.

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.
- *Red Hat Linux Booten* — Informationen über Runlevels, `rc.d` Verzeichnisse, und wie Sie Ihre Anwendungen zur Boot-Zeit starten können.
- *System-und Netzwerksicherheit* — Entdecken Sie die meist genutzten Angriffsmethoden auf Ihr System, und erfahren Sie, wie Sie Sicherheitsproblemen vorbeugen können.
- *RAID-Konzepte* — Fassen Sie verschiedene Diskettenlaufwerke zu einer einzigen Einheit zusammen, um die Leistung und Verlässlichkeit zu steigern.
- *Sichere Web-Server Installation* — Hinzufügen von Verschlüsselungsfähigkeiten für Ihren Apache Web-Server.

Bevor Sie dieses Handbuch durchlesen, sollten Sie den Inhalt des *Offiziellen Red Hat Linux Installationshandbuchs* über Installationsfragen und des *Offiziellen Red Hat Linux Handbuchs Erste Schritte* über grundlegende Linux Konzepte und des *Offiziellen Red Hat Linux Handbuchs Benutzerdefinierte Konfiguration* für generelle Anweisungen zur Benutzerdefinition durchlesen. Das *Offizielle Red Hat Linux Referenzhandbuch* enthält Informationen über fortgeschrittene Themen, die vielleicht nicht jeden Benutzer betreffen, was jedoch davon abhängt, wie Sie Ihr Red Hat Linux System benutzen.

HTML- und PDF-Versionen aller offizieller Red Hat Linux Handbücher sind online erhältlich unter http://www.redhat.com/support/manuals.

So finden Sie die richtige Dokumentation

Es ist wichtig, dass Sie sich die Dokumentation beschaffen, die für Ihren Kenntnisstand in Sachen Linux geeignet ist. Ansonsten könnten Sie sich schnell überfordert fühlen oder nicht an die Informationen gelangen, die Ihnen Ihre Probleme lösen. Das *Offizielle Red Hat Linux Referenzhandbuch* beschäftigt sich mit den technischeren Aspekten und Optionen Ihres Red Hat Linux Systems. Dieser Abschnitt wird Ihnen dabei helfen zu entscheiden, ob Sie dieses Handbuch als Bezugspunkt benutzen

wollen oder ob Sie andere Red Hat Linux-Handbücher, online Quellen inbegriffen, in Betracht ziehen wollen.

Es gibt drei verschiedene Kategorien von Red Hat Linux Benutzern, und jede dieser Kategorien benötigt eine andere Dokumentation und Informationsquelle. Um genauer sagen zu können, welche für Sie am geeignetsten ist, sollten Sie sich klar darüber werden, wie umfangreich Ihre Vorkenntnisse sind:

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 *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-Gurus* durchlesen.

Dokumentation für Linux-Neulinge

Ein Linux-Neuling könnte von den vielen Informationen die über jedes Argument, wie zum Beispiel Drucken und Starten zur Verfügung stehen, überfordert sein. Bevor Sie sich mit diesen fortgeschrittenen Problemen auseinandersetzen, könnte es hilfreich sein, einen Schritt zurück zu gehen, um genügend Informationen darüber zu sammeln, wie Linux funktioniert.

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

Sie sollten sich die folgende Linux Dokumentaion beschaffen:

- *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, werden Sie im Voraus

herausfinden, wie Sie viele potentielle Probleme lösen können, bevor Sie sich darin verwickelt finden.

- *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.
- *Eine einführende Befehlsübersicht (mit Beispielen)* — Dies ist vielleicht der wichtigste Punkt bei Ihrer Suche nach einer geeigneten Linux-Dokumentation. Die grundlegende Philosophie hinter Linux besteht darin, dass die Kombination "kleiner" Befehle mit eingeschränktem Funktionsumfang der Verwendung einiger weniger (und somit komplexer) Befehle vorzuziehen ist. 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.

  Sie sollten sich darüber im Klaren sein, dass Sie sich nicht an alle zur Verfügung stehenden Linux Befehle erinnern müssen. Es gibt verschiedene Techniken um herauszufinden, welche Art von Dokumentation Ihren Anforderungen vermutlich am besten gerecht wird. Sie sollten nur im Allgemeinen darüber Bescheid wissen, wie Linux funktioniert und wie Sie Zugang zu dem Tool finden, das Ihnen genaue Anweisungen dazu gibt, wie Sie den Befehl ausführen sollten.

Das *Offizielle Red Hat Linux Installationshandbuch* ist ein hervorragender Bezugspunkt, der Ihnen dabei behilflich ist, Ihr Red Hat Linux System erfolgreich zu installieren und zu konfigurieren. Das *Offizielle Red Hat Linux Handbuch Erste Schritte* enthält die Geschichte der Entwicklung der Grundbefehle des Linux Systems, GNOME, KDE, RPM und viele andere grundlegende Konzepte. Sie sollten mit diesen beiden Büchern beginnen und sie dazu verwenden, Ihre Red Hat Linux-Basiskenntnisse zu vertiefen. Früher oder später werden Ihnen auch kompliziertere Konzepte sinnvoll erscheinen, weil Sie bereits eine gewisse Grundkenntnis erlangt haben.

Außer den Red Hat Linux Handbüchern gibt es verschiedene andere Dokumentationsquellen welche entweder wenig kosten oder auch kostenlos zur Verfügung stehen:

Einführung in die Linux-Websites

- http://www.redhat.com — Auf der Red Hat Website, finden Sie Verknüpfungen zum Linux Documentation Project (LDP), den Online-Versionen der Red Hat Linux-Handbücher , den FAQs (häufig gestellte Fragen), der Datenbank für die Suche nach einer Linux-Benutzergruppe in Ihrer Nähe und einer weiteren Datenbank mit Wissenswertem zu Linux u.v.m.
- http://www.linuxheadquarters.com — In der Linux Headquarter-Website finden Sie leicht zu verstehende, schrittweise Anweisungen zu einer Vielzahl von Linux Aufgaben.

Einführung in die Linux Newsgroups

Sie können an den Newsgroups teilnehmen, indem Sie den Diskussionen anderer Benutzer folgen, die versuchen Probleme zu lösen, oder indem Sie aktiv selbst Fragen stellen oder beantworten. Erfahrene Linux-Benutzer sind bekanntlich sehr hilfreich beim Unterstützen der Neulinge im Bezug auf verschiedene Fragen zu Linux— vor allem wenn Sie die richtigen Fragen stellen. Wenn Sie keinen Zugang zu einer News Reader Anwendungen haben, können Sie unter der folgenden Webadresse nach diesen Informationen suchen http://www.deja.com. Es gibt Dutzende von Newsgroups zu Linux, darunter die folgenden:

- linux.help — Ein hervorragender Ort um die Hilfe anderer Linux-Benutzer in Anspruch zu nehmen.
- linux.redhat — Diese Newsgroup behandelt hauptsächlich spezifische Red Hat Linux Themen.
- linux.redhat.install — Stellen Sie dieser Newsgruppe Fragen zur Installation oder kontrollieren Sie, wie andere Benutzer ähnliche Probleme gelöst haben.
- linux.redhat.misc — Fragen, die nicht wirklich zu traditionellen Kategorien gehören kommen hier hin.
- linux.redhat.rpm — Eine ideale Quelle, in der Sie nachsehen können, wenn Sie Schwierigkeiten beim Gebrauch von RPM haben.

Linux Bücher anfangen

- *Red Hat Linux für Dummies, zweite Ausgabe* von Jon "maddog" Hall; IDG
- *Special Edition Using Red Hat Linux* von Alan Simpson, John Ray und Neal Jamison; Que
- *Running Linux* von Matt Welsh und Lar Kaufman; O'Reilly & Associates
- *Red Hat Linux 7 Unleashed* von William Ball und David Pitts; Sams

Die hier erwähnten Bücher sind sicher eine wertvolle Informationsquelle für Grundkenntnisse über ein Red Hat Linux System. Für detailliertere Informationen über die hier im Handbuch besprochenen Argumente finden Sie in vielen Kapiteln eine Liste spezifischer Büchertitel, gewöhnlich in einem Abschnitt mit dem Titel *Zusätzliche Resourcen*.

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. Nach der Installation von Linux können Konfigurationsfragen sehr verwirrend wirken.

Das *Offizielle Red Hat Linux Handbuch Benutzerdefinierte Konfiguration* soll dazu verhelfen, die verschiedenen Konfigurationsmöglichkeiten von Red Hat Linux zu erklären, um spezifische Ziele zu

erreichen. Benutzen Sie dieses Handbuch, um sich mit den verschiedenen Konfigurationsoptionen vertraut zu machen und damit, wie sie umgesetzt werden.

Wenn Sie Software installieren, die nicht im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration* enthalten ist, ist es oft hilfreich zu sehen, was andere Benutzer unter ähnlichen Umständen getan haben. Die HOWTO Dokumente vom Linux Documentation Project, erhältlich unter http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html, dokumentieren bestimmte Aspekte von Linux, von Low-Level Kernel Esoterische Veränderungen bis zum Einsatz von Linux für einen Amateurradiosender.

Dokumentation für Linux-Gurus

Wenn Sie Red Hat Linux schon seit langem benutzen, wissen Sie wahrscheinlich bereits, dass der beste Weg, um ein spezifisches Programm zu verstehen, das Lesen seines Quellcodes und/oder der Konfigurationsverzeichnisse ist. Ein großer Vorteil von Red Hat Linux ist, dass der Quellcode von allen Benutzern gelesen werden kann.

Natürlich ist nicht jeder ein C-Programmierer, daher könnte der Quellcode nicht sehr hilfreich für Sie sein. Wenn Sie jedoch ein wenig Erfahrung hiermit haben, finden Sie im Quellcode die Antworten auf alle Fragen.

Konventionen

Beim Durchlesen dieses Handbuchs wird Ihnen sicherlich auffallen, dass bestimmte Worte verschiedene Schriftarten, Schriftbilder und Größen aufweisen. Diese Hervorhebemethode folgt einer bestimmten Logik: verschiedene Worte sind auf eine bestimmte Weise geschrieben, um in eine spezifische Kategorie eingeschlossen zu werden. Im Folgenden einige Beispiele:

`Befehl`

Linux Befehle (und andere Befehle des Betriebssystems, falls sie verwendet werden) werden auf diese Weise dargestellt. Dieser Stil zeigt Ihnen an, dass Sie das Wort oder die Phrase auf der Befehlszeile eingeben und anschließend die [Eingabetaste] drücken können, um einen Befehl auszuführen. Manchmal enthält ein Befehl Worte, die eigentlich anders geschrieben werden würden (beispielsweise Verzeichnisnamen). In diesen Fällen werden sie als Teil des Befehls angesehen, so dass die gesamte Phrase als Befehl angezeigt wird. Zum Beispiel:

Benutzen Sie den Befehl `Cat Testfile`, um den Inhalt eines Verzeichnisses anzuzeigen, das im laufenden Verzeichnis `Testdatei` heißt.

`Dateinamen`

Dateinamen, Verzeichnisnamen, Pfade und RPM Paketnamen werden auf diese Weise angegeben. Dieser Stil zeigt an, dass eine bestimmte Datei oder ein bestimmtes Verzeichnis mit diesem Namen auf Ihrem Red Hat Linux System existiert. Zum Beispiel:

Die Datei `.bashrc` in Ihrem Home-Verzeichnis enthält Bash Shelldefinitionen und Decknamen für Ihren persönlichen Gebrauch.

Die Datei `/etc/fstab` enthält Informationen über verschiedene Systemgeräte und Dateisysteme.

Das Verzeichnis `/usr/share/doc` enthält die Dokumentation für verschiedene Programme.

Installieren Sie den `Webalizer` RPM, wenn Sie ein Web-Server Log Datei Analyseprogramm benutzen wollen.

Anwendung

Dieser Stil gibt an, dass das genannte Programm eine Endbenutzer-Anwendung ist (im Gegensatz zur System-Software).

Benutzen Sie Netscape Navigator, um das Web zu durchsuchen.

[Taste]

Eine Taste auf der Tastatur ist in diesem Stil hervorgehoben. Zum Beispiel:

Um den Abschluss [Tab] zu benutzen, geben Sie ein Schriftzeichen ein, und drücken Sie die Taste [Tab] . Ihr System gibt die Liste der Dateien im Verzeichnis an, die mit diesem Buchstaben anfangen.

[Taste]-[Kombination]

Eine Kombination von Tasten wird wie folgt dargestellt. Zum Beispiel:

Die Tastenkombination [Strg]-[Alt]-[Backspace] wird das X Window System neu starten.

Text auf einer graphischen Benutzeroberfläche (GUI)

Ein Titel, Wort oder eine Phrase, die auf einem GUI-Bildschirm oder Fenster erscheint, wird auf folgende Weise angezeigt. Wenn Sie einen Text sehen, der in diesem Stil geschrieben ist, so wird er dazu benutzt, einen besonderen GUI-Bildschirm oder ein Element auf einem GUI-Bildschirm zu identifizieren (zum Beispiel ein Text in Verbindung mit einem Kontrollkästchen oder Feld). Zum Beispiel:

Auf dem GNOME-Schirm **Kontrollzentrum** können Sie Ihren GNOME Window-Manager benutzerdefinieren.

Wählen Sie das Kontrollkästchen **Passwort anfordern**, wenn Sie möchten, dass Ihr Bildschirmschoner ein Passwort anfordert, bevor Sie ihn beenden.

Top Level eines Menüs auf einem GUI-Bildschirm oder Fenster

Wenn Sie ein Wort finden, das in diesem Stil geschrieben ist so heißt das, dass das Wort die oberste Stufe eines Pulldown Menüs bildet. Wenn Sie auf das Wort auf dem GUI-Bildschirm klicken, dürfte der Rest des Menüs erscheinen. Zum Beispiel:

Unter **Einstellungen** auf einem GNOME Terminal finden Sie die folgenden Menutitel **Präferenz**, **Rückstellung des Terminals**, **Rückstellen und Löschen** und **Farbwählschalter**.

Wenn Sie eine Reihe von Befehlen in einem GUI-Menü wählen wollen, werden Sie wie im folgenden Beispiel angegeben:

Klicken Sie auf **Programme**=>**Anwendungen**=>**Emacs**, um den Texteditor Emacs zu starten.

Taste auf einem GUI-Bildschirm oder Fenster

Dieser Stil zeigt an, dass Text angezeigt wird, wenn Sie auf eine Schaltfläche des GUI-Bildschirms drücken. Zum Beispiel:

Klicken Sie auf die Taste **Zurück**, um in die Website zurückzugelangen, die Sie zuletzt gesehen haben.

`Computer Output`

Wenn Sie Text in diesem Stil vorfinden, so bedeutet das, dass der Text im Computer auf der Befehlszeile erscheint. Antworten auf von Ihnen eingegebene Befehle, Fehlerbenachrichtigungen und interaktive Prompts werden auf diese Art angezeigt. Zum Beispiel:

Benutzen Sie `ls` um den Inhalt eines Verzeichnisses anzuzeigen.

```
$ ls
Desktop                 axhome           logs          nirvana.gif
Mail                    backupfiles      mail          reports
```

Die Ausgabe, die als Antwort auf den erfolgten Befehl erscheint (in diesem Fall der Inhalt des Verzeichnisses), wird in diesem Stil angezeigt.

`Prompt`

Ein Prompt, mit dem der Computer Sie darauf hinweist, dass er für weitere Einträge bereit ist, wird auf folgende Weise angezeigt. Beispiele:

```
$
```

```
#
```

```
[truk@bleach truk]$
```

```
Leopard Login:
```

`Benutzer Input`

Ein Text, den der Benutzer entweder auf eine Befehlszeile oder in ein Textkästchen auf einem GUI-Bildschirm schreibt, wird wie folgt angezeigt. Im folgenden Beispiel wird **`Text`** in diesem Stil angezeigt:

Um Ihr System in das textbasierte Installationsprogramm zu booten, werden Sie den Befehl **`Text`** in den Prompt `boot:` eingeben müssen.

Ein weiteres Beispiel mit dem Wort **`Root`** als eine Eingabe, die der Benutzer vornimmt:

Wenn Sie sich als Root anmelden müssen, bevor Sie sich in Ihr System einloggen, und wenn Sie den graphischen Anmeldebildschirm verwenden, geben Sie **`Root`** am `Login` Prompt ein. Geben Sie das Root-Passwort am `Passwort` Prompt ein.

Glossar Eingabe

Ein Wort, das im Glossar vorkommt, wird auf diese Weise im Dokument erscheinen. Zum Beispiel:

Das Lpd **Dämon** behandelt Drucknachfragen.

In diesem Fall weist Sie die Art, in der das Wort **Dämon** geschrieben ist, darauf hin, dass die Definition des Wortes im Glossar enthalten ist.

Außerdem werden in diesem Handbuch verschiedene Strategien verwendet, die Ihre Aufmerksamkeit auf bestimmte Argumente lenken. Je nachdem, wie wichtig eine Information für Ihr System ist, werden die diesbezüglichen Anmerkungen mit Bitte beachten, Vorsicht oder Warnung hervorgehoben. Zum Beispiel:

Bitte beachten

Vergessen Sie nicht, dass Linux sehr präzise ist. In anderen Worten ist eine ROSE nicht dasselbe wie eine rOsE.

Führen Sie Routineaufgaben nicht als Rootbenutzer aus — benutzen Sie ein normales Benutzer-Account, es sei denn, Sie benutzen das Root-Account zur Verwaltung Ihres Systems.

WARNUNG

Wenn Sie sich entscheiden, nicht manuell zu partitionieren, wird eine Serverklassen-Installation alle existierenden Partitionen auf allen installierten Festplattenlaufwerken entfernen. Wählen Sie diese Installationsklasse nur dann, wenn Sie sicher sind, dass hier keine wichtigen Daten gespeichert sind.

Verwenden der Maus

Red Hat Linux verwendet eine Maus mit drei Tasten. Wenn Sie eine Maus mit zwei Tasten haben, sollten Sie während dem Installationsprozeß eine Drei-Tasten-Maus emulieren. Wenn Sie dies tun, entspricht das gleichzeitige Drücken beider Maustasten dem Drücken der fehlenden (mittleren) dritten Maustaste.

Wenn Sie in diesem Dokument darauf hingewiesen werden, mit der Maus auf etwas zu klicken, so bedeutet das, dass Sie auf die linke Maustaste klicken müssen. Wenn Sie dagegen die mittlere oder rechte Maustaste drücken sollen, werden Sie ausdrücklich darauf hingewiesen. (Natürlich wird dieser Prozeß umgekehrt wenn Sie Linkshänder sind.)

Der Ausdruck "Drag und Drop" kommt Ihnen vielleicht bekannt vor. Wenn Sie dazu aufgefordert werden, etwas auf ihrem Desktop zu verschieben, müssen Sie darauf klicken und die Maustaste gedrückt halten. Während Sie die Maustaste gedrückt halten, ziehen Sie die Textstelle zu einer neuen Stelle. Wenn Sie an der gewünschten Stelle angekommen sind, lassen Sie die Maustaste los und lassen somit die Textstelle fallen.

Kopieren und Einsetzen von Text mit X

Das Kopieren und Einsetzen von Text mit der Maus und dem X Window System ist ganz einfach. Um Texte zu kopieren, müssen Sie auf die Maustaste drücken und die Maus über den Text ziehen, um die gewünschte Stelle zu markieren. Um den Text an einer bestimmten Stelle einzusetzen, drücken Sie auf die mittlere Maustaste und klicken Sie auf die Lücke, in die der Text eingesetzt werden soll.

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.

Hier könnten wir Ihre Hilfe gebrauchen.

Wir brauchen Ihre Unterstützung!

Wenn Sie Fehler im *Offiziellen Red Hat Linux Referenzhandbuch* entdecken oder Ideen dazu haben, wie das Handbuch verbessert werden könnte, würden wir uns freuen, von Ihnen zu hören! Wenden Sie sich bitte unter folgender Adresse an unser Team: http://bugzilla.redhat.com/bugzilla.

Geben Sie dabei bitte die Kenn-Nummer dieses Handbuchs an:

```
rhl-rg(DE)-7.1-Print-RHI (2001-02-21T10:50-0500)
```

Nur so wissen wir genau, welche Version des Handbuchs Sie vorliegen haben.

Wenn Sie Vorschläge dazu haben, wie das Handbuch verbessert werden kann, seien Sie bitte so präzise wie möglich in der Beschreibung. Wenn Sie einen Fehler gefunden haben, geben Sie bitte den genauen Abschnitt und die Textstelle an, so dass wir den Fehler sofort finden können.

Lassen sie sich registrieren, um den Support nutzen zu können

Wenn Sie über eine offizielle Ausgabe von Red Hat Linux 7.1 verfügen, vergessen Sie nicht, sich registrieren zu lassen, um die Vorteile zu nutzen, die Ihnen als Red Hat Kunde zustehen.

Je nachdem, welches offizielle Red Hat Linux Produkt Sie erworben haben, können Sie einen oder mehrere der folgenden Vorteile nutzen:

- Offizieller Red Hat Support — Das Team für technischen Support von Red Hat, Inc. unterstützt Sie bei Installationsfragen.
- Red Hat Network — Sie können Ihre Pakete leicht aktualisieren und Sicherheitsinformationen erhalten, mit denen Sie Ihr System individuell anpassen können. Weitere Informationen hierüber finden Sie unter http://www.redhat.com/network
- Zugriff auf den Priority FTP-Server — Keine Besuche mehr auf hoffnungslos überlasteten Mirror Sites spät in der Nacht. Die Besitzer von Red Hat Linux 7.1 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.
- *Under the Brim: Die offiziellen Red Hat E-Newsletter* — Sie erhalten die neuesten Nachrichten und Produktinformationen jeden Monat direkt von Red Hat.

Wenn Sie sich registrieren lassen wollen, steht Ihnen die folgende Adresse zur Verfügung: http://www.redhat.com/apps/activate. Sie finden Ihre persönliche Produkt-ID auf einer rotweißen Karte in Ihrer offiziellen Red Hat Linux Packung.

Wenn Sie mehr über den technischen Support von Red Hat Linux wissen möchten, lesen Sie den Anhang *Technischen Support erhalten* im *Offiziellen Red Hat Linux Installationshandbuch*.

Viel Glück, und vielen Dank, dass Sie Red Hat Linux gewählt haben!

Ihr Red Hat Dokumentationsteam

Teil I Das System

1 Struktur des Dateisystems

1.1 Warum eine gemeinsame Struktur?

Die Struktur des Dateisystems ist die niedrigste organisatorische Stufe eines Betriebssystems. Die Art und Weise, mit der ein Betriebssystem mit seinen Benutzern, seinen Anwendungen und seinem Sicherheitsmodell interagiert, hängt davon ab, wie es die Dateien in einem primären Speichergerät (gewöhnlich ein Festplattenlaufwerk) speichert. Es ist aus zahlreichen Gründen sehr wichtig, dass Benutzern und Programmen bei der Installation und danach zum Lesen der Binärdateien, der Konfiguration, des Protokolls und anderen notwendigen Dateien eine gemeinsame Basis zur Verfügung steht.

Ein Dateisystem kann als zwei verschiedene logische Dateikategorien betrachtet werden:

- Gemeinsam genutzte und nicht gemeinsam genutzte Dateien
- Variable und statische Dateien

Gemeinsam nutzbare Dateien sind Dateien, auf die verschiedene Rechner zugreifen können, während **nicht gemeinsam nutzbare** Dateien für andere Rechner nicht zur Verfügung stehen. **Variable** Dateien können jederzeit ohne das (aktive oder passive) Zutun des Systemadministrators geändert werden, während **statische** Dateien, beispielsweise Dokumentation und Binärdateien, ohne Eingriff des Systemadministrators unverändert bleiben.

Der Grund für eine solche Klassifizierung der Dateien ist in der Art Berechtigung für das Verzeichnis zu suchen, in dem sich diese Dateien befinden. Die Art, wie das Betriebssystem und seine Benutzer die Dateien verwenden, bestimmt das Verzeichnis, wo sie abgelegt werden - und zwar unabhängig davon, ob das Verzeichnis schreibgeschützt gemountet wird oder nicht - und die Zugriffsstufe, die für jede Datei zugelassen ist. Besonders wichtig ist die höchste Stufe dieser Organisation, da der Zugriff auf die darunter liegenden Verzeichnisse eingeschränkt werden kann oder sich Sicherheitsprobleme ergeben können, wenn diese Stufe nicht organisiert oder strukturlos ist.

Eine Struktur allein hat jedoch nur als Standardstruktur Sinn, denn konkurrierende Strukturen können mehr Probleme bereiten als lösen. Aus diesem Grund hat sich Red Hat Linux für die am meisten verbreitete Dateisystemstruktur entschieden und diese nur etwas erweitert, um sie an spezielle, innerhalb von Red Hat Linux verwendete Dateien anzupassen.

1.2 Überblick über Filesystem Hierarchy Standard (FHS)

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 Speicherstellen

vieler Dateien und Verzeichnisse festgelegt sind. Unser Unternehmen wird sich auch weiterhin nach diesem Standard richten, damit Red Hat Linux ihn auch in Zukunft erfüllt.

Das aktuelle FHS-Dokument ist die maßgebende Referenz für alle FHS-konformen Dateisysteme, wobei der Standard jedoch viele Bereiche undefiniert oder erweiterbar lässt. 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 sind sicherlich 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.

1.2.1 FHS-Organisation

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.

`/dev`-Verzeichnis

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

`/etc`-Verzeichnis

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.

/lib-Verzeichnis

Das Verzeichnis /lib sollte nur jene Bibliotheken enthalten, die für das Ausführen der Binärdateien in /bin und /sbin gebraucht werden. Diese gemeinsam benutzten Bibliothek-Images sind insbesondere für das Booten des Systems und das Ausführen von Befehlen innerhalb des Root-Dateisystems von Bedeutung.

/mnt-Verzeichnis

Das /mnt-Verzeichnis bezieht sich auf zeitweilig gemountete Dateisysteme wie CD-ROMs und Disketten.

/opt-Verzeichnis

Das Verzeichnis /opt liefert einen Bereich für die Speicherung von großen und statischen Software-Paketen.

Für Pakete, die es vermeiden möchten, ihre Dateien über das Dateisystem abzulegen, bietet /opt ein logisches und vorhersehbares organisatorisches System unter dem Verzeichnis dieses Pakets. Für den Systemadministrator bedeutet dies eine einfache Art und Weise, die Rolle jeder Datei innerhalb eines bestimmten Pakets zu bestimmen.

Wenn zum Beispiel ein bestimmtes Software-Pakte in /opt den Namen sample besitzt, dann können alle zugehörigen Dateien in Verzeichnisse innerhalb von /opt/sample abgelegt werden (z.B. /opt/sample/bin für Binärdateien und /opt/sample/man für man-Seiten).

Große Pakete, die zahlreiche Unterpakete umfassen, die jeweils verschiedene Aufgaben erfüllen, werden in /opt positioniert, so dass das große Paket eine standardmäßige Organisation erhält. Das sample-Paket kann auf diese Weise verschiedene Tools in eigenen Unterverzeichnissen besitzen - beispielsweise /opt/sample/tool1 und /opt/sample/tool2, die wiederum ihre eigenen Verzeichnisse wie bin - man u.ä. aufweisen.

/sbin-Verzeichnis

Das Verzeichnis /sbin enthält die ausführbaren Dateien, die nur vom Rootbenutzer verwendet werden und ausschließlich dem Booten und Mounten von /usr sowie Wiederherstellungsvorgängen dienen. Laut FHS gilt:

> "/sbin enthält gewöhnlich Dateien, die zum Booten des Systems unerlässlich sind, sowie Binärdateien in /bin. Jede nach dem Mounten von /usr verwendete ausführbare Datei (sofern keine Probleme aufgetreten sind) muss in /usr/sbin und die lokalen Systemverwaltungsdateien in /usr/local/sbin abgelegt werden."

Die folgenden Programme sollten sich in /sbin befinden:

```
arp, clock, getty, halt, init, fdisk,
```

```
fsck.*, ifconfig, lilo, mkfs.*, mkswap, reboot,
route, shutdown, swapoff, swapon, update
```

/usr-Verzeichnis

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
  |- bin
  |- doc
  |- etc
  |- games
  |- include
  |- kerberos
  |- lib
  |- libexec
  |- local
  |- man
  |- sbin
  |- share
  |- src
  |- X11R6
```

Das Verzeichnis `bin` enthält ausführbare Dateien, `doc` enthält nicht FHS-Dokumentation, `etc` enthält Konfigurationsdateien für das gesamte System, `games` ist für Spiele reserviert, `include` enthält C-Header-Dateien, `kerberos` enthält Binärdateien und vieles mehr für Kerberos, und `lib` enthält Objektdateien und Bibliotheken, die nicht konzipiert wurden, um direkt von Benutzern oder Shell-Skripten verwendet zu werden. Das Verzeichnis `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, `src` ist für den Quellcode reserviert und `X11R6` ist für das X Window System gedacht (XFree86 in Red Hat Linux).

/usr/local-Verzeichnis

Laut FHS gilt:

> "Die Hierarchie `/usr/local` kann vom Systemadministrator für die Installation lokaler Software benutzt werden. Bei der Aktualisierung der Systemsoftware 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
```

`/var`-Verzeichnis

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
  |- arpwatrch
  |- cache
  |- db
  |- ftp
  |- gdm
  |- kerberos
  |- 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
    |- www
    |- yp
```

Systemprotokolldateien wie `wtmp` und `lastlog` werden im Verzeichnis `/var/log` abgelegt. Das Verzeichnis `/var/lib` enthält auch die RPM-Systemdatenbanken. LOCK-Dateien werden in `/var/lock` abgelegt. Das Verzeichnis `/var/spool` enthält Unterverzeichnisse, in denen verschiedene Systeme Datendateien speichern können.

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

1.3 `/proc` und seine "Dateien"

Das Verzeichnis `/proc` enthält spezielle "Dateien", die Informationen mit dem Kernel austauschen.

Das Verzeichnis `/proc` ist sehr viel leistungsfähiger als anfänglich erscheinen mag. Über die verschiedenen hier abgelegten "Dateien" (die nicht wirkliche Dateien sind, sondern Schnittstellen zum Kernel darstellen) kann der Systemadministrator `/proc` ganz einfach auf Informationen über den Status des Kernels, die Systemattribute, den Status der einzelnen Prozesse usw. zugreifen. Durch die Verwendung von `cat` in Kombination mit den Schnittstellen von `/proc` haben Sie unmittelbar Zugriff auf eine Vielzahl von Informationen über jedes System. Wenn Sie zum Beispiel erfahren möchten, wie die Speicherregister derzeit auf Ihrem Computer zugewiesen sind:

```
[truk@tictactoe /proc]$ cat iomem
00000000-0009fbff : System RAM
0009fc00-0009ffff : reserved
000a0000-000bffff : Video RAM area
000c0000-000c7fff : Video ROM
000f0000-000fffff : System ROM
00100000-07ffffff : System RAM
  00100000-002553d7 : Kernel code
  002553d8-0026d91b : Kernel data
e0000000-e3ffffff : VIA Technologies, Inc. VT82C597 [Apollo VP3]
e4000000-e7ffffff : PCI Bus #01
  e4000000-e4003fff : Matrox Graphics, Inc. MGA G200 AGP
  e5000000-e57fffff : Matrox Graphics, Inc. MGA G200 AGP
e8000000-e8ffffff : PCI Bus #01
  e8000000-e8ffffff : Matrox Graphics, Inc. MGA G200 AGP
ea000000-ea00007f : Digital Equipment Corporation DECchip 21140
  ea000000-ea00007f : eth0
ffff0000-ffffffff : reserved
[truk@tictactoe /proc]$
```

Oder Sie können (was nützlicher ist) den folgenden Befehl verwenden, wenn Sie sich mit einem unbekannten Rechner verbinden und dessen CPU-Typ und Geschwindigkeit erfahren möchten:

```
cat /proc/cpuinfo
```

Weitere wertvolle Systeminformationen finden Sie u.a. unter `cmdline`, `meminfo`, `partitions` und `version`.

Die Verzeichnisse in `/proc` enthalten eine Reihe an Informationen über eine bestimmte Anwendung oder einen besonderen Prozess. In `/proc/sys/kernel` finden Sie zum Beispiel zahlreiche Angaben über den Kernel, darunter die maximale Anzahl an geketteten Dateien (`threads-max`) oder die Höchstzahl an Meldungen (`msgmax`).

1.4 Spezielle Speicherstellen von Dateien bei Red Hat Linux

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

Die von Red Hat Linux gelieferten Konfigurationstools 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, jedoch auch von Linuxconf, einem Tool des Control Panels, oder einem anderen Konfigurationstool konfiguriert werden. Im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration* finden Sie Anweisungen für den Gebrauch von Linuxconf.

2 Benutzer und Gruppen

Benutzer und **Gruppen** werden vom Kern der Red Hat Linux System-Administration kontrolliert.

Benutzer können sowohl tatsächliche Personen sein (Zugriffe, die an einen bestimmten Benutzer gebunden sind) als auch logische Benutzer (Zugriffe für Anwendungen, um bestimmte Aufgaben erledigen zu können). Beide Benutzer-Typen haben eine **Benutzer-ID** und **Gruppen-ID**. Benutzer-IDs sind üblicherweise einzigartig (müssen es aber nicht sein).

Gruppen sind immer ein logischer Ausdruck der Organisation. Die Benutzer bilden Gruppen, die die Grundlage der miteinander verbundenen Benutzer darstellen und ihnen die Berechtigung zum Lesen, Schreiben und Ausführen einer Datei erteilt.

Jede Datei wird bei ihrer Erstellung einem Benutzer oder einer Gruppe zugewiesen. Darüber hinaus wird dem Dateiinhaber, der zugeordneten Gruppe und allen Benutzern dieses Rechners die Berechtigung zum Lesen, Schreiben und Ausführen zugewiesen. Die Benutzer und Gruppen einer bestimmten Datei und die Berechtigungen für diese Datei können durch den Rootbenutzer geändert werden oder, mit weniger Aufwand, vom Ersteller der Datei.

Die Verwaltung von Benutzern und Gruppen sowie das Zuweisen und Widerrufen von Berechtigungen ist eine der wichtigsten Aufgaben der System-Administratoren. Red Hat Linux erleichtert diese Aufgabe unter Beibehaltung der Sicherheit der Dateien des Rechners.

2.1 Tools für die Verwaltung von Benutzern und Gruppen

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

Sie können den Befehl `useradd` verwenden, um vom Shell-Prompt aus einen neuen Benutzer zu erstellen. Am besten lassen sich Benutzer und Gruppen mit Linuxconf verwalten (Details über Linuxconf finden Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*).

2.2 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 2.4, *Benutzereigene Gruppen*.

Tabelle 2–1 Standardbenutzer

Benutzer	UID	GID	Home-Directory	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	
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 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

Gruppe	GID	Mitglieder
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	
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	

2.4 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. Beim Erstellen eines neuen Benutzers wird diesem standardmäßig eine eigene Gruppe zugeordnet. Hier das Prinzip:

Benutzereigene Gruppen

Jeder Benutzer hat eine 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 bisher 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 *devel*, bei dem viele Benutzer die Dateien im Verzeichnis *devel* bearbeiten.Erstellen Sie eine Gruppe mit der Bezeichnung `devel`, fügen Sie das Verzeichnis `devel` (`chgrp devel`) und alle Benutzer des Projekts der Gruppe `devel` hinzu.

Mit Linuxconf können Sie einen Benutzer zu einer Gruppe hinzufügen (siehe *Offizielles Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*). Wenn Sie für die Erstellung einer Gruppe lieber die Befehlszeile verwenden, geben Sie den Befehl `/usr/sbin/groupadd` *`Gruppenname`*. Mit dem Befehl `/usr/bin/gpasswd -a` *`loginname groupname`* wird ein *Login-Name* eines Benutzers zu eine Gruppe hinzugefügt (in den man-Seiten `groupadd` und `gpasswd` finden Sie mehr Informationen über diese Optionen). Die Datei `/etc/group` enthält Informationen über die Gruppen Ihres Sytems.

Wenn Sie die Gruppe `devel` erstellt haben, Benutzer zu der Gruppe `devel` hinzugefügt haben, die Gruppe für das Verzeichnis `devel` in der Gruppe `devel` geändert haben und das setgid-Bit für das Verzeichnis `devel` eingerichtet haben, können alle Benutzer die Dateien `devel` bearbeiten und neue Dateien im Verzeichnis `devel` erstellen. Diese Dateien sind dauerhaft der Gruppe `devel` zugeordnet und können daher jederzeit von anderen Benutzern desselben Projekts bearbeitet werden.

Wenn die Benutzer an mehreren Projekten wie *devel* 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.

2.4.1 Grundprinzip der benutzereigenen Gruppen

Obwohl UPGs nicht ganz neu in Red Hat Linux 7.1 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.
- Erstellen Sie zuerst eine `emacs` Gruppe:

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

  Geben Sie als Nächstes

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

  ein, um den Inhalt des Verzeichnisses mit der `emacs` Gruppe zu verbinden und die richtigen Benutzer der Gruppe hinzuzufügen:

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

- 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 soweit 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.
- 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.

3 Bootprozess, Init und Shutdown

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

3.1 Einführung

Einige der wichtigsten Elemente in Bezug auf die Leistungsfähigkeit von Red Hat Linux sind das flexible Starten und Herunterfahren des Betriebssystems, in das das System spezifische Programme mithilfe ihrer besonderen Konfigurationen herunterlädt, sowie die Möglichkeit, zwecks Kontrolle des Bootprozesses diese Konfigurationen zu ändern, und das abschließende organisierte Herunterfahren des Systems. Während andere Betriebssysteme prinzipiell den Bootvorgang kontrollieren oder keine Möglichkeit zu einer benutzerdefinierten Konfiguration des Herunterfahrens bieten, erlaubt Ihnen Red Hat Linux den vollen Zugriff auf jeden einzelnen Schritt in diesem Prozess.

Abgesehen von der Kontrolle des Startens oder Herunterfahrens unterstützt Red Hat Linux den Benutzer dabei, die genaue Ursache der meisten Probleme im Rahmen dieser beiden Prozesse herauszufinden, die dabei erläutert werden. Das Verständnis dieser Vorgänge ist auch im Sinne der allgemeinen Fehlerbehebung von großem Nutzen.

3.2 Hintergrundwissen für den Bootprozess

Bitte beachten

In diesem Kapitel wird insbesondere der Bootprozess des Systems x86 beschrieben. Je nach Architektur Ihres Systems kann der entsprechende Bootprozess leicht von den hier beschriebenen Vorgängen abweichen. Nachdem der Kernel gefunden und vom System geladen wurde, verläuft der standardmäßige Bootprozess von Red Hat Linux jedoch in allen Systemarchitekturen auf die gleiche Weise. Weitere Informationen über das Starten des x86-Systems finden Sie unter Abschnitt 3.8, *Differenzen im Bootprozess bei anderen Architekturen*.

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) und sucht anschließend auf der Festplatte. Die Reihenfolge der zum Booten verwendeten Laufwerke wird gewöhnlich durch eine bestimmte BIOS-Einstellung vorgegeben. Nachdem Red Hat Linux auf einer Festplatte installiert wurde, sucht das BIOS einen **Master Boot Record** (MBR), der im ersten Sektor der ersten Festplatte beginnt, speichert den Inhalt 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 LILO, und LILO übernimmt den Prozess (wenn er auf dem MBR installiert wurde). In der standardmäßigen Konfiguration von Red Hat Linux verwendet LILO die MBR-Einstellungen, um die Bootoptionen anzuzeigen, und ermöglicht es dem Benutzer anzugeben, welches Betriebssystem effektiv gestartet werden soll.

An dieser Stelle ergibt sich die Frage: woher weiß LILO, was zu tun ist, wenn der MBR gelesen wurde? Antwort: LILO hat die Anweisungen bereits mithilfe von `lilo` mit der Konfigurationsdatei `/etc/lilo.conf` gelesen.

3.2.1 Optionen in `/etc/lilo.conf`

In den meisten Fällen wird es nicht notwendig sein, den MBR auf Ihrer Festplatte zu ändern, es sei denn, Sie müssen ein neu installiertes Betriebssystem booten oder einen neuen Kernel verwenden. Wenn Sie mithilfe von LILO und mit einer anderen Konfiguration einen neuen Kernel erstellen müssen, bearbeiten Sie `/etc/lilo.conf` und führen Sie erneut `lilo` aus.

WARNUNG

Wenn Sie `/etc/lilo.conf` bearbeiten möchten, sollten Sie eine Backup-Kopie erstellen, bevor Sie Änderungen vornehmen. Versichern Sie sich darüber hinaus, über eine funktionierende Diskette zu verfügen, so dass Sie das System booten und den MBR verändern können, wenn ein Problem auftreten sollte. Weitere Informationen finden Sie auf den man-Seiten über `mkbootdisk`.

`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 erste IDE-Festplatte). Eine Beispieldatei für `/etc/lilo.conf` sieht wie folgt aus:

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
```

```
prompt
timeout=50
message=/boot/message
lba32
default=linux

image=/boot/vmlinuz-2.4.0-0.43.6
 label=linux
 initrd=/boot/initrd-2.4.0-0.43.6.img
 read-only
 root=/dev/hda5

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

Dieses Beispiel zeigt ein System, das konfiguriert wurde, um zwei Betriebssysteme zu booten: Red Hat Linux und DOS. Im Folgenden eine nähere Betrachtung einiger Zeilen dieser Datei (Ihre Datei `/etc/lilo.conf` sieht eventuell ein wenig anders aus):

- `boot=/dev/hda` weist LILO an, auf der ersten Festplatte auf dem ersten IDE-Controller zu suchen.
- `map=/boot/map` lokalisiert die Map-Datei und sollte nicht geändert werden.
- `install=/boot/boot.b` weist LILO an, die angegebene Datei als neuen Boot-Sektor zu installieren und sollte nicht geändert werden. Wenn die Zeile `install` fehlt, nimmt LILO standardardmäßig `/boot/boot.b` als zu verwendende Datei an.
- `prompt` weist LILO an anzuzeigen, was sich in der Zeile `message` befindet. Es wird nicht empfohlen, die Zeile `message` zu entfernen. Sollten Sie dies dennoch tun, können Sie in jedem Fall ein Prompt aufrufen, wenn Sie die Taste [Shift] drücken, während Ihr Rechner bootet.
- `timeout=50` stellt das Zeitlimit ein, während dessen der Benutzer Eingaben vornehmen kann, bevor LILO die Zeile `default` bootet. Die Zeitüberschreitung wird in Zehntelsekunden gemessen und ist standardmäßig auf 50 eingestellt.
- `message=/boot/message` gibt den den Bildschirm an, den LILO zur Auswahl des zu bootenden Kernels oder Betriebssystems anzeigt.
- `lba32` gibt LILO die Geometrie der Festplatte an. Ein weiterer häufiger Eintrag an dieser Stelle ist `linear`. Sie sollten diese Zeile nur dann verändern, wenn Sie sich ganz sicher sind. Andernfalls besteht das Risiko, dass Ihr System nicht booten kann.
- `default=linux` gibt LILO an, welches Betriebssystem von den unterhalb dieser Zeile aufgelisteten Optionen Optionen gebootet werden soll. In diesem Fall steht der der Name `linux` in der Zeile `label`, die für jede Bootoption zur Verfügung steht.

- `image=/boot/vmlinuz-2.4.0-0.43.6` gibt den Linux-Kernel an, der mit dieser Bootoption gebootet werden soll.
- `label=linux` bezeichnet die Betriebssystemoption auf dem LILO-Bildschirm. In diesem Fall handelt es sich auch um den Namen, der in der Zeile `default` angegeben ist.
- `initrd=/boot/initrd-2.4.0-0.43.6.img` bezieht sich auf das **initial ram disk** Image, das beim Booten des Kernels verwendet wird, um die hierzu benötigten Geräte zu initialisieren und zu starten. Die initiale Ramdisk enthdlt eine Sammlung von rechnerspezifischen Geräten, die für das Funktionieren der Festplatte und aller Geräte für das Laden des Kernels erforderlich sind. Sie sollten es in jedem Fall vermeiden, initiale Ramdisks für verschiedene Rechner zu verwenden, es sei denn, sie besitzen dieselbe Hardware-Konfiguration (aber selbst in diesem Fall ist es nicht empfehlenswert).
- `read-only` gibt an, dass die Root-Partition (siehe Zeile `root` unten) schreibgeschützt ist und damit nicht geändert werden kann.
- `root=/dev/hda5` gibt LILO die Partition an, die als Root-Partition verwendet werden soll.

LILO zeigt anschließend den Red Hat Linux Einstiegsbildschirm mit den verschiedenen Betriebssystemen oder Kerneln, für die er konfiguriert wurde. Wenn Sie ausschließlich Red Hat Linux installiert haben und in `/etc/lilo.conf` nichts geändert haben, wird nur linux als Option angezeigt. Wenn Sie LILO auf zum Booten eines anderen Betriebssystems konfiguriert haben, dann können Sie in diesem Bildschirm das System wählen, das Sie booten möchten. Markieren Sie es mithilfe der Pfeiltasten und drücken Sie die [Eingabetaste].

Wenn Sie ein Prompt für die Eingabe von Befehlen für LILO zur Verfügung haben möchten, drücken Sie die Tastenkombination [Ctrl]-[X]. LILO zeigt das `LILO:` Prompt auf dem Bildschirm und lässt Ihnen eine voreingestellte Zeitspanne, um Eingaben vorzunehmen (diese Zeitspanne wird in der Zeile `timeout` in der Datei `/etc/lilo.conf` eingestellt). Wurde `/etc/lilo.conf` so eingestellt, dass mehrere Betriebssysteme angezeigt werden, können Sie an dieser Stelle die Kennung für das Betriebssystem eingeben, das Sie booten möchten.

Beim Booten von Linux bootet LILO zuerst den Kernel, bei dem es sich um eine `vmlinuz`-Datei (plus Versionsnummer, z.B. `vmlinuz-2.4.0-xx`) handelt, die sich im Verzeichnis `/boot` befindet. Dann übernimmt der Kernel den weiteren Bootprozess.

Linux ist an diesem Punkt bereits gestartet, wenn auch auf einem noch sehr einfachen Niveau. Ohne Anwendungen, die den Kernel verwenden, und ohne die Möglichkeit für den Benutzer, sinnvolle Eingaben in das System vorzunehmen, ist Linux noch nicht funktionstüchtig. Das Programm `init` löst dieses Problem, indem es all die Dienste liefert, die es dem System ermöglichen, seine Funktionen auszuführen.

3.2.2 Init

Der Kernel sucht `init` in `/sbin` und startet die Ausführung. `init` übernimmt den weiteren Bootprozess.

Init startet alle Prozesse Ihres Linux-Systems (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`, um den Netzwerkprozess u zu initialisieren. Die meisten Systeme verwenden eine Uhr. In diesem Fall verwendet `rc.sysinit` die Datei `/etc/sysconfig/clock`, um die Uhr zu initialisieren. Außerdem wird `rc.serial` ausgeführt, falls Sie über serielle Port-Prozesse verfügen, die initialisiert werden müssen.

Init wertet anschließend die Datei `/etc/inittab` aus, die beschreibt, wie das System auf jedem **Runlevel** einzurichten ist, und legt das Standard-Runlevel fest (unter Abschnitt 3.4, *Init Runlevels* finden Sie weitere Informationen über init-Runlevels). Diese Datei legt u.a. fest, dass `/sbin/update` beim Start eines Runlevels ausgeführt werden muss. Das Programm `update` gibt fehlerhafte Buffer auf der Festplatte wieder frei.

Sobald sich das Runlevel ändert, verwendet `init` die Skripten in `/etc/rc.d/rc` um verschiedene Dienste wie zum Beispiel Ihren Web-Server, den DNS-Server etc. zu starten und anzuhalten. Zuerst legt `init` 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. Anschließend bestimmt `init` das aktuelle und das vorige Runlevel.

Die Datei `init` startet alle Hintergrundprozesse, die für die Ausführung des Systems erforderlich sind, und sucht nach einem passenden rc-Verzeichnis für dieses Runlevel (`/etc/rc.d/rc`*<x>*`.d`, wobei das *<x>* eine Zahl zwischen 0 und 6 sein kann). `init` beendet alle kill-Skripten (ihr Dateiname beginnt mit einem K). Dann initialisiert es alle start-Skripten (ihr Dateiname beginnt mit einem S) im geeigneten Runlevel-Verzeichnis (so dass alle Dienste und Anwendungen korrekt gestartet werden). Sie können diese Skripten nach dem Booten des Systems auch manuell mit einem Befehl wie `/etc/rc.d/init.d/httpd stop` oder `service httpd stop` und als Root ausführen. Auf diese Weise wird der `httpd` Server gestoppt.

Bitte beachten

Wenn Sie Dienste manuell starten, sollten Sie sich als Root anmelden. Tritt ein Fehler beim Ausführen von `service httpd stop` auf, besteht vielleicht kein `/sbin`-Pfad in `/root/.bashrc` (oder die korrekte `.rc`-Datei für Ihre bevorugte Shell). In diesem Fall können Sie entweder den vollständigen Befehl `/sbin/service httpd stop` eingeben oder in Ihrer `.rc`-Shell `export PATH="$PATH:/sbin"` hinzufügen. Wenn Sie die Konfigurationsdatei Ihrer Shell bearbeiten, müssen Sie sich abmelden und anschließend als Root wieder anmelden, um die geänderte Shell- Konfiguration anzuwenden.

Keiner der Skripten, die die Dienste starten und stoppen, befindet in `/etc/rc.d/init.d`. Alle Dateien in `/etc/rc.d/rc<x>.d` sind **symbolische Links**, die auf Skripten in `/etc/rc.d/init.d` zeigen. Ein symbolischer Link ist nichts anderes als eine Datei, die auf eine andere Datei zeigt. Sie werden in diesem Fall verwendet, da sie erstellt und gelöscht werden können, ohne sich auf das Skript auszuwirken, das den Dienst startet oder stoppt. Die symbolischen Links zu den verschiedenen Skripten sind in einer bestimmten Reihenfolge nummeriert, um in dieser Reihenfolge gestartet zu werden. Sie können die Reihenfolge, in der die Dienste gestartet oder gestoppt werden, ändern, indem Sie den Namen des symbolischen Links ändern, der sich auf das Skript bezieht, das den Dienst startet oder stoppt. Weiterhin ist es möglich, symbolischen Links dieselbe Nummer wie anderen symbolischen Links zu geben, wenn Sie möchten, dass der entsprechende Dienst unmittelbar vor oder nach einem anderen Dienst gestartet oder gestoppt wird.

Beispiel für Runlevel 5: `init` sucht im Verzeichnis `/etc/rc.d/rc5.d` und stellt Folgendes fest (Ihr System und Ihre Konfiguration entsprechen diesem Beispiel vielleicht nicht ganz):

```
K01pppoe -> ../init.d/pppoe
K05innd -> ../init.d/innd
K10ntpd -> ../init.d/ntpd
K15httpd -> ../init.d/httpd
K15mysqld -> ../init.d/mysqld
K15pvmd -> ../init.d/pvmd
K16rarpd -> ../init.d/rarpd
K20bootparamd -> ../init.d/bootparamd
K20nfs -> ../init.d/nfs
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwalld -> ../init.d/rwalld
K20rwhod -> ../init.d/rwhod
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
```

```
K30mcserv -> ../init.d/mcserv
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K50snmpd -> ../init.d/snmpd
K54pxe -> ../init.d/pxe
K55routed -> ../init.d/routed
K60mars-nwe -> ../init.d/mars-nwe
K61ldap -> ../init.d/ldap
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
K75gated -> ../init.d/gated
K80nscd -> ../init.d/nscd
K84ypserv -> ../init.d/ypserv
K90ups -> ../init.d/ups
K96irda -> ../init.d/irda
S05kudzu -> ../init.d/kudzu
S06reconfig -> ../init.d/reconfig
S08ipchains -> ../init.d/ipchains
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13portmap -> ../init.d/portmap
S14nfslock -> ../init.d/nfslock
S18autofs -> ../init.d/autofs
S20random -> ../init.d/random
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
S35identd -> ../init.d/identd
S40atd -> ../init.d/atd
S45pcmcia -> ../init.d/pcmcia
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S60lpd -> ../init.d/lpd
S75keytable -> ../init.d/keytable
S80isdn -> ../init.d/isdn
S80sendmail -> ../init.d/sendmail
S85gpm -> ../init.d/gpm
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
```

```
S90FreeWnn -> ../init.d/FreeWnn
S90xfs -> ../init.d/xfs
S95anacron -> ../init.d/anacron
S97rhnsd -> ../init.d/rhnsd
S99linuxconf -> ../init.d/linuxconf
S99local -> ../rc.local
```

Diese symbolischen Links weisen `init` an, Folgendes zu stoppen: `pppoe`, `innd`, `ntpd`, `httpd`, `mysqld`, `pvmd`, `rarpd`, `bootparamd`, `nfs`, `rstatd`, `rusersd`, `rwalld`, `rwhod`, `squid`, `amd`, `mcserv`, `yppasswdd`, `dhcpd`, `smb`, `vncserver`, `arpwatch`, `named`, `snmpd`, `pxe`, `routed`, `mars-nwe`, `ldap`, `kadmin`, `kprop`, `krb524`, `krb5kdc`, `gated`, `nscd`, `ypserv`, `ups`, and `irda`. Nachdem alle Prozesse geschlossen wurden, kontrolliert `init` im gleichen Verzeichnis und sucht nach Startskripten für `kudzu`, `reconfig`, `ipchains`, `portmap`, `nfslock`, `autofs`, `random`, `netfs`, `apmd`, `identd`, `atd`, `pcmcia`, `sshd`, `rawdevices`, `xinetd`, `lpd`, `keytable`, `isdn`, `sendmail`, `gpm`, `canna`, `crond`, `FreeWnn`, `xfs`, `anacron`, `rhnsd`, and `linuxconf`. Die letzte Aktion von `init` ist es, `/etc/rc.d/rc.local` zu starten, um alle speziellen Skripten auszuführen, die für diesen Host konfiguriert wurden. Das System läuft nun auf Runlevel 5.

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). `getty` öffnet tty-Zeilen, stellt die Modi ein, gibt das Anmelde-Prompt aus, stellt den Benutzernamen fest und initialisiert anschließend den Anmeldeprozess für diesen Benutzer. Auf diese Weise können sich die Benutzer authentifizieren und das System benutzen.

`/etc/inittab` weist `init` an, was zu tun ist, wenn der Benutzer die Tastenkombination [Strg]-[Alt]-[Entf] auf drückt. Da Red Hat Linux korrekt heruntergefahren und unmittelbar neu gestartet werden sollte, wird `init` angewiesen, in solchen Fällen den Befehl `/sbin/shutdown -t3 -r now` auszuführen. Darüber hinaus bestimmt `/etc/inittab`, was `init` im Falle eines Stromausfalls tun soll, wenn Ihr System mit einer UPS-Einheit verbunden ist.

Auf Runlevel 5 führt `/etc/inittab` ein Skript mit dem Namen `/etc/X11/prefdm` aus. Das `prefdm` führt den gewünschten X-Desktop-Manager (`gdm`, wenn Sie GNOME verwenden, `kdm`, wenn Sie sich für KDE entscheiden, oder `xdm`, wenn Sie AnotherLevel benutzen) entsprechend dem Inhalt des Verzeichnisses `/etc/sysconfig/desktop` aus.

Nun sollte ein Anmelde-Prompt erscheinen. Und der gesamte Prozess benötigte nur wenige Sekunden.

3.2.3 SysV Init

Init wird beim Booten vom Kernel ausgeführt. Es ist für das Starten aller normalen Prozesse verantwortlich, die beim Booten ausgeführt werden müssen: die 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`, `rc.local`, `rc.sysinit` und die folgenden Verzeichnisse:

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

SysV init stellt jedes init-Runlevel mit einem eigenen Verzeichnis dar und verwendet hierzu `init` und symbolische Links in jedem Verzeichnis, um die Dienste zu starten und anzuhalten, wenn das System von einem Runlevel auf einen anderen übergeht.

Die Ereigniskette eines SysV-init-Bootvorgangs kann wie folgt kurz zusammengefasst werden:

- Der Kernel sucht `init` in `/sbin`.
- `init` führt die `/etc/rc.d/rc.sysinit` Datei aus.
- `rc.sysinit` bearbeitet die meisten Bootloader-Prozesse und führt anschließend `rc.serial` (wenn vorhanden) aus.
- `init` führt alle Dateien für den Standardrunlevel aus.
- `init` führt `/etc/rc.d/rc.local` aus.

Der Standardrunlevel wird in `/etc/inittab` bestimmt. Im oberen Teil des Bildschirms sollte eine Zeile erscheinen, die ungefähr wie folgt aussieht:

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

In diesem Beispiel gilt Standardrunlevel 3 (die Nummer nach der ersten Spalte). Wenn Sie das Level ändern möchten, können Sie `/etc/inittab` manuell bearbeiten. Gehen Sie hierbei jedoch sehr sorgfältig vor. Sollte trotzdem ein Fehler auftreten, können Sie das System mithilfe der Tastenkombination [Strg]-[X] neu starten und am `boot:` Prompt Folgendes eingeben:

```
boot:  linux single
```

Auf diese Weise *sollten* Sie in der Lage sein, den Einzelbenutzermodus zu booten, so dass Sie `inittab` wieder auf den vorherigen Wert einstellen können.

Im Folgenden werden die Informationen in den Dateien in `/etc/sysconfig` bearbeitet, die die Parameter bestimmen, die von den verschiedenen Systemdiensten beim Starten verwendet werden.

3.3 Sysconfig Informationen

Die folgenden Informationen beziehen sich auf die verschiedenen Dateien in `/etc/sysconfig` sowie ihre Funktionen und ihren Inhalt. Die hier beschriebenen Angaben erheben keinen Anspruch auf Vollständigkeit, da viele der Dateien eine Reihe Optionen besitzen, die nur in sehr spezifischen Fällen verwendet werden.

3.3.1 Dateien in `/etc/sysconfig`

Die folgenden Dateien befinden sich gewöhnlich in `/etc/sysconfig`:

- `amd`
- `apmd`
- `authconfig`
- `cipe`
- `clock`
- `desktop`
- `firewall`
- `harddisks`
- `hwconf`
- `i18n`
- `init`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`
- `network`
- `pcmcia`
- `rawdevices`

- `sendmail`
- `soundcard`
- `ups`
- `vncservers`

Möglicherweise fehlen einige dieser Dateien in Ihrem System, wenn die entsprechenden Programme, die sie verwenden, nicht installiert sind.

Im Folgenden wird jede Datei einzeln betrachtet.

`/etc/sysconfig/amd`

Die Datei `/etc/sysconfig/amd` enthält verschiedene Parameter, die von `amd` verwendet werden und das automatische Mounten und Unmounten von Dateisystemen ermöglichen.

`/etc/sysconfig/apmd`

Die Datei `/etc/sysconfig/apmd` wird von `apmd` verwendet um zu erfahren, 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. `apm` ist ein Dämon mit Kontrollfunktion, der im Linux-Kernel einen APM-Code verwendet und Sie zum Beispiel darauf hinweist, wenn die Batterie entladen ist, falls Sie einen Laptop-Computer verwenden.

`/etc/sysconfig/authconfig`

Die Datei `/etc/sysconfig/authconfig` legt die Authorisierungsart fest, die auf dem Rechner verwendet werden soll, und enthält eine oder mehrere der folgenden Zeilen:

- `USEMD5=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` einer der folgenden Werte ist:
  - `yes` — MD5 wird zur Authentifizierung verwendet.
  - `no` — MD5 wird nicht zur Authentifizierung verwendet.

- `USEKERBEROS=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` einer der folgenden Werte ist:
  - `yes` — Kerberos wird zur Authentifizierung verwendet.
  - `no` — Kerberos wird nicht zur Authentifizierung verwendet.

- `USELDAPAUTH=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` einer der folgenden Werte ist:

- yes — LDAP wird zur Authentifizierung verwendet.
- no — LDAP wird nicht zur Authentifizierung verwendet.

/etc/sysconfig/cipe

Die Datei /etc/sysconfig/cipe konfiguriert cipe beim Starten.

Es können Werte wie im folgenden Beispiel enthalten sein:

- DEVICE=eth0 gibt den Netzadapter an, den cipe verwenden wird.
- PORT=9999 gibt die UDP-Port-Nummer an, die von cipe an beiden Gegenstellen verwendet wird.
- PEER=0.0.0.0 gibt die effektive Adresse der fernen cipe-Gegenstelle an. Sie können diese Adresse dynamisch konfigurieren, indem Sie den Wert auf 0.0.0.0 einstellen.
- IPADDR=0.0.0.0 gibt die virtuelle Adresse am lokalen Ende des cipe-Tunnels an.
- PTPADDR=0.0.0.0 gibt die virtuelle Adresse am fernen Ende des cipeTunnels an.

/etc/sysconfig/clock

Die Datei /etc/sysconfig/clock legt fest, wie die Werte der Systemuhr interpretiert werden sollen. In früheren Red Hat Linux Versionen wurden die folgenden Werte verwendet (in dieser Version bitte nicht mehr verwenden):

- CLOCKMODE=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - GMT — zeigt an, dass die Uhr auf UTC (oder auch GMT) eingestellt ist.
  - ARC — zeigt (nur bei Alpha- basierten Systemen) an, dass der 42-Jahre-Zeitoffset der ARC-Konsole wirksam ist.

In neueren Versionen gelten die folgenden Werte:

- UTC=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - true — zeigt an, dass die Uhr auf UTC eingestellt ist. Jeder andere Wert stellt die Uhr auf die lokale Zeit.
- ARC=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - true — zeigt (nur bei Alpha-basierten Systemen) an, dass der 42-Jahre-Zeitoffset der ARC-Konsole wirksam ist. Jeder andere Wert stellt die Uhr auf die 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, zum Beispiel:

```
DESKTOP="GNOME"
```

/etc/sysconfig/firewall

Die Datei `/etc/sysconfig/firewall` enthält verschiedenen Firewalleinstellungen. Diese Datei wird standardmäßig erstellt, ist jedoch leer.

/etc/sysconfig/harddisks

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

WARNUNG

Nehmen Sie in dieser Datei keine Änderungen vor. Wenn Sie die hier gespeicherten Standardwerte ändern, besteht das Risiko, dass Sie alle Daten Ihrer Festplatte verlieren.

Die Datei `/etc/sysconfig/harddisks` kann Folgendes enthalten:

- `USE_DMA=1`, der Wert 1 aktiviert DMA. Bei einigen Chipsätzen und Festplattenkombinationen kann dies jedoch zu Datenverlusten führen. *Lesen Sie in der Dokumentation Ihrer Festplatte nach oder wenden Sie sich an den Hersteller, bevor Sie diesen Befehl aktivieren.*
- `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. kudzu findet und konfiguriert neue bzw. geänderte Hardware-Komponenten. Die Datei /etc/sysconfig/hwconf darf nicht verändert werden. Wenn Sie diese Datei bearbeiten, kann es passieren, dass manche Geräte plötzlich als *hinzugefügt* oder *entfernt* angezeigt werden.

/etc/sysconfig/i18n

Die Datei /etc/sysconfig/i18n stellt die Standardsprache ein, zum Beispiel:

```
LANG="en_US"
```

/etc/sysconfig/init

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

Folgende Werte können verwendet werden:

- BOOTUP=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - BOOTUP=color stellt die standardmäßige Bildschirmdarstellung beim Systemstart dar, wobei der Erfolg oder das Fehlschlagen von Geräten und Diensten beim Booten in verschiedenen Farben angezeigt wird.
  - BOOTUP=verbose erzeugt eine Bildschirmdarstellung im herkömmlichen Stil, die mehr Informationen liefert als nur eine Meldung des Erfolgs oder Fehlschlagens des Bootvorgangs.
  - Alle übrigen Werte erzeugen eine neue Bildschirmdarstellung ohne ANSI-Formatierung.

- RES_COL=<*Wert*>, wobei <*Wert*> die Nummer der Spalte des Bildschirms ist, wo Statuskennungen beginnen. Die Standardeinstellung ist 60.
- MOVE_TO_COL=<*Wert*>, wobei <*Wert*> den Cursor auf RES_COL bewegt. Die Standardeinstellung ist die Ausgabe von ANSI-Sequenzen durch echo -e.
- SETCOLOR_SUCCESS=<*Wert*>, wobei <*Wert*> 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=<*Wert*>, wobei <*Wert*> 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=<*Wert*>, wobei <*Wert*> 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=<*Wert*>, wobei <*Wert*> die Farbe auf 'normal' einstellt. Die Standardeinstellung ist die Ausgabe von ANSI-Sequenzen durch echo -e.
- LOGLEVEL=<*Wert*>, wobei <*Wert*> 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.
- PROMPT=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - yes — Aktiviert die Key-Überprüfung für den interaktiven Modus.
  - no — Deaktiviert die Key-Überprüfung für den interaktiven Modus.

/etc/sysconfig/irda

Die Datei /etc/sysconfig/irda prüft, wie Infrarot-Geräte auf Ihrem System beim Starten konfiguriert sind.

Folgende Werte können verwendet werden:

- IRDA=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - yes — irattach wird ausgeführt, der regelmäßig überprüft, ob irgendeine Komponente versucht, sich mit dem Infrarot-Port zu verbinden: zum Beispiel ein anderer Notebook-Computer, der versucht, eine Netzwerkverbindung herzustellen. Wenn Sie Infrarot- Geräte verwenden möchten, muss diese Zeile auf yes eingestellt werden.
  - no — irattach wird nicht ausgeführt und keine entsprechende Meldung angezeigt.

- DEVICE=<*Wert*>, wobei <*Wert*> das Gerät (normalerweise ein serieller Port) ist, das Infrarot-Verbindungen verwendet.
- DONGLE=<*Wert*>, wobei <*Wert*> gibt die Art Dongle an, die für die Infrarot-Kommunikation verwendet wird. Diese Einstellung ist für die Benutzer wichtig, die serielle Dongles statt eigentliche Infrarot- Ports verwenden. Ein Dongle ist ein Gerät, das mit einem traditionellen seriellen Port verbunden ist, um über Infrarot zu kommunizieren. Diese Zeile wird standardmäßig auskommentiert, da Notebook-Computer mit Infrarot-Ports sehr viel herkömmlicher sind als Computer mit hinzugefügten Dongles.
- DISCOVERY=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:

  - yes — Startet irattach im Modus Discovery, d.h. der Befehl prüft nach anderen Infrarot-Geräten. Der Befehl muss aktiviert werden, damit das System nach einer Infrarot-Verbindung sucht.
  - no — Startet irattach nicht im Modus Discovery.

/etc/sysconfig/keyboard

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

- 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.
- KEYTABLE=<*Datei*>, wobei <*Datei*> der Name der keytable-Datei ist. Beispiel: KEYTABLE="us". Die Dateien, die als keytable-Dateien verwendet werden können, beginnen in /usr/lib/kbd/keymaps/i386 und verzweigen von hier zu verschiedenen Tastatur-Layouts, die alle die Kennung <*Datei*> besitzen. Die erste Datei unter /usr/lib/kbd/keymaps/i386, die mit der KEYTABLE-Einstellung übereinstimmt, wird verwendet.

/etc/sysconfig/kudzu

Die Datei /etc/sysconfig/kudzu ermöglicht Ihnen beim Booten mithilfe von kudzu eine sichere Prüfung Ihrer System-Hardware. Bei einer sicheren Prüfung handelt es sich um eine Prüfung, die den seriellen Port und die Prüfung des DDC-Monitors deaktiviert.

- SAFE=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - yes — kuzdu führt eine sichere Prüfung aus.
  - no — kuzdu führt eine normale Prüfung aus.

/etc/sysconfig/mouse

Die Datei /etc/sysconfig/mouse wird verwendet, um Informationen über die verfügbare Maus anzugeben. Die folgenden Werte können verwendet werden:

- FULLNAME=<*Wert*>, wobei sich <*Wert*> auf den vollen Namen der Mausart, die verwendet wird, bezieht.
- MOUSETYPE=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - microsoft — Microsoft- Maus.

  - `mouseman` — MouseMan- Maus.
  - `mousesystems` — Mouse Systems-Maus.
  - `ps/2` — PS/2-Maus.
  - `msbm` — Microsoft-Bus- Maus.
  - `logibm` — Logitech- Bus-Maus.
  - `atibm` — ATI-Bus- Maus.
  - `logitech` — Logitech- Maus.
  - `mmseries` — eine ältere MouseMan-Maus.
  - `mmhittab` — mmhittab- Maus.

- `XEMU3=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` einer der folgenden Werte ist:
  - `yes` — Die Maus besitzt nur zwei Tasten, es sollten jedoch drei Tasten emuliert werden..
  - `no` — Die Maus besitzt bereits drei Tasten.

- `XMOUSETYPE=<`*`Wert`*`>`, wobei sich `<`*`Wert`*`>` auf die Art Maus bezieht, die auf X verwendet wird. Die hier aufgeführten Optionen entsprechen den `MOUSETYPE`-Einstellungen dieser Datei.

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=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` einer der folgenden Werte ist:
  - `yes` — Das Netzwerk soll konfiguriert werden.
  - `no` — Das Netzwerk soll nicht konfiguriert werden.

- `HOSTNAME=<`*`Wert`*`>`, wobei als `<`*`Wert`*`>` der **Vollständige Domänenname** (**FQDN, Fully Qualified Domain Name**), zum Beispiel `hostname.domain.com`, angegeben werden muss. Sie können aber auch jeden gewünschten Rechnernamen eintragen.

Bitte beachten

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

- `GATEWAY=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` die IP-Adresse für das Netzwerk-Gateway ist.
- `GATEWAYDEV=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` der Gerätename ist, z.B. `eth0`.
- `NISDOMAIN=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` 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=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` einer der folgenden Werte sein kann:
  - `yes` — Die PCMCIA-Unterstützung soll aktiviert werden.
  - `no` — Die PCMCIA-Unterstützung soll nicht aktiviert werden.

- `PCIC=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` einer der folgenden Werte ist:
  - `i82365` — Der Computer verfügt über einen Chipsatz mit i82365-PCMCIA-Steckplatz.
  - `tcic` — Der Computer verfügt über einen Chipsatz mit tcic-PCMCIA- Steckplatz.

- `PCIC_OPTS=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` die Timing-Parameter für den Steckplatztreiber angibt (i82365 oder tcic).
- `CORE_OPTS=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` die Liste der `pcmcia_core`-Optionen ist.
- `CARDMGR_OPTS=<`*`Wert`*`>`, wobei `<`*`Wert`*`>` die Liste der Optionen für den PCMCIA-Kartenmanager `cardmgr` ist (zum Beispiel `-q` für den Modus 'quiet mode' und `-m` für die Suche nach ladbaren Kernelmodulen im angegebenen Verzeichnis usw.). Weitere Informationen finden Sie in der man-Seite zu `cardmgr`.

/etc/sysconfig/rawdevices

Die Datei /etc/sysconfig/rawdevices wird verwendet, um Rawdevice-Verbindungen zu konfigurieren. Beispiel:

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

/etc/sysconfig/sendmail

Die Datei /etc/sysconfig/sendmail ermöglicht das Versenden von Nachrichten an einen oder mehrere Empfänger, wobei die Nachrichten je nach Erfordernis 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 ein Mal für den Fall, dass Nachrichten zurückgesendet wurden.

Folgende Werte können verwendet werden:

- DAEMON=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - yes — sendmail soll konfiguriert werden, um Port 25 auf eingehende Mails abzufragen. yes bedeutet die Verwendung der -bd-Optionen von sendmail.
  - 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. Informationen über die Soundkartenkonfiguration finden Sie in der Datei /etc/modules.conf.

Folgende Werte können enthalten sein:

- CARDTYPE=<*Wert*>, wobei <*Wert*> zum Beispiel als CARDTYPE=SB16 für eine Soundkarte Soundblaster 16 angegeben wird.

/etc/sysconfig/ups

Die Datei /etc/sysconfig/ups wird verwendet, um Informationen über jegliche Geräte zur **Kontinuierlichen Stromversorgung** (**UPS, Uninterruptable Power Supplies**) Ihres Systems anzugeben. Dies ist für das Red Hat Linux System sehr wertvoll, da das System auch im Falle von Stromausfall korrekt heruntergefahren werden kann. Die folgenden Werte können verwendet werden:

- SERVER=<*Wert*>, wobei <*Wert*> einer der folgenden Werte sein kann:
  - yes — Ein UPS-Gerät ist mit Ihrem System verbunden.
  - no — Kein UPS-Gerät ist mit Ihrem System verbunden.

- MODEL=<*Wert*>, wobei <*Wert*> einer der folgenden Werte sein muss oder auf NONE eingestellt werden muss, wenn kein UPS mit Ihrem System verbunden ist:
  - apcsmart — Für ein APC Smart-UPS oder ein ähnliches Gerät.
  - fentonups — Für ein Fenton-UPS.
  - optiups — Für ein OPTI-UPS.
  - bestups — Für ein Best Power-UPS.
  - genericups — Für ein generisches UPS-Gerät.
  - ups-trust425+625 — Für ein Trust-UPS.

- DEVICE=<*Wert*>, wobei <*Wert*> angibt, wo das UPS-Gerät verbunden ist, zum Beispiel /dev/ttyS0.
- OPTIONS=<*Wert*>, wobei <*Wert*> ein Sonderbefehl ist, der dem UPS-Gerät übergeben werden muss.

/etc/sysconfig/vncservers

Die Datei /etc/sysconfig/vncservers konfiguriert, wie der **Virtual Network Computing oder VNC**-Server startet. Bei VNC handelt es sich um ein System zur Remote-Anzeige, mit der Sie eine Bildschirmumgebung nicht nur auf dem zugehörigen Rechner anzeigen können, sondern auch über verschiedene Netzwerke (von LAN bis Internet), wobei eine Vielfalt von Rechnerarchitekturen verwendet werden kann.

Folgende Werte können verwendet werden:

- `VNCSERVERS=<`*`Wert`*`>`, wobei <*Wert*> zum Beispiel wie folgt eingestellt wird: `"1:root"`.

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

In der Regel enthält `/etc/sysconfig/network-scripts` die folgenden Dateien, wobei <*if-Name*> den Namen der Network-Interface darstellt:

- `/etc/sysconfig/network-scripts/ifup`
- `/etc/sysconfig/network-scripts/ifdown`
- `/etc/sysconfig/network-scripts/network-functions`
- `/etc/sysconfig/network-scripts/ifcfg-<`*`if-Name`*`>`
- `/etc/sysconfig/network-scripts/ifcfg-<`*`if-Name`*`>-<`*`clone-Name`*`>`
- `/etc/sysconfig/network-scripts/chat-<`*`if-Name`*`>`
- `/etc/sysconfig/network-scripts/dip-<`*`if-Name`*`>`
- `/etc/sysconfig/network-scripts/ifup-post`

Es folgt eine Beschreibung der einzelnen Dateien.

`/etc/sysconfig/network-scripts/ifup` und `/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: das Programm, das die Netzwerkverwaltungsskripte anweist, ein

SIGIO-Signal an den Prozess zu senden (der `netreport` aufgerufen hat) sobald sich der Netzwerkschnittstellenstatus ändert.

`/etc/sysconfig/network-scripts/ifcfg-<`*`if-Name`*`>` und `/etc/sysconfig/network-scripts/ifcfg-<`*`if-Name`*`>:<`*`clone-Name`*`>`

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. Bei beiden ist es erforderlich, einen `<`*`if-Name`*`>` (Name einer Netzwerkschnittstelle) anzugeben. 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 physischen Geräts ist (mit Ausnahme von dynamisch eingerichteten PPP-Geräten, bei denen hier der "logische Name" eingetragen wird).
- `IPADDR=<`*`addr`*`>`, wobei `<`*`addr`*`>` die IP-Adresse ist.
- `NETMASK=<`*`mask`*`>`, wobei `<`*`mask`*`>` der Wert für die Netzmaske ist.
- `NETWORK=<`*`addr`*`>`, wobei `<`*`addr`*`>` die Netzwerkadresse ist.
- `BROADCAST=<`*`addr`*`>`, wobei `<`*`addr`*`>` die Broadcast-Adresse ist.
- `GATEWAY=<`*`addr`*`>`, wobei `<`*`addr`*`>` die Gateway-Adresse ist.
- `ONBOOT=<`*`answer`*`>`, wobei `<`*`answer`*`>` einer der folgenden Werte ist:
  - `yes` — Dieses Gerät soll beim Systemstart aktiviert werden.
  - `no` — Dieses Gerät soll beim Systemstart nicht aktiviert werden.
- `USERCTL=<`*`answer`*`>`, wobei `<`*`answer`*`>` einer der folgenden Werte sein 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=<`*`proto`*`>`, wobei `<`*`proto`*`>` einer der folgenden Werte sein 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=<answer>`, wobei `<answer>` einer der folgenden Werte sein 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 Leistungsgeschwindigkeit des Modems ist (z.B. "`115200`").
- `DEFABORT=<answer>`, wobei `<answer>` einer der folgenden Werte sein 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-<if-Name>`

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/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.

3.4 Init Runlevels

Das Konzept hinter der Ausführung von verschiedenen Diensten auf verschiedenen Runlevels ist, dass verschiedene Systeme auf verschiedene Weise verwendet werden können. Einige Dienste können solange nicht verwendet werden, wie sich das System in einem bestimmten Status oder **Modus** befindet, zum Beispiel für mehr als einen Benutzer betriebsbereit ist, oder aber mit einem Netzwerk verbunden

ist. Sie könnten das System beispielsweise in einem niedrigen Modus laufen lassen (Prüfen eines Netzwerkproblems auf Runlevel 2 oder das Beenden des Systems auf Runlevel 3, ohne dass X ausgeführt wird). In diesen Fällen hat es keinen Sinn, Dienste auszuführen, die von einem höheren Systemmodus abhängen, da die Ausführung nicht korrekt verlaufen würde. Indem Sie für jeden Dienst festlegen, dass er gestartet wird, sobald der entsprechende Runlevel erreicht ist, gewährleisten Sie ein korrektes Starten und können den Rechnermodus ändern, ohne dabei beachten zu müssen, welche Dienste manuell gestartet oder gestoppt werden müssen.

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

Der standardmäßige Runlevel für das Booten und Herunterfahren eines Systems ist in `/etc/inittab` konfiguriert. Weitere Informationen über `/etc/inittab` finden Sie in Abschnitt 3.2.3, *SysV Init*.

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.

3.5 Initscript-Dienstprogramme

Das Dienstprogramm `chkconfig` in `/sbin` 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` in `/usr/sbin`, das im Gegensatz zur befehlszeilenorientierten Oberfläche von `chkconfig` sicherlich benutzerfreundlicher ist. Für beide Dienstprogramme sollten Sie als Root angemeldet sein.

Weitere Informationen finden Sie in den man-Seiten von `chkconfig` und `ntsysv`.

3.6 Ausführen von Programmen beim Systemstart

Die Datei `/etc/rc.d/rc.local` wird beim Systemstart von `init` 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. Dieses Skript kann eine Vielzahl von `setserial`-Befehlen ausführen, um die seriellen Ports des Systems zu konfigurieren. Weitere Informationen finden Sie auf der man-Seite von `setserial`.

Die Standarddatei `/etc/rc.d/rc.local` erstellt ein Login-Meldung mit Ihrer Kernelversion und Ihrem Rechnertyp.

3.7 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:

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

Sie müssen sich als Root anmelden, um den Befehl `shutdown` auszuführen. 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 in der Lage sind, `shutdown` aufzurufen, 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.

WARNUNG

Wenn Ihr Rechner nicht selbst herunterfährt, sollten Sie Ihn trotzdem nicht ausschalten, bis eine Meldung erscheint, die Sie darüber informiert, dass das System angehalten hat oder vollständig heruntergefahren ist.

Wenn Sie nicht auf die Anzeige dieser Meldung warten, laufen Sie die Gefahr, dass das Unmounten der Festplattenpartitionen unterbrochen wird. Dies kann das Dateisystem beschädigen und auch dazu führen, dass Ihr System beim nächsten Mal nicht bootet. Haben Sie daher beim Herunterfahren des Systems ein wenig Geduld.

3.8 Differenzen im Bootprozess bei anderen Architekturen

Jede von Red Hat Linux gestützte Computerarchitektur startet das Betriebssystem auf eine andere Weise. Nachdem der Red Hat Linux Kernel den Bootprozess eingeleitet und ihn an `init` übergeben hat, folgen jedoch weitere Schritte, die für jede Systemarchitektur gelten. Der einzige Unterschied besteht in der Art, wie Red Hat Linux den Kernel sucht, um ihn zu laden und den Befehl `init` zu starten.

Detaillierte Informationen über die verschiedenen Bootmethoden finden Sie in den Anleitungen zur Installation der verschiedenen Architekturen.

4 Lightweight Directory Access Protocol (LDAP)

4.1 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 wie ein Telefonbuch betrachtet. LDAP kann auch andere Informationen verarbeiten, doch wird es derzeit 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 Server** (**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 die gleiche 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 andernfalls 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 Rechenleistungen 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.

4.2 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. Derzeit sind jedoch nur 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.

4.3 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 auf dem neuesten Stand halten. (siehe Abschnitt 4.11, *Zusätzliche Ressourcen*).

LDAP ist ein offenes, konfigurierbares Protokoll, es kann fast alle Informationen im Zusammenhang mit bestimmten Organisationsstrukturen speichern.

4.3.1 LDAP Anwendungen

Einige LDAP-Client Anwendungen stehen für eine sehr vereinfachte Anzeige und das Ändern von LDAP Informationen zur Verfügung:

- LDAP Browser/Editor — Ein benutzerfreundliches Tool, 100% in Java geschrieben, für den einfachen Einsatz zwischen verschiedenen Plattformen. Er steht unter http: //www.iit.edu/~gawojar/ldap zur Verfügung
- GQ — Ein GTK-basierter LDAP- Client, erhältlich bei der Red Hat Linux 7.1 Distribution oder unter http://biot.com/gq
- kldap — Ein LDAP-Client für das KDE Projekt, erhältlich unter http://www.mountpoint.ch/oliver/kldap

4.3.2 LDAP und PAM

LDAP kann als Authentifikations-Service per `pam_ldap` Modul verwendet werden. LDAP wird häufig als zentraler Authentifikationsservice verwendet. Somit haben Benutzer ein einheitliches Login, das Konsolen-Logins, POP-Server, IMAP-Server, mit dem Netzwerk (das SAMBA verwendet) verbundene Computer und auch Computer mit Windows NT/2000 umfasst. Bei der Verwendung von LDAP können sich alle diese Login-Situationen auf eine Benutzer-ID und Passwort-Kombination beziehen und die Administration erheblich vereinfachen. Das `pam_ldap` Modul ist in `nss_ldap` Paket enthalten.

4.4 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:

```
[<eindeutiger Name>]
dn: <Distinguished Name>
<Attributtyp>: <Attributwert>
<Attributtyp>: <Attributwert>
<Attributtype>: <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.

Ihre *<Attributtyp>* und *<Attributwert>* Paare *müssen* in einem Schema definiert sein, bevor sie verwendet werden können. Sie können sie nicht einfach in einer LDIF-Datei definieren und dann erwarten, dass ein LDAP-Server diese Informationen benutzen kann, wenn er keine entsprechenden Daten in seinen Schemadateien besitzt.

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.

4.5 OpenLDAP 2.0 Erweiterungen

OpenLDAP 2.0 ist das Hauptupgrade für die Anwendung und beinhaltet:

- *LDAPv3 Support* — Arbeitet jetzt mit SASL, TLS und SSL sowie mit anderen Verbesserungen und entspricht vollständig RFC 2251-2256. Die vielen Änderungen von LDAPv2 wurden durchgeführt, um LDAP zu einem sichereren Protokoll zu machen.
- *IPv6 Support* — Unterstützt nun die nächste Internet-Protokoll Generation.
- *LDAP über IPC* — OpenLDAP kann innerhalb eines bestimmten Systems kommunizieren, ohne über das Netzwerk gehen zu müssen, um es sicherer zu machen.
- *Updated C API* — Verbessert für Programmierer die Verbindung und Verwendung der Anwendung.
- *LDIFv1 Support* — Entspricht vollständig dem LDAP Data Interchange Format (LDIF) Version 1.
- *Verbesserter Stand-Alone LDAP Server* — Enthält ein aktualisiertes Zugriff-Kontroll-System, eine Thread-Gruppe, bessere Tools und vieles mehr.

4.6 OpenLDAPDateien

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  schema
ldapfilter.conf  ldaptemplates.conf    slapd.conf
```

4.6.1 Bearbeiten/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=edu"
```

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 ist zu ändern von:

```
rootdn          "cn=root, dc=ihre domäne, dc=com"
```

in einen Eintrag wie dem folgenden:

```
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 7.1).

4.6.2 Das Schema Verzeichnis

Neu an der OpenLDAP Version 2 ist, dass das `schema` Verzeichnis die verschiedenen LDAP Definitionen beinhaltet, die zuvor in den Dateien `slapd.at.conf` und `slapd.oc.conf` abgelegt waren. Alle **Attributsyntaxdefinitionen** und **Objektklassendefinitionen** sind jetzt in den unterschiedlichen Schemadateien abgelegt. Die verschiedenen Schemadateien sind ein Teil von `/etc/openldap/slapd.conf`, das die `include` Zeilen wie im folgenden Beispiel angezeigt verwendet: angezeigt:

```
include  /etc/openldap/schema/core.schema
include  /etc/openldap/schema/cosine.schema
include  /etc/openldap/schema/inetorgperson.schema
include  /etc/openldap/schema/nis.schema
include  /etc/openldap/schema/rfc822-MailMember.schema
include  /etc/openldap/schema/autofs.schema
include  /etc/openldap/schema/kerberosobject.schema
```

Sie sollten keines der Schemata aus den Schemadateien, die von OpenLDAP installiert wurden, ändern.

Sie können die von OpenLDAP verwendeten Schemata erweitern, um zusätzliche Attributtypen und Objektklassen, die die Schemadateien standardmäßig verwenden, zu unterstützen. Erstellen Sie dafür eine `local.schema` Datei im Verzeichnis `/etc/openldap/schema`. Stellen Sie einen Bezug zwischen diesem neuen Schema und der `slapd.conf` Datei her, indem Sie die folgende Zeile zu Ihren standardmäßigen `include` Schemazeilen hinzufügen:

```
include  /etc/openldap/schema/local.schema
```

Weisen Sie anschließend Ihre neuen Attributtyen und Objektklassen der `local.schema` Datei zu. Viele Organisationen verwenden die standardmäßig installierten Attributtypen und Objektklassen der Schemadateien und modifizieren diese für die Verwendung in der `local.schema` Datei. Das kann Ihnen helfen, die Schemasysnatx zu verstehen, während Sie gleichzeitig die unmittelbaren Voraussetzungen Ihrer Organisation erfüllen.

Das Erweitern der Schemata zum Vergleichen bestimmter spezieller Anforderungen ist ziemlich komplex und übersteigt den Umfang dieses Kapitels. Weitere Informationen über die Erstellung neuer Schemata erhalten Sie unter http://www.openldap.org/doc/admin/schema.html

4.7 OpenLDAP Dämonen und Dienstprogramme

Das Paket OpenLDAP enthält zwei Dämonen: `slapd` und `slurpd`.

Der Dämon `slapd` ist ein autonomer LDAP-Dämon, den Sie zum Ausführen des LDAP-Supports verwenden.

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:

- `ldapmodify` — Dient zum Ändern von Einträgen in eine LDAP-Datenbank und zum Annehmen von Eingaben per Datei oder Standardeingaben.
- `ldapadd` — Dient zum Hinzufügen von Einträgen zu Ihrem Verzeichnis und Annehmen von Eingaben per Datei oder Standardeingaben. `ldapadd` ist eigentlich ein Hardlink mit `ldapmodify -a`.
- `ldapsearch` — Dient zum Suchen nach Einträgen im LDAP-Verzeichnis unter Verwendung des Shell-Prompts.
- `ldapdelete` — Dient zum Löschen von Einträgen aus dem LDAP-Verzeichnis und Annehmen von Eingaben per Datei oder Shell-Prompt.

Alle diese Dienstprogramme sind für den Fall, dass Änderungen in einer Datei vorzunehmen sind, einfacher anzuwenden. Ausnahme ist das Dienstprogramm `ldapsearch`, bei dem alle Befehle einzeln einzugeben sind. Alle jeweiligen man-Seiten zeigen die Syntax dieser Dateien.

Zum Importieren oder Exportieren von Informationsblöcken mit einem `slapd` Verzeichnis oder um ähnliche administrative Tasks durchzuführen, werden verschiedene Dienstprogramme benötigt, die unter `/usr/sbin` abgelegt sind:

- `slapadd` — Fügt Eingaben von einer LDIF- Datei in ein LDAP-Verzeichnis ein. Zum Beispiel den Befehl `/usr/sbin/slapadd -l`*`ldif`* ausführen, wo die LDIF-Datei *`ldif`* angezeigt wird, die die neuen Engaben enthält.
- `slapcat` — Entnimmt Einträge aus dem LDAP- Verzeichnis und speichert sie in einer LDIF-Datei. Zum Beispiel den Befehl `/usr/sbin/slapcat -l`*`ldif`* ausführen, wo die LDIF-Datei angezeigt wird, die die Einträge aus dem LDAP-Verzeichnis enthält.
- `slapindex` — Erstellt den Index der `slapd` Datenbank auf der Grundlage des Inhalts der aktuellen Datenbank neu.

- `slappasswd` — Erstellt ein Benutzerpasswort für die Verwendung des Befehls `ldapmodify` oder der Datei `rootpw` in der Datei `/etc/openldap/slapd.conf`. Führen Sie den Befehl `/usr/sbin/slappasswd` aus, um das Passwort zu erstellen.

WARNUNG

Stellen Sie sicher, dass `slapd` unterbrochen wird, bevor `slapadd`, `slapcat` oder `slapindex` ausgeführt werden. Andernfalls besteht ein Risiko für die Konsistenz Ihrer Datenbank.

Weitere Informationen zu diesen Dienstprogrammen finden Sie auf den jeweiligen man-Seiten.

4.8 Module zum Hinzufügen von zusätzlichen Funktionen zu LDAP

Red Hat Linux enthält einige 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.

4.9 LDAP How To (Bedienungsanleitung): kurzer Überblick

Dieser Abschnitt gibt einen kurzer Überblick 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/doc/admin/ quickstart.html — Beginnen Sie mit "Edit the configuration file", da die Dateien bereits installiert sind, oder mit LDAP Linux HOWTO (http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html). In diesen Dokumentationen werden weitere Schritte beschrieben.

3. Passen Sie die Datei `slapd.conf` an Ihr System an. Weitere Informationen für das Bearbeiten der Datei `slapd.conf` erhalten Sie unter Abschnitt 4.6.1, *Bearbeiten `/etc/openldap/slapd.conf`*

4. Zum Starten von `slapd` geben Sie `/etc/rc.d/init.d/ldap start` ein. (Nachdem Sie LDAP korrekt konfiguriert haben, sollten Sie zum Starten des Systems Linuxconf oder `ntsysv` benutzen.)

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.

4.10 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 umfassendere Dokumentation, als wir Ihnen hier bieten können. Weitere Informationen finden Sie in den in Abschnitt 4.11, *Zusätzliche Ressourcen* angegebenen Literaturhinweisen.

4.10.1 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`.

4.10.2 Anpassen der Konfigurationsdateien

Anpassen von /etc/openldap/slapd.conf

Bearbeiten Sie anschließend die Datei `slapd.conf` um sicherzustellen, dass sie mit den Angaben Ihrer Organisation übereinstimmen.

Unter Abschnitt 4.6.1, *Bearbeiten/etc/openldap/slapd.conf* finden Sie weitere Anweisungen für das Anpassen der Datei `slapd.conf` .

Edit ldap.conf

Die Datei `ldap.conf` ist in `/etc` und `/etc/openldap` auf den LDAP-Servern und -Clients abgelegt.

Passen Sie die Konfigurationsdatei `/etc/ldap.conf` an die `nss_ldap` Datei und `pam_ldap`an, um Ihre Organisation widerzuspiegeln und die Basis zu finden. Die Datei `/etc/openldap/ldap.conf` ist die Konfigurationsdatei für Befehlszeilentools wie z.B. `ldapsearch`, `ldapadd` usw. Sie muss ebenfalls an Ihre LDAP- Einstellungen angepasst werden. Für Client-Rechner müssen beide Dateien modifiziert werden.

Edit /etc/nsswitch.conf

Wenn Sie `nss_ldap` verwenden möchten, müssen Sie `ldap` in die entsprechenden Felder von `/etc/nsswitch.conf` einfügen. (Bearbeiten Sie diese Dateien sehr vorsichtig. Sie sollten sicher wissen, was Sie durchführen wollen, z.B).

```
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 Kapitel 8, *Pluggable Authentication Modules (PAM)* und/oder auf den man-Seiten zu PAM.)

4.10.3 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";
```

einen Eintrag in der Form:

```
$DEFAULT_MAIL_DOMAIN = "your_company.com";
```

Die Standardannahme muss ebenfalls geändert werden von:

```
$DEFAULT_BASE = "dc=padl,dc=com";
```

in einen Eintrag der Form:

```
$DEFAULT_BASE = "dc=your_company,dc=com";
```

Nun müssen Sie sich entscheiden, welches Skript verwendet werden soll. Die folgende Tabelle hilft Ihnen bei Ihrer Entscheidung:

Tabelle 4–1 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`
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`.

4.11 Zusätzliche Ressourcen

Es sind viele nützliche, LDAP betreffende Informationen erhältlich, zum Beispiel im Internet. Sie sollten diese Quellen nutzen, insbesondere die OpenLDAP -Website und die LDAP HOWTOs, bevor Sie LDAP in Ihrem System konfigurieren.

4.11.1 Installationsdokumentation

- Auf der `ldap` man-Seite erhalten Sie Informationen über LDAP. Für die verschiedenen LDAP-Dämonen und -Dienstprogramme gibt es ebenfalls man-Seiten. Wenn Sie mehr Informationen über `ldapmodify`, `ldapsearch` und andere benötigen, schauen Sie auf den man-Seiten nach.
- `/usr/share/docs/openldap-`*`Versionnummer`* — Enthält allgemeine `README` Dokument- und sonstige Informationen.

4.11.2 Hilfreiche Websites

- http://www.openldap.org — Die wichtigste Seite des OpenLDAP-Projekts: Der gemeinschaftliche Versuch eine "robuste", kommerzielle Open-Source-LDAP-Suite von Anwendungen und Entwicklungstools zu erstellen.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — LDAP Linux HOWTO Dokument; Informiert über die Installation durch Authentifikation und Logging.
- http://www.padl.com — Für Entwickler von `nss_ldap` und `pam_ldap` und anderer hilfreicher LDAP Tools.
- http://www.innosoft.com/ldapworld — Enthält Informationen bezüglich der Spezifikationen von LDAP RFC und LDAP Version 3.
- http://www.kingsmountain.com/ldapRoadmap.shtml — Jeff Hodges' LDAP Road Map enthält Links für verschiedene FAQs und aktuelle Neuigkeiten über das LDAP Protokoll.
- http://www.rudedog.org/auth_ldap — In `auth_ldap` finden Sie Authentifikationsmodule für Apache.
- http://www.stanford.edu/~bbense/Inst.html — Behandelt die Verwendung von LDAP mit Sendmail.
- http://www.webtechniques.com/archives/2000/05/wilcox — Ein hilfreicher Einblick in das Verwalten von Gruppen in LDAP.
- http://www.ldapman.org/articles — Artikel zur Einführung in LDAP einschließlich Methoden zur Erstellung eines Verzeichnisbaums und benutzerdefinierter Verzeichnisstrukturen.

4.11.3 Bücher zu diesem Thema

- *Implementing LDAP* von Mark Wilcox; Wrox Press, Inc.
- *Understanding and Deploying LDAP Directory Services* von Tim Howes et al.; Macmillan Technical Publishing

5 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 **POS**, **Point Of Sale**) 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 den 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/software/ecommerce/ccvs finden Sie weitere Informationen darüber, wie Sie CCVS aktivieren können.

5.1 Verwenden von CCVS

CCVS stellt Verbindung zwischen einer e-Commerce Anwendung und einem Kreditkarten-Zahlungs-Gateway her. Obwohl die Verwendung von CCVS davon abhängt, welches Protokoll Ihre Zahlungs-Gateway benutzt, kann es in den meisten Fällen nach kleinen Änderungen des bestehenden Systems angewendet werden. Unter http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/protocol-specific.html erhalten Sie genauere Informationen über die von CCVS unterstützten Protokolle.

In den folgenden Beispielen wird die Verwendung von CCVS dargestellt:.

- 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 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.
- CCVS kann bei der Verarbeitung von Zahlungen für ein Storefront hilfreich sein, das telefonische Bestellungen per Call-Center erhält. Auf diese Weise werden Bestellungen über das Web mit der Standardanwendung CGI verarbeitet. Oder sie werden durch einen Verkaufsagenten unter Verwendung eines kundenspezifischen Java-Programms verarbeitet, das über LAN ausgeführt wird, wobei für die Bearbeitung und die Zahlungen der Bestellungen die gleiche Verbindung verwendet wird. Zusätzlich wird das Address Verification System (AVS) von CCVS verwendet, um Betrug bei beiden Bestellmethoden zu verhindern, ohne dieses System dabei gesondert in jeder Anweisung implementieren zu müssen, was Zeit erspart.

Dies sind nur einige 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 üblicherweise 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 sind.
- Die Sicherheit, das Produkt jederzeit testen und neuprogrammieren zu können, ohne dass dabei tatsächlich existierende Kreditkarten belastet werden.

5.2 Verifizieren einer Kreditkarte

Wie kann nun ein Händler anhand dieser kleinen Plastikkarte feststellen, ob Sie sich z.B. den Fernseher 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.

5.3 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.

5.3.1 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 zu aktivieren 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://hardware.redhat.com.

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.

5.3.2 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/products/software/ecommerce/ccvs/support/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 Golbal Payment Systems
- NDC-Protokoll (auch bekannt als Atlanta) von Global Payment Systems
- VITAL-Protokoll (auch bekannt als VisaNet, Visa 2nd generation, K format)
- 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/products/software/ecommerce/ccvs/support/docs/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.

5.3.3 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 CCVSE

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 (`ccvs_configure`) 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 7.1 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 7.1 enthalten.

5.4 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` — 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` — Tcl-Schnittstelle für CCVS
- `CCVS-examples` — Beispielquellcode, erforderlich für die Entwicklung

5.5 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. Unter Abschnitt 5.11, *Zusätzliche Ressourcen* finden Sie installierte und Online-Dokumentationen über CCVS

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/software/ecommerce/ccvs/support/docs/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. Die folgenden init-Strings können für die unterstützten Modems verwendet werden:

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
```

Wenn Sie eines des unterstützten Modems verwenden, werden Sie vom Konfigurationsprogramm aufgefordert, den init-String zu bestätigen. 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.

5.6 Konfigurieren von CCVS

Sie müssen CCVS für Ihr System konfigurieren, und zwar entweder führen Sie CCVS im Demo-Modus oder für die Verarbeitung von echten Daten aus.

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. Diesem Zweck dient `setup.txt` Workstreet-Datei, die Sie vervollständigt haben

sollten, bevor das CCVS Konfigurationsprogramm ausgeführt wird. Unter Abschnitt 5.5, *Bevor Sie mit dem Konfigurieren von CCVS beginnen* erhalten Sie weitere Informationen über die Verwendung von `setup.txt` .

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 Stapelverarbeitungen 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.
```

5.7 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.

5.8 Starten von CCVS

Um CCVS für eine bestimmte Anwendung auszuführen, sollten Sie als Benutzeraccount angemeldet sein, der diese Konfiguration erstellt hat. Wenn Sie den ccvs Benutzeraccount verwenden und im System als anderer Benutzer angemeldet sind, müssen Sie mit dem Befehl `succvs` zum richtigen Benutzer wechseln.

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).

5.8.1 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 im 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`.

5.8.2 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`.

5.9 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/products/software/ecommerce/ccvs/support/docs/Admin-Java.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.

5.10 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 für CCVS finden Sie unter http://www.redhat.com/products/software/ecommerce/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

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.

5.11 Zusätzliche Ressourcen

Es sind zusätzliche Informationen über CCVS erhältlich.

5.11.1 Installierte Dokumentation

- `/usr/share/doc/CCVS–<version- number>` — Enthält die Dateien `CHANGES`, `LICENSE`, und `README` sowie das `setup.txt` Arbeitsblatt, das beim Zusammentragen der notwendigen Informationen hilft, bevor das Konfigurationsprogramm gestartet wird.
- Geben Sie den Befehl `man ccvs` ein und Sie erhalten eine Beschreibung der verschiedenen Stadien einer Transaktion, der CCVS Fehlercodes und vieles andere mehr. In den man-Seiten für die Befehle `ccvsd`, `cvreport` und `cvupload` finden Sie eine Anzahl verschiedener Optionen, die mit diesen Befehlen durchgeführt werden können.

5.11.2 Hilfreiche Websites

- http://www.redhat.com/products/software/ecommerce/ccvs — Von dieser Stelle aus können Sie mit den umfangreichen CCVS Ressourcen verbunden werden, einschließlich FAQs, technische Erläuterungen und allgemeine Informationen über CCVS .
- http://www.redhat.com/products/software/ecommerce/ccvs/support/documentation.html — Enthält Links zu einigen Anleitungen, die speziell für die unterschiedlichen Anwendungsmöglichkeiten von CCVS geschrieben wurden. In diesen Online- Handbüchern finden Sie alles, von der Installation und Konfiguration von CCVS bis zu einer kompletten Beschreibung der APIs für die verschiedenen Programmiersprachen, die verwendet werden können.

6 Sendmail

6.1 Einführung in Sendmail

Sendmail ist ein weit verbreiteter **Mail-Transfer-Agent** (**MTA**) im Internet. Er verwaltet einen sehr großen Prozentsatz aller im Internet von einem zum anderen Rechner verschickten E-Mails. Es gibt zwar auch andere Mail-Transfer-Agenten (die ebenfalls von Red Hat Linux verwendet werden können), die meisten Administratoren entscheiden sich jedoch aufgrund der Leistung, Scalierbarkeit und Kompaltbilität des MTA mit den Internet-Standards für die Verwendung von Sendmail.

Die Hauptaufgabe von Sendmail besteht im sicheren Versenden von E-Mails zwischen Rechnern, wobei ein **Simple Mail Transfer Protocol** (**SMTP**) verwendet wird. Da Sendmail sehr gut zu konfigurieren ist, können Sie nahezu alle Aspekte beim Verwalten einer E-Mail kontrollieren.

Sendmail kann bis zum Anfang der Erstellung einer E-Mail zurückverfolgt werden, wie zu der Zeit, als es ARPANET (den Vorläufer vom Internet) noch nicht gab. Zu diesem Zeitpunkt war jede Mailbox des Benutzers eine Datei, die nur vom Benutzer gelesen werden konnte, und Mail-Anwendungen fügten zu dieser Datei einfach Text hinzu. Jeder Benutzer musste seine Mail-Datei komplett durchsuchen, um alte E-Mails zu finden, und das Lesen einer neuen Mail war lästige Pflicht. Die erste tatsächliche Übermittlung einer Datei von Mitteilungen fand nicht vor 1972 statt, dabei wurde begonnen, E-Mails per FTP über das NCP-Netzwerkprotokoll zu versenden. Diese einfachere Art der Kommunikation wurde schnell populär und machte in weniger als einem Jahr den größten Teil des ARPANET Datenverkehrs aus. Da es jedoch keine standardisierten Protokolle gab, wurde es für einige Systeme schwieriger, E-Mails zu versenden. Dieser Zustand hielt an, bis 1982 ARPANET für TCP/IP standardisiert wurde. Für die Übermittlung von Mitteilungen entstand ein neues Protokoll - SMTP. Diese Entwicklungen sowie das Ersetzen der HOSTS-Dateien durch DNS führten zur Verwirklichung von MTA. Sendmail, das aus aus dem früheren E-Mail System Delivermail hervorgeht, wurde schnell zum Standard, als das Internet sich vergrößerte und überall verwendet wurde.

Es ist wichtig, die Funktionen von Sendmail zu kennen und zu wissen, wobei es Sie unterstützen kann oder auch nicht. Wahrscheinlich gehen Sie davon aus, dass Sendmail (wie die heutigen monolithischen Anwendungen, die vielseitige Aufgaben erfüllen können) die einzige Anwendung ist, um einen E-Mail-Server in Ihrer Organisation auszführen. Technisch gesehen ist das auch richtig, denn Sendmail kann Mails in Ihre Benutzer-Verzeichnisse übertragen und akzeptiert neue E-Mails durch die Befehlszeile. Die Benutzer erwarten heutzutage mehr als nur das Übertragen von E-Mails, sie möchten fast immer mit ihrer E-Mail unter Verwendung von **Mail User Agent** (**MUA**) im **Post Office Protocol** (**POP**), **Internet Message Access Protocol** (**IMAP**) oder auch im Web interagieren. Diese Protokolle arbeiten in Verbindung mit Sendmail und SMTP, dienen jedoch einem anderen Zweck und können unabhängig voneinander arbeiten.

Es würde über dieses Kapitels hinausgehen, alle Konfigurationen zu beschreiben,, die für Sendmail durchgeführt werden können oder sollen. Für Informationen über Sendmail sollten Sie die vielen guten Online- und Offlinequellen nutzen, um es zu gestalten und Ihre genaue Spezifikation anzupassen. Sie sollten wissen, welche Dateien standardmäßig mit Sendmail in Ihrem System installiert werden, wie grundlegende Konfigurationen durchzuführen sind. Achten Sie darauf, wie Sie unerwünschte E-Mails (spam) stoppen können, und wie Sie Sendmail mit **Lightweight Directory Access Protocol** (**LDAP**) erweitern können.

6.2 Die Standardinstallation von Sendmail

Während des Herunterladens des Quellcodes für Sendmail und dem Erstellen einer Kopie bevorzugen viele Benutzer das Installieren von Sendmail per RPM von der CD-ROM (bei der Installation von Red Hat Linux oder zu einem späteren Zeitpunkt).

Die Sendmail Anwendung ist in `/usr/sbin` abgelegt..

Die ausführliche und detaillierte Konfigurationsdatei (`sendmail.cf`) für Sendmail ist in `/etc` installiert. Sie sollten die Datei `sendmail.cf` nicht sofort bearbeiten, bis Sie genau wissen, was Sie sie bearbeiten wollen, da die Datei sehr komplex ist. Sie sollten stattdessen die Datei `/etc/mail/sendmail.cf` bearbeiten und unter Verwendung des darin enthaltenen `m4` Macro-Prozessors eine neue `/etc/ sendmail.cf`-Datei erstellen. (nachdem Sie die vorher die `/etc/sendmail.cf`-Originaldatei gesichert haben). Weitere Informationen über die Konfiguration von Sendmail erhalten Sie unter Abschnitt 6.3, *Änderungen der Konfiguration*

In `/etc/mail` sind verschiedene Sendmail Konfigurationsdateien installiert, einschließlich:

- `access` — Gibt an, welche Systeme Sendmail für die Übertragung von E-Mails nutzen können.
- `domaintable` — Erlaubt das Aufgliedern der Domänennamen.
- `local-host-names` — Hier sind alle Aliasnamen für Ihren Computer enthalten.
- `mailertable` — Gibt Anleitungen, um das Routing für bestimmte Domänen außer Kraft zu setzen.
- `virtusertable` — Erlaubt eine domänenspezifische Form des Aliasing und erlaubt multiple virtuelle Domänen auf einem Computer.

Einige dieser Konfigurationsdateien aus `/etc/mail`, zum Beispiel `access`, `domaintable`, `mailertable` und `virtusertable` müssen ihre Informationen in Datenbank-Dateien speichern, bevor Sendmail die Änderungen, die bei der Konfiguration vorgenommen wurden, verwenden kann. Um alle diese Änderungen in den Dateibankdateien zu speichern, müssen Sie einen Befehl mit der Syntax `makemaphash /etc/mail/`*`name`* `< /etc/mail/`*`name`* ausführen, wobei *name* den Namen der konvertierten Konfigurationsdatei angibt.

Wenn Sie zum Beispiel möchten, dass alle E-Mails, die an den `domain.com` Zugriff adressiert sind, an `bob@otherdomain.com` verschickt werden sollen, müssen Sie in der Datei `virtusertable` eine Zeile einfügen:

```
@domain.com       bob@otherdomain.com
```

Um diese neuen Informationen dann zu der Datei `virtusertable` hinzuzufügen, führen Sie `makemaphash /etc/mail/ virtusertable < /etc/mail/virtusertable` als Root aus. Dadurch wird eine neue Datei (`virtusertable.db`) erstellt, die die neue Konfiguration enthält.

6.3 Änderungen der Konfiguration

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 `/etc/sendmail.cf` zum Konfigurieren von Sendmail zu erstellen, sollten Sie den `m4` Macro-Prozessor verwenden. Wenn Sie `/etc/mail/sendmail.mc` bearbeiten, um für Sendmail Funktionen hinzuzufügen, sichern Sie Ihre aktuelle `/etc/sendmail.cf` Datei, erstellen Sie eine neue, indem Sie den Befehl `m4 /etc/mail/ sendmail.mc >/etc/sendmail.cf` ausführen, und fügen Sie alle vorherigen Änderungen von `/etc/sendmail.cf` hinzu, die Sie in der neuen Datei `/etc/sendmail.cf` vorgenommen haben. Nachdem Sie `/etc/sendmail.cf` neu erstellt haben, müssen Sie Sendmail erneut starten. Führen Sie dazu einfach den Befehl `/sbin/ service sendmail restart` als Root aus.

Der Macro-Prozessor `m4` wird standardmäßig mit Sendmail installiert. Er ist im Paket `sendmail-cf` enthalten, das in `/usr/ lib/sendmail-cf` installiert ist.

Bevor Sie eine der Dateien aus dem `/usr/lib/sendmail-cf` Verzeichnis bearbeiten, sollten Sie sich unter der Datei `/usr/lib/sendmail-cf/README` darüber informieren.

WARNUNG

Verwenden Sie zum Konfigurieren von Sendmail auf keinen Fall Linuxconf! Das Linuxconf Modul von `mailconf` wurde erstellt, um die Bearbeitung von `/etc/ sendmail.cf` zu vereinfachen. Es enthält ältere Informationen über die Regeln, die beim Konfigurieren von Sendmail beachtet werden müssen.

Mit Sendmail steht Ihnen eine Konfiguration für Ihren Computer zur Verfügung, die Sie als Mail-Gateway für alle Computer in Ihrem Netzwerk verwenden können. Eine Firma möchte zum Beispiel, dass der Computer mit dem Namen `mail.bigcorp.com` alle Mails erhält. Dafür müssen einfach die Namen der Computer hinzugefügt werden, für die `mail.bigcorp.com` die Mails in `/etc/mail/local- host-names` verwalten soll. Wie zum Beispiel:

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

Auf den anderen Computern `torgo`, `poodle`, und `devel` muss die Datei `/etc/sendmail.cf` bearbeitet werden, um sich als `mail.bigcorp.com` zu "verkleiden", wenn Mails verschickt werden und die lokale E-Mail-Verarbeitung an `bigcorp.com` weitergeleitet wird. 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.bigcorp.com

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

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

Aufgrund dieser Konfiguration erscheinen alle verschickten Mails so, als wären sie von `bigcorp.com` versandt worden, und alle Mails an `torgo.bigcorp.com` oder andere Rechner werden an `mail.bigcorp.com` verschickt.

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.

6.4 Vermeiden von Spam

Spam: Hierbei handelt es sich um unnötige und nicht erwünschte E-Mails, deren Absender nicht bekannt ist und auf die nie geantwortet wird. Das ist eine sehr lästige, teure und weit verbreitete Belästigung der normalen Internet-Kommunikation.

Durch Sendmail ist es (relativ) einfach, die neuentwickelten Spamm-Techniken zu blockieren. Es werden viele der üblichen Spam-Techniken bereits standardmäßig blockiert: um die solche E-Mails zu erhalten, müssten Sie die `/etc/mail/ sendmail.cf` Datei bewusst so verändern, dass Ihr System für die Spams zugänglich wird. Zum Beispiel wurde das Versenden von SMTP-Mitteilungen (auch bekannt unter **SMTP relaying**) standardmäßig ab der Sendmail Version 8.9 deaktiviert. Vor dieser Änderung erlaubte Sendmail es Ihrem Mail-Host (`x.org`), Mitteilungen von einer Gruppe (`y.com`) zu akzeptieren und diese an eine andere Gruppe (`z.net`) zu schicken. Jetzt müssen Sie Sendmail speziell anweisen, es einer Domäne zu erlauben, E-Mails über Ihre Domäne zu empfangen. Um die Änderungen zu aktivieren, bearbeiten Sie einfach `/etc/mail/relay-domains` und starten Sie Sendmail als Root neu, indem Sie den Befehl `/sbin/service sendmail restart` eingeben.

Ihre Benutzer werden jedoch oft unkontrolliert durch Spams von anderen Servern in Internet bombardiert. Unter diesen Umständen können Sie die Zugriffskontrolle von Sendmail aktivieren, die in der `/etc/mail/access` Datei zu finden ist. Als Root-Benutzer können Sie die Domänen hinzufügen, die Sie blockieren wollen oder zulassen möchten, wie z.B:

```
badspammer.com       550 Go away and don't spam us anymore
tux.badspammer.com   OK
10.0                 RELAY
```

Da `/etc/mail/access` eine Datenbank ist, müssen Sie makemap verwenden, um die Änderungen zu aktivieren, die beim Neuerstellen des Abbildes der Datenbank vorgenommen wurden. Führen Sie dazu einfach den Befehl `makemap hash /etc/mail/access < /etc/mail/access` als Root aus.

Dieses Beispiel zeigt, dass alle Mails, die von `badspammer.com` versandt werden, durch den 550 RFC 821 Fehlercode blockiert und an den Absender zurückgeschickt werden, mit Ausnahme der Mails, die von der untergeordneten Domäne `tux.badspammer.com` verschickt werden. Diese werden akzeptiert. Die letzte Zeile zeigt, dass alle Mails, die über das 10.0.*.* Netzwerk verschickt werden, von Ihrem Mail-Server empfangen werden.

Wie Sie sich vorstellen können, gibt dieses Beispiel nur einen kleinen Überblick über die Möglichkeiten, die Sendmail im Bezug auf das Blockieren und Zulassen von Zugriffen bietet. Unter `/usr/share/doc/sendmail/README.cf` finden Sie weitere Informationen und Beispiele.

6.5 Verwendung von Sendmail mit LDAP

Wie bereits in Kapitel 4, *Lightweight Directory Access Protocol (LDAP)* beschrieben, ist Lightweight Directory Access Protocol (LDAP) eine schnelle und gute Möglichkeit, um genauere Informationen über einen bestimmten Benutzer aus einer größeren Gruppe zu erhalten. Sie können den LDAP-Server zum Beispiel verwenden, um eine E-Mail-Adresse aus einem Verzeichnis zu finden, das von einer Firma benutzt wird. Hierbei besteht ein großer Unterschied zu Sendmail: mit LDAP speichern Sie hierarchische Benutzerinformationen, und Sendmail zeigt die Risultate von LDAP bei der Suche nach voradressierten E-Mail Mitteilungen.

Sendmail unterstützt eine größere Integration von LDAP, das verwendet wird - um einzelne Dateien, wie zum Beispiel `aliases` und `virtusertables` auf den verschiedenen Mail-Servern auszutauschen - die zusammenarbeiten um mittlere bis große Organisationen zu unterstützen.

Die aktuelle Version von Sendmail enthält Support für LDAP. Verwenden Sie für die Erweiterung des Sendmail Servers LDAP. Sie erhalten einen korrekt konfigurierten LDAP-Server, wie zum Beispiel OpenLDAP. Dann müssen Sie `/etc/mail/sendmail.mc` bearbeiten und Folgendes einfügen:

```
LDAPROUTE_DOMAIN('IhreDomäne.com')dnl
FEATURE('ldap_routing')dnl
```

Bitte beachten

Das ist nur die Standard-Konfiguration von Sendmail mit LDAP, von der sich Ihre Konfiguration erheblich unterscheiden wird. Dies ist abhängig von Ihrer LDAP-Implementierung, im Besonderen, wenn Sie mehrere Computer für die Verwendung eines gemeinsamen LDAP-Servers konfigurieren möchten.

Unter `/usr/share/doc/sendmail/README.cf` erhalten Sie genaue Anweisungen über die Konfiguration von LDAP sowie weitere Beispiele.

Erstellen Sie als Nächstes die Datei `/etc/sendmail.cf` neu, indem Sie `m4` ausführen und Sendmail neu starten. Unter Abschnitt 6.3, *Änderungen der Konfiguration* erhalten Sie weitere Anweisungen.

Weitere Informationen über LDAP finden Sie unter Kapitel 4, *Lightweight Directory Access Protocol (LDAP)*

6.6 Zusätzliche Ressourcen

Viele Benutzer empfinden das Konfigurieren von Sendmail, vor allem wegen der vielen möglichen Optionen, als schwierig. Der Zugriff auf zusätzliche Dokumentationen über Sendmail kann besonders bei der Einstellung der Konfigurationsoptionen sehr hilfreich sein.

6.6.1 Installierte Dokumentation

Die besten Quellen für Informationen über das Konfigurieren von Sendmail finden Sie in den Paketen `sendmail` und `sendmail-cf`.

- `/usr/share/doc/sendmail/README.cf` — Enthält Informationen über `m4`, Dateiverzeichnisse für Sendmail, unterstützte Mailer und Arten, wie auf verbesserte Merkmale zugegriffen werden kann u.v.m.
- `/usr/share/doc/sendmail/README` — Enthält Informationen über die Verzeichnisstruktur von Sendmail, IDENT-Protokoll-Support, Einzelheiten über Verzeichnisberechtigungen und die Probleme, die auftreten, wenn diese Berechtigungen nicht richtig konfiguriert sind.

6.6.2 Hilfreiche Websites

- http://www.sendmail.net — Neuigkeiten, Interviews und Artikel über Sendmail. Bietet einen größeren Überblick über die verfügbaren Optionen.
- http://www.sendmail.org — Zeigt einen umfassenden technischen Ausfall von Sendmail Merkmalen und Beispiele für eine Konfiguration.

6.6.3 Zusätzliche Literatur

- *Sendmail* von Bryan Costales mit Eric Allmanet al; O'Reilly & Associates — Eine gutes Nachschlagewerk für Sendmail, das unter Mithilfe des Autors von Delivermail und Sendmail geschrieben wurde.

Teil II Die Sicherheit

7 Basishandbuch über die Sicherheit von Red Hat

Neben der korrekten Installation und Konfiguration Ihres Red Hat Linux Systems ist es von grundlegender Bedeutung, das System entsprechend seiner Rolle und seines Gebrauchs mit einer angemessenen Sicherheitsstufe auszustatten. Bei der Sicherheit handelt es sich um ein extrem komplexes Thema, bei dem ständig neue reale und potentielle Probleme ans Tageslicht kommen.

Viele Systemadministratoren begehen aufgrund der amorphen und komplexen Natur dieses Themas den Fehler, sich auf kleine und vereinzelte Schwierigkeiten zu konzentrieren und verlieren dabei die größeren und wichtigeren Probleme aus den Augen. Die wahre Systemsicherheit geht jedoch weit über die Installation der jüngsten Version oder die Konfiguration einer bestimmten Datei oder die sorgfältige Verwaltung des Benuterzugriffs auf die Ressourcen des Systems hinaus. Es handelt sich hierbei vielmehr darum, die zahlreichen Gefahren für Ihr System zu ermitteln und die entsprechenden Gegenmaßnahmen zu treffen.

Kein System ist wirklich sicher, es sei denn, es ist ausgeschaltet (und selbst dann besteht noch die Möglichkeit, dass es gestohlen wird). Ist es dagegen eingeschaltet, ist es ständigen Angriffen ausgesetzt: von harmlosen Streichen bis hin zu Viren, die die Hardware zerstören und Daten löschen können. Aber damit ist noch nicht alles verloren. Mit der richtigen Umsicht und den geeigneten Instrumenten können Sie Ihren Computer auch jahrelang benutzen, ohne dass Probleme auftreten. In den folgenden Abschnitten wird der korrekte Ansatz in Bezug auf das Problem der Sicherheit und die potentiellen Gefahren sowie die zahlreichen Instrumente, die Kosten und die Vorteile der Verwendung von Red Hat Linux beschrieben.

7.1 Das unvermeidliche Dilemma mit der Sicherheit

Die Benutzer von Betriebssystemen sehen sich beim Ausarbeiten eines Sicherheitsmodells für ihr System einem gemeinsamen Dilemma gegenüber. Einerseits werden sie vermeiden, das System so sicher zu gestalten, dass nichts korrekt funktioniert. Andererseits werden sie jedoch vermeiden wollen, das System so unsicher zu machen, dass jedermann jederzeit damit machen kann (und wird), was er möchte, beispielsweise die Arbeit anderer Benutzer zu löschen oder noch Schlimmeres.

Es gibt keinen definitiven Ausweg aus diesem Dilemma. Einige Benutzer wählen aufgrund ihres Betriebszwecks oder der Bedeutung der zu schützenden Daten die eine Lösung, andere wiederum aufgrund der zahlreichen Benutzer oder der Tatsache, dass es sich um Testrechner handelt, die andere Lösung.

Das Wichtigste bei der Konfiguration der Sicherheit Ihres Systems ist zu bestimmen, wo sich Ihr System innerhalb der Bandbreite des Dilemmas befindet. In einigen Fällen liegt dies zum Beispiel in der Verantwortung der Unternehmenspolitik, Sie könnten aber auch zu Forschungszwecken ein System

benutzen, das nie mit öffentlichen Netzwerken verbunden wird und niemand sonst Zugriff auf den Rechner hat. Ein weiterer Fall sind die privaten Benutzer, die eine Breitbandverbindung besitzen und sich (gerechtfertigterweise) darüber Gedanken machen, wie Benutzer auf der anderen Seite der Welt ihre Daten mutwillig beschädigen könnten.

Unabhängig davon, welches der unzähligen Szenarien auf Sie zutrifft, sind Sie dafür zuständig zu bestimmen, inwieweit Sie Ihr System gemäß seinem Verwendungszweck möglichen Risiken aussetzen möchten. Nachdem Sie diese Entscheidung getroffen haben, konfigurieren Sie Ihre Systemsicherheit entsprechend und halten Sie sich auch in Zukunft an diese Richtlinien.

7.2 Aktiver und passiver Ansatz im Vergleich

Es gibt zwei Ansätze im Rahmen des Themas Sicherheit: der **aktive** und der **passive** Ansatz. Der **aktive** Ansatz deckt alle Vorgänge, die einem Versagen des Sicherheitsmodells Ihres Systems vorbeugen. Der **passive** Ansatz umfasst die Vorgänge, die die Sicherheit Ihres Systems auf der Grundlage des gewählten Sicherheitsmodells überwachen.

Alle Benutzer sollten sowohl den aktiven als auch den passiven Ansatz verwenden, da sie sich gegenseitig stützen. Wenn Sie zum Beispiel entdecken, dass ein bestimmter Benutzer versucht, auf Ihr System zuzugreifen (passiver Ansatz), werden Sie wahrscheinlich eine Anwendung installieren, die ihn daran hindert, bis an das Anmelde-Prompt zu gelangen (aktiver Ansatz). Wenn Sie dagegen keine Shadow-Passwörter (aktiver Ansatz) zum Schutz Ihres Systems verwenden, werden Sie zum Beispiel die Schlüsseldateien Ihres Systems mithilfe eines Tools wie Tripwire ändern (passiver Ansatz). Weitere Informationen über Tripwire finden Sie unter Kapitel 10, *Installieren und Konfigurieren von Tripwire*.

Red Hat Linux enthält eine Vielfalt an Tools für beide Ansätze im Rahmen der Systemsicherheit. Die korrekte Anwendung der Methoden jedes Ansatzes ist jedoch sehr wichtig, um eine übermäßige Abhängigkeit von diesen Instrumenten zu vermeiden.

7.2.1 Tools und Methoden für einen aktiven Sicherheitsansatz

Der Großteil der Sicherheitstools für Red Hat Linux ist für die aktive Sicherheit Ihres Systems konzipiert. Im Folgenden einige der gebräuchlichsten und nützlichsten Open-Source-Tools:

- *Shadow-Dienstprogramme* — Eine Reihe von Tools für die Verwaltung von lokalen Benutzern und Gruppen auf einem System, das verschlüsselte Passwörter verwendet.
- *Kerberos 5* — Ein sicheres System, das Dienste zur Netzwerkauthentifizierung liefert und den Gebrauch von offensichtlichen Passwörtern verhindert, die über ein Netz übertragen werden, um auf Dienste zugreifen zu können (weitere Informationen über Kerberos 5 finden Sie unter Kapitel 9, *Verwenden von Kerberos 5 in Red Hat Linux*).

- *OpenSSL* — Dieses Tool dient dem Schutz zahlreicher Dienste, die Operationen über eine verschlüsselte Ebene unterstützen (mehr Informationen über OpenSSL finden Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*).
- *OpenSSH* — Eine Reihe von Dienstprogrammen, die leicht solche allgegenwärtigen und gleichzeitig unsicheren Tools wie `telnet` und `ftp` mit den leistungsstarken und sicheren `ssh` und `scp` ersetzen können (weitere Informationen über OpenSSH finden Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*).

Zu den Methoden, die einen aktiven Ansatz unterstützen, gehören die folgenden:

- *Schränken Sie die Anzahl der Benutzer ein, die Befehle als Root ausführen können* — Sehr viele Probleme im Rahmen der Sicherheit hängen, zumindest indirekt, damit zusammen, dass ein Benutzer das Root-Passwort kennt oder über `sudo` die Berechtigung erhält, einen Befehl als Root auszuführen.
- *Informieren Sie sich, welche Software-Pakete auf Ihrem System installiert sind, sowie über neu entdeckte "Löcher" in der Systemsicherheit* — Sie müssen wissen, welche Pakete auf Ihrem System installiert sind, wenn Sie sich auf dem neuesten Stand halten möchten, und Sie müssen die Informationsquellen wie Red Hat Network konsultieren, um zu erfahren, ob die Pakete zu aktualisieren sind.
- *Schränken Sie die Dienste Ihres Systems auf die ein, die Sie wirklich benötigen* — Es gilt das Prinzip: über je mehr Dienste Sie verfügen, desto größer ist die Gefahr eines unerlaubten Zugriffs. Sparen Sie sich Systemressourcen (und damit das Problem der Verwaltung von Diensten, die Sie nicht verwenden) und entfernen Sie die unnötigen Pakete. Führen Sie abschließend ein Tool wie `ntsysv` aus, das verhindert, dass unnötige Dienste beim Booten ebenfalls aktiviert werden (siehe *Kontrolle des Zugriffs auf Dienste* im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*.)
- *Beauftragen Sie die Benutzer damit, sichere Passwörter zu erstellen und sie oft zu ändern* — Der Grund für die meisten Sicherheitsprobleme ist, dass nicht berechtigte Benutzer auf das System zugreifen. Diese Gefahr kann dadurch erheblich vermindert werden, indem Sie Ihre Benutzer damit beauftragen, sichere aktive Sicherheitsmethoden anzuwenden, um Ihre Schlüssel zu Ihrem System zu schützen.
- *Versichern Sie sich, dass Dateiberechtigungen nur dann offen sind, wenn es tatsächlich notwendig ist* — Praktisch alle Dateien sollten von nur einem einzigen Benutzer geändert werden können.

7.2.2 Tools und Methoden für einen passiven Sicherheitsansatz

Während die meisten Sicherheitstools für Red Hat Linux für einen aktiven Sicherheitsansatz konzipiert sind, gibt es auch einige Instrumente, die die passive Sicherheit zu einer sehr geringe administrativen Last werden lassen:

- *Tripwire* — Hierbei handelt es sich um eine Anwendung, die Sie darauf hinweist, wenn spezifische Dateien und Verzeichnisse Ihres System geändert wurden. Auf diese Weise erfahren Sie, wenn nicht berechtigte Benutzer auf Ihr System zugreifen oder berechtigte Benutzer nicht gewünschte Änderungen an wichtigen Dateien vornehmen (mehr Informationen über Tripwire finden Sie unter Kapitel 10, *Installieren und Konfigurieren von Tripwire*).
- *COPS* — Eine Reihe von Sicherheitstools, die für zahlreiche verschiedene Funktionen konzipiert wurden, beispielsweise die Kontrolle der offenen Ports auf einem bestimmten Rechner bis hin zum Auffinden von zu offensichtlichen Passwörtern.

Zu den Methoden, die einen aktiven Ansatz unterstützen, gehören die folgenden:

- *Führen Sie systematische Kontrollen der Systemprotokolle aus* — Red Hat Linux sammelt eine Menge nützlicher Daten in den Systemprotokollen im Verzeichnis `/var/log`, insbesondere in der Datei `messages`. Eine einfache, als Root ausgeführte Aufgabe, beispielsweise `grep "session opened for user root" /var/log/messages | less` ermöglicht Ihnen eine teilweise Prüfung Ihres Systems und der Benutzer, die als Root auf Ihr System zugreifen. Auf diese Weise können Sie eventuell leicht die Anzahl potentieller Benutzer herausfinden, die Änderungen an einer bestimmten Datei vorgenommen haben, die nur von einem Root-Benutzer modifiziert werden können. Hierzu brauchen Sie nur die Uhrzeit der Änderung mit den Uhrzeiten der Anmeldevorgänge zur Datei `/var/log/messages` zu vergleichen. Es handelt sich hierbei jedoch nicht um eine "narrensichere" Methode, da ein Benutzer mit der Berechtigung zu einer wichtigen Datei wahrscheinlich auch authorisiert ist, `/var/log/messages` zu ändern, um keine Spuren zu hinterlassen.

7.3 Entwicklung der Sicherheitspolitik

Auf jedem Rechner sollte eine Sicherheitspolitik angewendet werden, unabhängig davon, ob er von nur einer Person oder von tausenden Benutzern eines Unternehmens benutzt wird. Bei der Sicherheitspolitik handelt es sich um eine Reihe von Richtlinien, die eingesetzt werden um zu beurteilen, ob eine bestimmte Aktivität oder Anwendung auf einem System entsprechend dem Zweck desselben ausgeführt bzw. verwendet werden sollte oder nicht.

Die Sicherheitspoltik kann von System zu System sehr unterschiedlich sein. Wichtig ist jedoch, dass für Ihr System effektiv eine solche Politik existiert - ob sie nun Bestandteil des Handbuchs der Unternehmenspolitik ist oder nicht.

Jede Art der Sicherheitspolitik sollte anhand der folgenden Richtlinien entwickelt werden:

- *Lieber einfach als komplex* — Je einfacher und eindeutiger die Sicherheitspolitik, desto wahrscheinlicher ist es, dass die Richtlinien befolgt werden und damit die Sicherheit des Systems gewährleistet wird.
- *Einfache statt schwierige Wartung* — Sicherheitsmethoden und -tools sind wie alles andere auch ständig neuen Erfordernissen und Veränderungen unterworfen. Die Sicherheitspolitik für Ihr System sollte daher so konzipiert sein, dass die Auswirkungen solcher Entwicklungen auf Ihr System und seine Benutzer möglichst gering sind.
- *Die Freiheit durch das Vertrauen in die Systemintegrität fördern statt die Leistungsfähigkeit des Systems zu hemmen* — Vermeiden Sie Methoden und Tools, die das System zwar sicher machen, den Nutzen Ihres System jedoch unnötig mindern. Leistungsstarke Sicherheitsmethoden und -tools machen das System sicherer, bieten den Benutzern aber gleichzeitig einen mölichst größeren Handlungsspielraum.
- *Erkennen von Fehlern statt falsche Sicherheit* — Eine erfolgreiche Art und Weise, ein Sicherheitsproblem zu verursachen, ist zu glauben, in Ihrem System können keine Probleme auftauchen.
- *Sich auf wirkliche Probleme konzentrieren statt sich nur mit der Theorie zu befassen* — Verwenden Sie Ihre Zeit darauf, sich mit den größten tatsächlichen Problemen zu befassen. Setzen Sie Prioritäten. Um besser zu verstehen, welche Prioritäten gesetzt werden sollten, besuchen Sie http://www.sans.org/topten.htm oder ähnliche Websites, die sich umfassend mit Sicherheitsproblemen, die eine reale Gefahr darstellen, auseinandersetzen und Lösungsvorschläge bieten.
- *Sofort handeln statt aufschieben* — Stellen Sie eventuelle Probleme fest und bestimmen Sie, ob sie eine Gefahr darstellen. Geben Sie sich nicht der Illusion hin, dass Sie sie auch später noch lösen können. Es muss hier und jetzt gehandelt werden, insbesondere dann, wenn Risiken für Ihr System bestehen.

Wenn Sie der Meinung sind, dass Ihre Sicherheitspolitik so restriktiv ist, dass das System nicht mehr so genutzt werden kann wie eigentlich vorgesehen, dann sollten Sie in Erwägung ziehen, den Zugriff auf das System weniger strikt zu kontrollieren. Wenn Ihre Sicherheit dagegen ständig gefährdet ist, dann sollten Sie die Politik dahingehend ändern, dass der Zugriff eingeschränkt wird. Vergessen Sie dabei nie, dass eine Sicherheitspolitik kein statisches Dokument oder Konzept ist und daher ständig an die sich verändernden Ziele und Benutzer angepasst werden muss. Überarbeiten Sie Ihre Sicherheitspolitik immer im Hinblick auf die sich ergebenden neuen Erfordernisse.

7.4 Weitere Schritte im Rahmen der Sicherheit

Viele Benutzer basieren Ihre Systemsicherheit auf die Begrenzung der Anzahl der Benutzer, die einen Root-Zugriff auf das System haben. Dies ist natürlich ein sehr wichtiger erster Schritt, eine effektive Sicherheit verlangt jedoch nach mehr. Ein wirklich sicheres System verbindet Sicherheitsmethoden

und -tools mit dem Bewusstsein, dass es auch andere Arten gibt, wie solche Schäden hervorgerufen werden können.

Wenn Ihr System von mehreren Benutzern verwendet wird und diese oft wechseln, müssen Sie sich versichern, dass die Accounts der alten Benutzer sofort gelöscht werden, sobald sie nicht mehr notwendig sind. Zu diesem Zweck wird empfohlen, eine Kontrollliste der Punkte zu erstellen, die zu erledigen sind, wenn ein Benutzeraccount oder eine Gruppe nicht mehr länger verwendet wird.

Schränken Sie auch den physischen Zugriff auf Ihr System ein. Wenn sich in Ihrem System sehr wichtige Dateien befinden, so werden diejenigen, die daran interessiert sind, es sicherlich einfacher finden, gleich den gesamten Rechner zu entwenden, um genug Zeit zu haben, die Informationen zu suchen. Vermeiden Sie es daher, Informationen über den Rechner zu verbreiten, der solche wichtigen Dateien enthält.

Beschränken Sie sich darüber hinaus nicht nur auf die grundlegendsten Arten der Sicherheitsmethoden für Ihr System. Es hat keinen Sinn, einen Zugriffsweg zu schützen, wenn dadurch ein anderer ungeschützt bleibt. Welche Maßnahmen Sie hier ergreifen, hängt natürlich von Ihren Erfordernissen oder den Erfordernissen Ihrer Benutzer ab. Wichtig ist, dass Sie Ihr Augenmerk hier nicht nur auf einen einzigen Punkt richten.

7.5 Die Bedeutung wichtiger Passwörter

Passwörter sind die Schlüssel zu Ihrem System. Es versteht sich dabei von selbst, dass sie so sicher wie möglich sein sollten, um nicht berechtigte Anmeldungen zu vermeiden, was den ersten Schritt für größere Sicherheitsprobleme darstellen würde. Eine einfache Möglichkeit zur Verhinderung eines nicht authorisierten Zugriffs ist es daher, komplexe und unentschlüsselbare Passwörter zu erstellen.

Viele Passwörter sind relativ leicht zu erraten. Red Hat Linux bietet mehrere Möglichkeiten der Berechtigung zu einem System, beispielsweise verschlüsselte Passwörter mithilfe von `crypt`, Shadow-Passwörter (die detailliert in Abschnitt 12.1, *Shadow Dienstprogramme* behandelt werden), Kerberos 5 usw. In jeder Situation, in der Sie sich für Passwörter als Teil der Systemberechtigung entscheiden, hängt die Sicherheit dieser Methode zumindest teilweise von der Komplexität der Passwörter ab.

Warum sollten Sie grundsätzlich Passwörter erstellen, die schwierig zu entschlüsseln sind? In erster Linie, da der Preis leistungsstarker Computerhardware kontinuierlich sinkt, während immer mehr qualitativ hochwertige Tools und Methoden zum Entschlüsseln von Passwörtern kostenlos erhältlich sind. Aufgrund der Art, wie die Passwörter in vielen einfachen Berechtigungsschemata gespeichert werden, kann ein Hacker, der Zugriff auf die Dateien mit den Benutzerpasswörtern Ihres Systems erhält, in relativ kurzer Zeit wenigstens eins dieser Passwörter herausfinden und mithilfe einer Liste von in Wörterbüchern enthaltenen Wörtern die verschlüsselten Passwörter überprüfen. Die Berechtigungsschemata berücksichtigen zwar diese Art von unerlaubtem Zugriff und verwenden verschiedene Methoden, um dies so weit wie möglich zu verhindern, sind aber nicht 100% sicher. Daher sollten Sie die Passwörter, insbesondere die Root-Passwörter, sorgfältig auswählen und oft ändern.

Ein sicheres Passwort besitzt die folgenden Eigenschaften:

- *Es besteht aus mindestens acht Stellen* — Je kürzer das Passwort, desto leichter ist es zu entschlüsseln.
- *Es besteht aus Buchstaben, Ziffern und Symbolen* — Ziffern und Symbole in Kombination mit Buchstaben reduzieren die Wahrscheinlichkeit eines bestimmten Schriftzeichens,wodurch das gesamte Passwort sicherer wird.
- *Es ist einzigartig* — Wählen Sie nur Passwörter, die sich von anderen von Ihnen verwendeten Passwörtern unterscheiden. Sind alle Ihre Passwörter identisch oder sehr ähnlich, so ist die Sicherheit Ihres Systems einem sehr viel größeren Risiko ausgesetzt.

Vermeiden Sie Passwörter, die

- *aus einem Wörterbuch stammen bzw. Sinneinheiten darstellen* — Solche Passwörter sind wesentlich einfacher zu entschlüsseln. Überschreiben Sie darüber hinaus nicht die Sicherheitsschemata, die die Verwendung von solchen Wörtern verhindern.
- *auf irgendeine Weise mit Ihren persönlichen Daten zu tun haben* — Wenn Sie Ihr Geburtsdatum, den Namen Ihres Ehemannes/Ihrer Ehefrau oder die Marke Ihres Autos verwenden, dann fordern Sie Sicherheitsprobleme regelrecht heraus. Wählen Sie jedes Passwort sehr sorgfältig und denken Sie dabei darüber nach, ob es jemand erraten könnte. Wenn nur die geringste Möglichkeit hierzu besteht, dann verwenden Sie ein solches Passwort nicht.
- *nicht schnell und einfach eingegeben werden können* — wenn Ihr Passwort so kompliziert ist, dass Sie jedes Mal mühsam nach den Buchstaben suchen müssen, dann könnte es für einen aufmerksamen Beobachter sehr leicht sein, Ihr Passwort herauszufinden. Um dies zu verhindern, sollten Sie Ihr Passwort üben, wenn Sie allein sind, so dass die Eingabe möglichst automatisch erfolgt.

7.6 Netzwerk-Sicherheit

Wenn Sie Ihr Red Hat Linux System in einem Netzwerk (beispielsweise LAN, WAN oder Internet) verwenden, bedeutet dies sicherlich ein größeres Sicherheitsrisiko, als wenn Sie nicht an ein solches Netzwerk gebunden sind. Abgesehen von unerlaubten Zugriffen auf Ihre Passwortdateien und Benutzer, die unerlaubt auf Ihr System zugreifen, bestehen hier mehr potentielle Gefahren für Ihre Systemsicherheit, die darüber hinaus mehrere Formen annehmen können.

Red Hat Linux sieht eine Vielzahl von Maßnahmen im Rahmen der Systemsicherheit vor, wozu auch zahlreiche Open-Source Sicherheitstools gehören, die mit der Basisdistribution geliefert werden. Trotzdem können aufgrund der Netzwerktopologie oder vielen weiteren Faktoren Sicherheitsprobleme auftreten. Um den Ursprung und die Methode eines solchen Problems zu bestimmen, beachten Sie die Arten, in denen es wahrscheinlich auftritt:

- *Aufspüren der Berechtigungsdaten* — Bei vielen standardmäßigen Berechtigungsmethoden von Linux und anderen Betriebssystemen werden der Benutzername und das Passwort "eindeutig" als

normaler Text bzw. unverschlüsselt in das Netzwerk eingegeben. Es gibt zahlreiche Tools für die Benutzer, die Zugriff auf Ihr Netzwerk (oder auf Internet, wenn Sie es für den Zugriff auf Ihr System verwenden) haben, mit denen sie Ihr Passwort "aufspüren" oder ermitteln und alle über das Netzwerk übertragenen Daten aufzeichnen können, um sie zu analysieren und gemeinsame Anmeldeanweisungen herauszufinden. Auf diese Weise können *alle* Informationen aufgespürt werden, die Sie unverschlüsselt senden, wozu auch Ihr Root-Passwort gehört. Es ist daher unerlässlich, dass Sie Tools wie Kerberos 5 und OpenSSH implementieren, um zu vermeiden, dass Passwörter oder andere wichtige Daten unverschlüsselt gesendet werden. Wenn solche Tools aus irgendeinem Grund auf Ihrem System nicht verwendet werden könnne, dann melden Sie sich nie als Root an, es sei denn, Sie befinden sich an der Konsole.

- *Frontaler Angriff* — Angriffe wie Denial of Service (DoS) o.ä. können auch ein sicheres System beschädigen, indem sie es mit unpassenden Anforderungen überschütten oder Verarbeitungsprozesse einleiten, die Ihr System und Ihre Daten sowie andere Systeme, die mit Ihrem System verbunden sind, zahlreichen Gefahren aussetzen. Um dies zu verhindern, stehen mehrere Instrumente zur Verfügung, beispielsweise Firewalls mit Paketfiltern. Frontalangriffe sind jedoch am besten zu handhaben, wenn Sie untersuchen, wie unzuverlässige Systeme mit Ihrem sicheren System kommunizieren. Sie können mögliche Schäden auf einem Minimum halten, indem Sie schützende Barrieren zwischen beiden Systemen einrichten und schnelle Lösungsmöglichkeiten für jede Art Problem entwickeln.

- *Ausnutzen eines Bugs oder von Loopholes* — Gelegentlich werden Software-Fehler entdeckt, die, würden sie genutzt, ein ungeschütztes System schwer beschädigen würden. Aus diesem Grund sollten Sie so wenig Prozesse wie möglich als Root ausführen. Verwenden Sie darüber hinaus die Tools, die Ihnen zur Verfügung stehen (beispielsweise Red Hat Network für Paketaktualisierungen und Sicherheitsprobleme), um jegliche Art von Sicherheitsproblemen sofort lösen zu können. Versichern Sie sich auch, dass beim Booten Ihres Systems keine unnötigen Programme gestartet werden. Je weniger Programme aktiviert werden, desto geringer ist das Risiko von Fehlern.

7.7 Zusätzliche Ressourcen

Die Sicherheitsinformationen ändern sich ständig, und Websites stellen eine bequeme Art dar, sich auf dem Laufenden zu halten. Besuchen Sie daher regelmäßig die Websites von Linux und auch andere Websites über dieses Thema. Wenn Sie Hilfe für die Entwicklung einer soliden Sicherheitspoltik benötigen, so sollten Sie sich hierzu ein gutes Buch besorgen.

7.7.1 Nützliche Websites

- http://www.redhat.com/support/errata — Rufen Sie auf der Website von Red Hat das Kapitel über Support auf, um Informationen über die Sicherheit und die Aktualisierungen jeder von Red Hat erstellen Version von Red Hat Linux zu erhalten.

- http://www.cert.org — Die CERT-Website bietet eine Liste mit den jüngsten und schwerwiegendsten Sicherheitsproblemen und Schwachstellen und liefert detaillierte Informationen darüber, wie der ursprüngliche Zustand eines beschädigten Systems wiederhergestellt werden kann.
- http://www.sans.org — Die Website des Networking and Security Institute (SANS) bietet Kurzfinformationen über Probleme im Rahmen der Sicherheit und nützliche Links zu aktualisierten RPMs (sofern verfügbar).
- http://www.linuxsecurity.com — Die Linux-Website in Bezug auf die Sicherheit bietet eine Auswahl an sicherheitsspezifischen Links sowie Dokumentation und vieles mehr in Bezug auf die Sicherheit des Linux-Systems.
- http://www.securityportal.com — Diese Website enthält mehrere Neuigkeiten in Bezug auf die Sicherheit, Informationen über linuxspezifische Probleme und Dokumentation über die Entwicklung von effizienteren Sicherheitsmodellen und -methoden.

7.7.2 Zusätzliche Literatur

- *Securing and Optimizing Linux: Red Hat Edition* von Gerhard Mourani; OpenNA — Dieses Buch kann auch kostenlos als PDF-Datei unter http://www.openna.com heruntergeladen werden.
- *Secrets & Lies* von Bruce Schneier; John Wiley & Sons, Inc. — Eine sorgfältige und pragmatische Analyse der aktuellen Themen in Bezug auf die Systemsicherheit.

8 Pluggable Authentication Modules (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.

Mit Pluggable Authentication Modules (PAM) kann der Systemadministrator die Authentifizierungsregeln festlegen, ohne dass die Authentifizierungsprogramme neu kompiliert werden müssen. Mit PAM können Sie kontrollieren, wie bestimmte Authentifikationsmodule in ein Programm eingefügt werden, indem Sie die entsprechende PAM-Konfigurationsdatei dieses Programms in `/etc/pam.d` bearbeiten.

Die wenigsten Benutzer von Red Hat Linux werden diese Konfigurationsdatei für eines Ihrer Programme verwenden. Wenn Sie mit RPM Programme installieren, die eine Authentifizierung vornehmen müssen, so nehmen diese die für die normale Passwort- authentifizierung notwendigen Änderungen automatisch mit PAM vor. Wenn Sie jedoch eine benutzerdefinierte Konfiguration vornehmen möchten, sollten Sie mit der Struktur der Konfigurationsdateien von PAM vertraut sein. Weitere Informationen finden Sie unter Abschnitt 8.2.2, *PAM-Module*.

8.1 Vorteile von PAM

Wenn PAM korrekt angewendet wird, bietet es einem Systemadministrator viele Vorteile, wie zum Beispiel:

- Ein gemeinsames Authentifikationsschema, das für viele verschiedene Anwendungen verwendet werden kann.
- Die Möglichkeit, verschiedene Anwendungen zu implementieren, ohne die Anwendungen für PAM neu kompilieren zu müssen.
- Große Flexibilität und Kontrolle der Authentifizierung für Administratoren und Entwickler von Anwendungen.
- Anwendungsentwickler müssen ihr Programm nicht speziell für die Verwendung bestimmter Authentifikationsschmata entwickeln. Sie können sich statt dessen auf die Details ihres Programms konzentrieren.

8.2 PAM-Konfigurationsdateien

Die PAM-Konfigurationsdateien sind im Verzeichnis `/etc/ pam.d` enthalten (in früheren Versionen von PAM im Verzeichnis `/etc/pam.conf`). Solange der Eintrag `/etc/pam.d/` nicht gefunden wurde, wird `pam.conf` eingelesen (sollte aber nicht mehr verwendet werden).

Jede Anwendung (oder *Dienst*, wie Anwendungen im Allgemeinen bei Benutzern bekannt sind) hat seine eigene Datei. Jede Datei besteht aus fünf verschiedenen Elementen: **Dienstname**, **Modultyp**, **Steuer-Flags**, **Modulpfad** und **Argumente**.

8.2.1 PAM-Dienstnamen

Der Dienstname jeder PAM-aktiven Anwendung ist der Name der Konfigurationsdatei in `/etc/pam.d` dieser Anwendung. Jedes Programm, das PAM verwendet, definiert seinen eigenen Dienstnamen.

Das Programm login definiert den Dienstnamen `login`, ftpd definiert den Dienstnamen `ftp` usw.

Generell ist der Dienstname der Name des Programms, das zum *Zugriff* auf den Dienst verwendet wird und nicht das Programm, das den Dienst *bereitstellt*.

8.2.2 PAM-Module

PAM enthält vier verschiedene Modultypen für die Zugriffskontrolle auf bestimmte Dienste:

- `auth`-Module nehmen die eigentliche Authentifizierung vor (z.B. durch Erfragen und Überprüfen des Passworts) und erstellen Berechtigungsmerkmale, wie z.B. 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. Die Reihenfolge der gestapelten Module ist für den Authentifikationsprozess sehr wichtig, weil es dadurch für einen Administrator einfacher wird, zu erkennen, dass bereits einige Voraussetzungen erfüllt sind, bevor die Benutzerauthentifizierung stattgefunden hat.

Zum Beispiel verwendet `rlogin` in der Regel vier gestapelte Authentifizierungsmethoden, wie in der PAM-Konfigurations- datei zu sehen:

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

Bevor `rlogin` ausgeführt wird, stellt PAM fest, dass die `/etc/nologin` Dateien nicht existieren, dass sie auch nicht als Root angemeldet sind und dass alle Umgebungsvariablen geladen werden können. Wenn die `rhosts` -Authentifizierung erfolgreich ist, kann die Verbindung zugelassen werden. Ist die Authentifizierung nicht erfolgreich ist, wird zur Standardauthentifizierung mit Passwort übergegangen.

Es können jederzeit neue PAM-Module hinzugefügt werden. PAM-kompatible Anwendungen können dann so angepasst werden, dass diese Module verwendet werden können. Falls Sie z.B. über ein Rechensystem für Einmal-Passwörter verfügen und festlegen können, dass es von einem PAM-Modul unterstützt werden soll, 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. Das ist sehr nützlich, da Sie dadurch sehr schnell Authentifizierungsmethoden mit verschiedenen Programmen vermischen und vergleichen sowie testen können, ohne die Programme dafür neu kompiliert zu haben.

Dokumentationen über das Schreiben von Modulen finden Sie unter `/usr/share/doc/pam–<`*`version- number`*`>`.

8.2.3 PAM Steuer-Flags

Alle PAM-Module erstellen bei einer Überprüfung Fehler- oder Erfolgsmeldungen. Die Steuer-Flags geben PAM an, was mit diesen Ergebnissen geschehen soll. Während Module in einer bestimmten Reihenfolge gestapelt werden können, können Sie mit den Steuer-Flags die Wertigkeit eines Moduls in Bezug auf die nachfolgenden Module einstellen.

Die `rlogin` PAM-Konfigurationsdatei sieht dann wie folgt aus:

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

Nachdem der Modultyp festgelegt wurde, entscheidet das Steuer-Flag wie wichtig ein bestimmte Modul in Bezug auf das Gesamtziel ist, diesem Benutzer den Zugriff zu dem Programm zu erlauben.

Vier Arten von Steuer-Flags sind für PAM standartmäßig festgelegt:

- Mit `required` gekennzeichnete Module müssen erfolgreich überprüft werden, bevor die Authentifizierung erfolgen kann. Wenn ein `required` Modul Fehler entdeckt, wird der Benutzer dann darüber informiert, wenn auch alle anderen Module des gleichen Modultyps überprüft worden sind.
- Mit `requisite` gekennzeichnete Module müssen ebenfalls überprüft werden, bevor die Authentifizierung erfolgreich sein kann. Wenn ein `requisite` Modul jedoch Fehler entdeckt, wird der Benutzer hierüber sofort informiert. Diese Mitteilung zeigt das erste fehlerhafte `required` *oder* `requisite`-Modul an.
- Bei `sufficient` gekennzeichneten Modulen werden Fehler ignoriert. Wenn ein `sufficient` Modul jedoch erfolgreich überprüft wurde, und kein `required` Modul fehlschlägt, werden keine weiteren Module dieses Modultyps überprüft, und dieser Modultyp gilt als erfolgreich überprüft.
- `optional` gekennzeichnete Module sind für die erfolgreiche oder fehlgeschlagene Authentifizierung dieses Modultys nicht von Bedeutung. Sie werden dann wichtig, wenn kein anderes Modul dieses Modultyps erfolgreich war oder fehlgeschlagen ist. In diesem Fall bestimmt der Erfolg oder Misserfolg eines `optional` Moduls die gesamte PAM-Authentifikation für diesen Modultyp. .

Eine neuere Steuer-Flag Syntax mit immer mehr Kontrollmöglichkeiten steht nun für PAM zur Verfügung. Mehr Informationen über diese neue Syntax finden Sie in den PAM-Dokumentationen unter `/usr/share/doc/pam–<`*`version-number`*`>` .

8.2.4 PAM Modul-Pfade

Modulpfade geben PAM an, wo die Pluggable Module zu finden sind, die von dem ausgewählten Modultyp verwendet werden. Sie geben üblicherweise den kompletten Pfad zu einem Modul an, wie zum Beispiel `/lib/security/pam_stack.so`. Wenn der komplette Pfad jedoch nicht angegeben ist (oder anders ausgedrückt: der Pfad beginnt nicht mit einem `/`) wird angenommen, dass sich das angegebene Modul in der Datei `/lib/security` (die Standardspeicherstelle für PAM-Module) befindet. modules.

8.2.5 PAM-Argumente

PAM verwendet Argumente, um während der Authentifizierung Informationen über einen bestimmten Modultyp an Pluggable Module zu übermitteln. Mit diesen Argumenten können die PAM-Konfigurationsdateien bestimmter Programme gemeinsame PAM-Module in unterschiedlicher Weise verwenden.

Zum Beispiel verwendet das Modul `pam_userdb.so` versteckte Dateien aus der Berkeley DB-Datei, um den Benutzer zu authentifizieren. (Berkeley DB ist ein in vielen Anwendungen eingebundenes Open-Source-Datenbank System, das zum Aufspüren einer bestimmten Art von Informationen erstellt wurde.) Das Modul verwendet ein `db` Argument, das für die verschiedenen Serviceleistungen unterschiedlich sein kann, und spezifiziert den von Berkeley DB zu verwendenden Dateinamen.

Eine `pam_userdb.so` Zeile in einer PAM- Konfigurationsdatei sieht wie folgt aus:

```
auth      required  /lib/security/pam_userdb.so db=path/to/file
```

Ungültige Argumente werden ignoriert und wirken sich auch nicht auf den Erfolg oder Misserfolg eines PAM-Moduls aus. Wenn ein ungültiges Argument auftaucht, erscheint in `/var/log/messages` normalerweise eine Fehlermeldung. Wenn jedoch diese Methode der Fehlermeldung durch ein PAM-Modul überwacht wird, muss das Modul den Fehler korrekt anzeigen.

8.2.6 Beispiele für PAM-Konfigurationsdateien

Eine Konfigurationsdatei einer PAM-Anwendung sieht wie folgt aus:

```
#%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 den Zeichen #). Die Zeilen zwei bis vier stapeln drei Module für die Authentifizierung bei der Anmeldung.

```
auth      required  /lib/security/pam_securetty.so
```

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.

```
auth      required  /lib/security/pam_unix.so shadow nullok
```

Zeile drei sorgt dafür, dass der Benutzer nach dem Passwort gefragt wird und dass dieses überprüft wird

```
auth      required  /lib/security/pam_nologin.so
```

Zeile vier prüft, ob die Datei `/etc/nologin` existiert. Falls sie existiert, und der Benutzer nicht als Root angemeldet ist, schlägt die Authentifizierung fehl.

Beachten Sie, dass alle drei `auth` Module überprüft werden, *auch wenn schon beim ersten `auth` Modul Fehler auftreten*. Dadurch wird verhindert, 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, diese zu knacken. Sie können diese Einstellung ändern, indem Sie statt `required` `requisite` eintragen. Wenn alle `requisite` Module Fehlermeldungen liefern, bricht PAM sofort ab, ohne weitere Module aufzurufen.

```
account   required  /lib/security/pam_unix.so
```

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.

```
password  required  /lib/security/pam_cracklib.so
```

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 Programm zum Knacken von Passwörtern, herausgefunden werden kann.

```
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
```

Die siebte Zeile 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.)

```
session   required  /lib/security/pam_unix.so
```

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 `sufficient` und `requisite` ist die Reihenfolge wichtig.

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

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

Erstens überprüft `pam_nologin.so`, ob `/etc/nologin` existiert. Ist dies der Fall, kann sich niemand anmelden, mit Ausnahme des Rootbenutzers.

```
auth       required     /lib/security/pam_securetty.so
```

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, siehe unter Abschnitt 8.4, *`rlogin`, `rsh`, und `rexec` mit PAM verwenden*).

```
auth       required     /lib/security/pam_env.so
```

Drittens lädt das `pam_env.so` Modul die Umgebungsvariablen, die in `/etc/security/pam_env.conf` spezifiziert sind. .

```
auth       sufficient   /lib/security/pam_rhosts_auth.so
```

Viertens: Wenn `pam_rhosts_auth.so` den Benutzer, der `.rhosts` in der Benutzer-Home-Dierctory authentifiziert hat, wird `rlogin` sofort von PAM authentifiziert, ohne das Passwort mit `pam_stack.so` zu überprüfen. Eine gescheiterte Authentifizierung des Benutzers durch `pam_rhosts_auth.so` wird ignoriert.

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

Fünftens: Wenn die Authentifizierung des Benutzers durch `pam_rhosts_auth.so` gescheitert ist, führt das `pam_stack.so` Modul eine normale Passwort-Authentifizierung durch, und erhält das `service=system-auth` Argument.

Bitte beachten

Wenn Sie den Prompt beim Eingeben des Passworts nicht angezeigt haben möchten, nachdem die `securetty` Prüfung fehlgeschlagen ist, und feststellen, dass ein Benutzer sich als Root anmelden möchte, können Sie das `pam_securetty.so` Modul von `required` in `requisite` ändern. Wenn Sie alternativ Anmeldungen als Root zulassen möchten (was nicht zu empfehlen ist), können Sie diese Zeile auskommentieren.

8.3 Shadow-Passwörter

Das Modul `pam_unix.so` erkennt automatisch, dass Sie Shadow-Passwörter verwenden und benutzt diese zur Benutzerauthentifizierung.

Weitere Informationen über die Shadow-Passwörter erhalten Sie unter Abschnitt 12.1, *Shadow Dienstprogramme*

8.4 `rlogin`, `rsh`, und `rexec` mit PAM verwenden

Aus Sicherheitsgründen sind `rexec`, `rsh` , und `rlogin` in Red Hat Linux 7.1 standardmäßig nicht aktiviert. Statt dessen sollten Sie die OpenSSH Tools verwenden. Informationen über diese Tools finden Sie unter Kapitel 11, *SSH-Protokoll* und im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*.

Wenn Sie `rexec`, `rsh` und `rlogin` verwenden und diese als Root ausführen, müssen Sie die Datei `/etc/securetty` neu modifizieren. Alle drei Tools haben PAM-Konfigurationsdateien, die ein `pam_securetty.so` PAM-Modul erfordern. Somit müssen Sie `/etc/securetty` so bearbeiten, dass der Zugriff als Root erfolgen kann.

Bevor Sie sich als Root anmelden können und diese Tools verwenden, müssen Sie sie korrekt eingestellt haben. Installieren Sie als Erstes `rsh-server` RPM (in Red Hat Linux 7.1 enthalten). Hilfe für die Anwendung von RPM erhalten Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*.

Führen Sie als nächstes `ntsysv` aus und aktivieren Sie `rexec`, `rsh`, und `rlogin`. Hilfe für die Verwendung dieses Tools finden Sie in der `ntsysv` man-Seite.

Starten Sie dann `xinetd` mit `/sbin/service xinetd restart` erneut, um die `ntsysv` Änderungen zu aktivieren. Ab diesem Zeitpunkt können alle Benutzer, mit Ausnahme von Root, `rexec`, `rsh` und `rlogin` verwenden.

Um Root die Verwendung dieser Tools zu erlauben, fügen Sie die Namen der Tools, die Sie verwenden möchten, in `/etc/securetty` ein. Wenn Sie möchten, dass Root `rexec`, `rsh` und `rlogin` soll, fügen Sie `/etc/securetty` die folgenden Zeilen hinzu:

```
rexec
rsh
rlogin
```

Um das Anmelden zu ermöglichen, wenn Root diese Tools per `telnet` verwendet (eine sehr schlechte Idee, jedoch in manchen Umbegungen notwendig), fügen Sie einige Zeilen mehr hinzu:

```
pts/0
pts/1
```

8.5 Zusätzliche Ressourcen

Dieses Kapitel enthält nur einen Teil der verfügbaren Informationen über PAM. Es gibt verschiedene zusätzliche Informationsquellen, die bei der Konfiguration und Verwendung von PAM in Ihrem System recht wertvoll sind.

8.5.1 Installierte Dokumentationen

- `pam` man-Seite — Gute Information zur Einführung von PAM, einschließlich Aufbau und Zweck der PAM- Konfigurationsdateien.
- `/usr/share/doc/pam-<version-number>` — Enthält sehr gute HTML-Dokumentationen für PAM, einschließlich *System Administrators' Guide* (Leitfaden für den Systemadministrator), *Module Writers' Manual* (Handbuch für Modulentwickler), *Application Developers' Manual* (Handbuch für den Anwendungsentwickler) und PAM-Standard DCE-RFC 86.0.

8.5.2 Hilfreiche Websites

- http://www.kernel.org/pub/linux/libs/pam — Die wichtigste Distribution-Website für Linux-PAM. Sie enthält Informationen über die verschiedenen PAM-Module und Anwendungen die verwendet oder entwickelt werden, FAQ und zusätzliche Dokumentationen über PAM.

Zusätzlich empfehlen wir Ihnen, bevor Sie mit PAM zu arbeiten beginnen, sich so viele Beispiele von Konfigurationsdateien wie möglich anzuschauen. Viele Websites bieten codierte Beispiele für Administratoren (zur Änderung von Standardkonfigurationsdateien) und Anwendungsentwickler (zur Verwendung von PAM mit ihren Programmen).

9 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 immer verschlüsselt im Netzwerk versendet.

9.1 Wozu Kerberos verwenden?

Die meisten herkömmlichen Netzwerksysteme verwenden passwortbasierte 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.

9.2 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 (wie z.B. `/etc/passwd` oder `/etc/shadow`)in eine Kerberos- Passwortdatenbank. Eine übertragung ist technisch möglich. Dies im Einzelnen zu beschreiben, würde dem Umfang dieses Kapitels überschreiten. Hilfe

bei der Entscheidung, ob eine Passwortübertragung für Ihre Kerberos-Installation sinnvoll ist, finden Sie unter Kerberos FAQ http://www.nrl.navy.mil/ CCS/people/kenh/kerberos-faq.html#pw-convert Question 2.23 zusätzliche Informationen erhalten Sie auch unter Abschnitt 9.8, *Weitere Informationen*.

- 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 9.7, *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.
- Kerberos nimmt an, dass Sie sichere Hosts auf einem unsicherem Netzwerk verwenden. Seine wichtigste Augfabe ist der Schutz von Passwörtern im Klartext wenn Sie im Netzwerk versendet werden. Wenn jedoch irgendein anderer als der richtige Benutzer tatsächlich Zugriff auf alle Hosts hat (insbesondere auf den Host, der die Tickets zur Authentifizierung enthält) besteht die Gefahr, dass das gesamte Kerberos Authentifizierungssystem abgehört werden kann.
- 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.

9.3 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-Datei

Credential Cache oder Ticket-Datei — 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

Daten, die zum Verschlüsseln bzw. Entschlüsseln von Daten verwendet werden. 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 Service, der Kerberos-Tickets ausgibt (normalerweise auf dem gleichen Host wie Ticket Granting Server).

key table oder keytab

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 leerem 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

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

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 Service (TGS)

Vergibt Tickets für einen angeforderten Service, die vom Benutzer verwendet werden, um Zugang zu diesem Service zu erhalten. TGS wird üblicherweise auf dem gleichen Host wie KDC ausgeführt.

Ticket Granting Ticket (TGT)

Ein spezielles Ticket, das es dem Client ermöglicht, zusätzliche Tickets zu erhalten, ohne diese beim KDC anfordern zu müssen.

9.4 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. 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 erhalten Sie unter Abschnitt 9.8, *Weitere Informationen*.

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-`*`Versions-nummer`*` /` im PostScript- und im HTML-Format zur Verfügung steht.

9.5 Einrichten von Kerberos5 Servern in Red Hat Linux 7.1

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. Stellen Sie sicher, dass Sie ein Zeitsynchronisierungsprogramm haben und DNS eingerichtet ist, bevor Sie Kerberos 5 installieren. Achten Sie im Besonderen auf die Zeitsynchronisation zwischen dem Kerberos-Server und seinen verschiedenen Clients. Wenn zwischen dem Server und

den Clients eine Differenz von mehr als 5 Minuten besteht (diese Standardgröße kann in Kerberos 5 konfiguriert werden), können die Kerberos-Clients nicht von Server authentifiziert werden. Diese Zeitsynchronisierung ist nötig zum Schutz vor Hackern, die sich mit Hilfe einer alten Berechtigung als gültigen Benutzer ausgeben.

Sie sollten ein Network Time Protocol (NTP) kompatibles Client/ Server Netzwerk bei der Verwendung von Red Hat Linux einrichten, vor allem, wenn Sie Kerberos nicht benutzen. Red Hat Linux 7.1 enthält das `ntp` Paket für die entsprechendene Installation. Zusätzliche Informationen über NTP erhalten Sie unter http://www. eecis.udel.edu/~ntp.

2. Installieren Sie die Pakete `krb5-libs`, `krb5-server` und `krb5-workstation` auf dem 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. Es enthält `krb5`, ein GUI-Tool für das Verwalten von Tickets, und `gkadmin`, ein GUI-Tool für das Verwalten von Kerberos- Realms.

3. 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.

4. 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` bewirkt 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).

5. 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 und verwenden Kerberos zum Verarbeiten von Authentifizierungen. Bevor Sie zu Verwaltungszwecken über das Netzwerk eine Verbindung mit dem Server herstellen können, müssen Sie einen Principal erzeugen. Erstellen Sie diesen ersten Principal mit dem Befehl `kadmin.local`, der speziell dafür entwickelt wurde, auf dem gleichen Host angewendet zu werden, das auch für KDC verwendet wird. Er benutzt Kerberos nicht zur Authentifizierung.

Geben Sie am KDC-Terminal folgenden `kadmin.local` Befehl ein, um den ersten Principal zu erzeugen:

```
/usr/kerberos/sbin/kadmin.local -q "addprinc
Benutzername/admin"
```

6. Starten Sie Kerberos mit Hilfe der folgenden Befehle:

```
/sbin/service krb5kdc start
/sbin/service kadmin start
/sbin/service krb524 start
```

7. Fügen Sie für Ihre Benutzer Principals hinzu. Verwenden Sie dazu den `addprinc` Befehl mit `kadmin` oder die `gkadmin`-Menüoption **Principal** => **Add** (Hinzufügen). `kadmin` (und `kadmin.local` im Master-KDC) ist ein Befehlszeilen-Interface für das Kerberos-Administrationssystem. Nachdem das Programm `kadmin` gestartet wurde, stehen Ihnen viele Befehle zur Verfügung. Unter der `kadmin` man-Seite finden Sie weiter Informationen.

8. 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 im System (nicht im Kerberos-Server) 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 (`kinit` *`principal`*) 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.

9.6 Einrichten von Kerberos 5 Clients in Red Hat Linux 7.1

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. Stellen Sie sicher, dass zwischen dem Kerberos-Client und KDC Zeitsynchronisation besteht. Unter Abschnitt 9.5, *Einrichten von Kerberos5 Servern in Red Hat Linux 7.1* erhalten Sie weitere Informationen. Zusätzlich sollte vor der Installation des Kerberos-Client-Programms, DNS auf dem Kerberos-Client korrekt eingerichtet sein.

2. 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.

3. 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.

4. Darüber hinaus müssen auch andere kerberisierte Netzwerkdienste gestartet werden. Um den kerberisierten `telnet`- Dienst verwenden zu können, müssen Sie `krb5-telnet` 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.

9.7 Kerberos und Pluggable Authentication Modules (PAM)

Derzeit 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.

9.8 Weitere Informationen

Für neue Benutzer könnte Kerberos schwierig zu verstehen, zu implementieren und zu konfigurieren sein. Weitere Beispiele und Anleitungen für Kerberos finden Sie in folgenden Informationsquellen:

9.8.1 Installierte Dokumentationen

- `/usr/share/doc/krb5-server-<version- number>` — Der *Kerberos V5 Installations-Guide* und der *Kerberos V5 System Administrator's Guide*, in PostScript und HTML Format, sind in `krb5-server` RPM installiert.
- `/usr/share/doc/krb5-workstation-< version-number>` — Der *Kerberos V5 UNIX User's Guide*, in PostScript und HTML Format sind in `krb5-workstation` RPM installiert.

9.8.2 Hilfreiche Websites

- http://web.mit.edu/ kerberos/www — Die Kerberos-Homepage auf der Website von MIT.
- http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq. html — Die Seite mit den am häufigsten gestellten Fragen zu Kerberos (Frequently Asked Questions - FAQ).
- ftp: //athena-dist.mit.edu/pub/kerberos/doc/usenix.PS — Ein Link zu einer PostScript-Version von *Kerberos: An Authentication Service for Open Network Systems* von Jennifer G. Steiner, Clifford Neuman und Jeffrey I. Schiller. Dieses Dokument ist die Originalbeschreibung zu Kerberos.
- 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.

10 Installieren und Konfigurieren von Tripwire

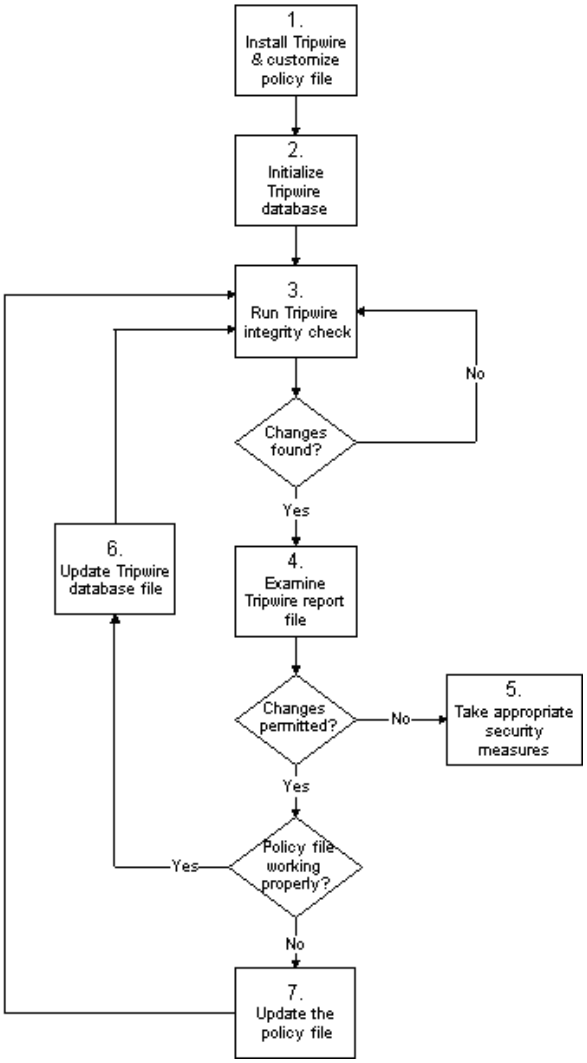
Die Tripwire Software unterstützt Sie dabei, die Unversehrtheit von kritischen Systemdateien und -verzeichnissen sicherzustellen, indem sie alle erfolgten Änderungen feststellt. In den Konfigurationsoptionen von Tripwire sind auch Warnmeldungen per E-Mail vorgesehen, wenn bestimmte Dateien geändert wurden, sowie eine automatische Prüfung der Dateiintegrität durch eine `cron` Funktion vor. Der Gebrauch von Tripwire für das Ermitteln von unerlaubten Zugriffen und Schäden ermöglicht es Ihnen, Änderungen im System zu verfolgen und die Wiederherstellung des Systems zu beschleunigen, indem die Anzahl der hierzu notwendigen und zurückzugewinnenden Dateien reduziert wird.

Tripwire vergleicht die Dateien und Verzeichnisse mit einer Basisdatenbank mit den Orten, an denen die Dateien abgelegt sind, den geänderten Daten sowie anderen Informationen. Die Datenbank wird erstellt, indem bestimmt Dateien und Verzeichnisse in einem bekannten sicheren Status aufgezeichnet werden. (Um eine maximale Sicherheit zu gewährleisten, sollte Tripwire installiert und die Datenbank erstellt werden, bevor das System das Risiko eines unberechtigten Zugriffs läft.) Nachdem die Basisdatenbank erstellt wurde, vergleicht Tripwire das aktuelle System mit der Datenbank und liefert einen Bericht aller Änderungen, Zusätze oder Löschvorgänge.

10.1 Der Gebrauch von Tripwire

Das folgende Flussdiagramm zeigt, wie Tripwire verwendet werden sollte:

Abbildung 10–1 Der Gebrauch von Tripwire



Folgende Schritte sind für die korrekte Installation, den Gebrauch und die Wartung von Tripwire notwendig:

1. *Installieren von Tripwire und benutzerdefiniertes Einstellen der Policy-Datei* — Wenn Sie es noch nicht getan haben, installieren Sie `Tripwire` RPM (siehe Abschnitt 10.2.1, *RPM Installationsanweisungen*). Benutzerdefinieren Sie anschließend die Beispieldateien für die Konfiguration (`/etc/tripwire/twcfg.txt`) und (`/etc/tripwire/twpol.txt`) und führen Sie das Konfigurationsskript (`/etc/tripwire/twinstall.sh`) aus. Mehr Informationen hierzu finden Sie unter Abschnitt 10.2.2, *Anweisungen für die Schritte nach der Installation*.

2. *Initialisieren der Tripwire Datenbank* — Erstellen Sie eine Datenbank der zu prüfenden kritischen Dateien auf der Grundlage der neuen Tripwire Policy-Datei (`/etc/tripwire/tw.pol`). Weitere Informationen finden Sie unter Abschnitt 10.7, *Initialisieren der Datenbank*.

3. *Ausführen einer Tripwire Integritätsprüfung* — Vergleichen Sie die neu erstellte Tripwire Datenbank mit den aktuellen Systemdateien, wobei fehlende oder geänderte Dateien ermittelt werden. Weitere Informationen finden Sie unter Abschnitt 10.8, *Ausführen einer Integritätsprüfung*.

4. *Analyse der Tripwire Berichtdatei* — Zeigen Sie die Tripwire Berichtdatei mithilfe von `twprint` an, um Differenzen zu ermitteln. Weitere Informationen finden Sie unter Abschnitt 10.9, *Drucken der Berichte*.

5. *Ergreifen angemessener Sicherheitsmaßnahmen* — Wenn an den genannten Dateien unrechtmäßige Änderungen vorgenommen wurden, können Sie die Originale über Sicherheitskopien wiederherstellen oder aber das Programm neu starten.

6. *Aktualisieren der Tripwire Datenbank* — Wurde die Integrität der Dateien effektiv und rechtmäßig geändert (z.B. wenn Sie absichtlich eine Datei bearbeiten oder ein bestimmtes Programm ersetzen), müssen Sie die Datenbankdatei von Tripwire anweisen, diese Änderungen in den zukünftigen Berichten nicht als Integritätsverletzungen auszuweisen. Weitere Informationen finden Sie unter Abschnitt 10.10, *Aktualisieren der Datenbank nach einer Integritätsprüfung*.

7. *Aktualisieren der Tripwire Policy-Datei* — Wenn Sie die Liste der von Tripwire geprüften Dateien oder die Art und Weise ändern möchten, wie die Anwendung Differenzen bearbeitet, dann rufen Sie die Beispieldatei (`/etc/tripwire/twpol.txt`) auf, erstellen eine unterzeichnete Kopie (`/etc/tripwire/tw.pol`) und aktualisieren Sie die Tripwire Datenbank. Weitere Informationen finden Sie unter Abschnitt 10.11, *Aktualisieren der Policy-Datei*.

In den entsprechenden Abschnitten dieses Kapitels finden Sie detaillierte Anweisungen für die Ausführung dieser Schritte.

10.2 Installationsanweisungen

Nach der Installation muss Tripwire korrekt initialisiert werden, um eine kontinuierliche Kontrolle der Dateien zu gewährleisten. In den folgenden Abschnitten wird beschrieben, wie das Programm installiert wird (falls dies noch nicht getan wurde) und wie die Tripwire Datenbank zu initialisieren ist.

10.2.1 RPM Installationsanweisungen

Die einfachste Art, Tripwire zu installieren, ist, bei der Installation von Red Hat Linux 7.1 die Datei `Tripwire` RPM zu installieren. Sollten Sie Red Hat Linux 7.1 bereits installiert haben, können Sie zu diesem Zweck RPM, Gnome-RPM oder Kpackage verwenden. Im Folgenden wird dieser Prozess mithilfe von RPM beschrieben:

1. Legen Sie das Verzeichnis `RedHat/RPMS` auf der Red Hat Linux 7.1 CD-ROM ab.
2. Legen Sie die binäre RPM-Datei `Tripwire` ab, indem Sie `ls -l tripwire*` in das Verzeichnis `RedHat/RPMS` eingeben.
3. Geben Sie `rpm -Uvh <Name>` ein (wobei *<Name>* der Name der Tripwire RPM-Datei des Schrittes 2 ist).
4. Folgen Sie nach der Installation der `Tripwire` RPM-Datei den unten angeführten Anweisungen für die Schritte nach der Installation.

Bitte beachten

Die Release Notes und die `README` Datei sind in `/usr/share/doc/tripwire-<Version-Nummer>` abgelegt. Diese Dokumente enthalten wichtige Informationen über die standardmäßige Policy- Datei und andere Themen.

10.2.2 Anweisungen für die Schritte nach der Installation

Die `Tripwire` RPM-Datei installiert die Programmdateien, die für das Ausführen der Software erforderlich sind. Nach der Installation von Tripwire muss die Anwendung wie im Folgenden beschrieben konfiguriert werden:

1. Wenn Sie bereits wissen, dass an der Konfigurationsdatei (`/etc/tripwire/twcfg.txt`) oder der Policy-Datei (`/etc/tripwire/twpol.txt`) Änderungen vorgenommen werden müssen, dann bearbeiten Sie diese Dateien jetzt.

Bitte beachten

Während Sie die genannten Dateien bearbeiten sollten, um Tripwire individuell auf Ihr System einzustellen, ist eine solche Bearbeitung nicht erforderlich, um Tripwire zu verwenden. Wenn Sie vorhaben, eine der Dateien zu ändern, dann sollten Sie dies tun, bevor Sie das Konfigurationsskript (`/etc/tripwire/twinstall.sh`) ausführen. Wenn Sie die Konfigurationsdatei oder die Policy-Datei bearbeiten, nachdem das Konfigurationsskript ausgeführt wurde, müssen Sie es vor der Initialisierung der Datenbankdatei erneut ausführen. Beachten Sie, dass Sie die Konfigurationsdatei und die Policy-Datei bearbeiten *können, nachdem* die Datenbankdatei initialisiert und eine Integritätsprüfung ausgeführt wurde.

---

2. Geben Sie `/etc/tripwire/twinstall.sh` in der Befehlszeile als Root ein und drücken Sie [Enter], um das Konfigurationsskript auszuführen. Das `twinstall.sh` Skript bearbeitet das Einstellen von Schlüsseln und erstellt dabei die Verschlüsselungen, die die Konfigurations- und Policy-Datei von Tripwire schützen, und unterzeichnet diese Dateien. Weitere Informationen über das Einstellen von Schlüsseln finden Sie unter Abschnitt 10.6, *Auswählen der Schlüssel*.

Bitte beachten

Nach der Verschlüsselung und der Unterzeichnung sollten die Konfigurationsdatei (`/etc/tripwire/tw.cfg`) und die Policy-Datei (`/etc/tripwire/tw.pol`), die beim Ausführen des `/etc/tripwire/twinstall.sh` Skripts erstellt wurden, nicht mehr umbenannt oder verschoben werden.

---

3. Initialisieren Sie die Tripwire Datenbankdatei, indem Sie `/usr/sbin/tripwire --init` in der Befehlszeile eingeben.
4. Geben Sie `/usr/sbin/tripwire --check` in der Befehlszeile ein, um die erste Integritätsprüfung auszuführen, wobei Ihre neue Tripwire Datenbank mit Ihren Systemdateien verglichen wird, und suchen Sie im erstellten Bericht nach Fehlern.

Sobald Sie diese Schritte erfolgreich ausgeführt haben, besitzt Tripwire einen Überblick über Ihr Dateisystem, das die Anwendung in der Folge nach Änderungen in kritischen Dateien überprüft. Darüber

hinaus wird durch die `tripwire` RPM-Datei eine Datei mit dem Namen `Tripwire-Prüfung` in das `/etc/cron.daily` Verzeichnis eingefügt, die automatisch ein Mal pro Tag eine Integritätsprüfung ausführt.

10.3 Datei-Speicherstellen

Bevor Sie Tripwire verwenden, sollten Sie wissen, wo für die Anwendung wichtige Dateien abgelegt sind. Tripwire speichert die zugehörigen Dateien je nach Funktion an verschiedenen Stellen:

- Das `/usr/sbin` Verzeichnis speichert die Programme `tripwire`, `twadmin` und `twprint`.
- Das `/etc/tripwire` Verzeichnis enthält die lokalen Schlüssel und die Site-Schlüssel (`*.key` files), das Installationsskript (`twinstall.sh`) sowie die Konfigurationsdatei und Policy-Datei und deren Beispiele.
- Das `/var/lib/tripwire` Verzeichnis enthält die Tripwire Datenbank der Dateien Ihres Systems (`*.twd`) und ein `report` Verzeichnis, in dem die Tripwire Berichte gespeichert sind. Die Tripwire Berichte mit dem Namen *`Rechner_Name-Datum des_Berichts-_Uhrzeit des Berichts`*`.twr` listet die Differenzen zwischen der Tripwire Datenbank und Ihrem aktuellen System detailliert auf.

10.4 Tripwire Konponenten

Die Tripwire Policy-Datei ist eine Textdatei mit Kommentaren, Regeln, Anweisungen und Variablen. Sie bestimmt die Art, mit der Tripwire Ihr System prüft. Jede in dieser Datei enthaltene Regel gibt ein Systemobjekt an, das geprüft werden soll. Weiterhin bestimmen diese Regeln, welche Änderungen in einem Bericht angezeigt und welche ignoriert werden sollen.

Systemobjekte sind die Dateien und Verzeichnisse, die überprüft werden sollen. Jedes Objekt besitzt einen Namen. Eine Eigenschaft bezieht sich auf ein einzelnes Objektmerkmal, das Tripwire überprüft. Anweisungen verwalten die bedingte Verarbeitung von Regelsätzen in einer Policy-Datei. Bei der Installation wird die textbasierte Policy-Datei verschlüsselt, umbenannt und in die effektive Policy-Datei (`/etc/tripwire/tw.pol`) umgewandelt.

Nach der ersten Initialisierung verwendet Tripwire die Regeln der unterzeichneten Policy-Dateien, um die Datenbankdatei (`/var/lib/tripwire/`*`Rechner_Name`*`.twd`) zu erstellen. Diese Datei enthält eine Übersicht über das System in einem bekannten sicheren Status. Tripwire vergleicht diese Basisdatei mit dem aktuellen System, um eventuelle Änderungen zu ermitteln. Dieser Vorgang ist die sog. **Integritätsprüfung**.

Bei der Integritätsprüfung erstellt Tripwire Berichtdateien im `/var/lib/tripwire/report` Verzeichnis. In diesen Dateien sind kurz die Änderungen dargestellt, die nicht den Regeln der Policy-Dateien entsprechen.

In der Tripwire Konfigurationsdatei (`/etc/tripwire/tw.cfg`) werden systemspezifische Informationen wie die Speicherstellen von Tripwire Datendateien gespeichert. Tripwire generiert bei der Installation die notwendigen Informationen für die Konfigurationsdatei, der Systemadministrator kann die Parameter dieser Datei jedoch jederzeit ändern. Beachten Sie, dass die geänderte Konfigurationsdatei ebenso unterzeichnet werden muss wie die Policy-Datei, damit sie standardmäßig verwendet werden kann.

Die Variablen der Konfigurationsdatei **POLFILE**, **DBFILE**, **REPORTFILE**, **SITEKEYFILE** und **LOCALKEYFILE** geben die Speicherstellen der Policy-Datei, der Datenbankdatei, der Berichtdateien und der Dateien der Siteschlüssel sowie der lokalen Schlüssel an. Diese Variablen werden standardmäßig bei der Installation definiert. Wenn Sie die Konfigurationsdatei bearbeiten und eine oder mehrere der Variablen nicht definieren, wird diese Datei von Tripwire als ungültig betrachtet. Dies verursacht einen Fehler und beendet das Programm.

Beachten Sie, dass die geänderte Konfigurationsdatei ebenso unterzeichnet werden muss wie die Policy-Datei, so dass sie von Tripwire verwendet werden kann. Anweisungen für die Unterzeichnung der Konfigurationsdatei finden Sie unter Abschnitt 10.11.1, *Unterzeichnen der Konfigurationsdatei*.

10.5 Ändern der Policy-Datei

Indem Sie die Policy-Datei (`twpol.txt`) entsprechend ändern, können Sie bestimmen, auf welche Art und Weise Tripwire Ihr System prüfen soll. Wenn Sie die genannte Datei an Ihre individuelle Systemkonfiguration anpassen, steigern Sie den Nutzen von Tripwire Berichten, da Sie die Anzahl der falschen Warnmeldungen für Dateien oder Programme reduzieren, die Sie zwar nicht verwenden, Tripwire jedoch weiterhin als geändert oder fehlend angibt.

Legen Sie die standardmäßige Policy-Datei unter `/etc/tripwire/twpol.txt` ab. Eine Beispieldatei (die unter `/usr/share/doc/tripwire-<`*`Version-Nummer`*`>/policy-guide.txt` abgelegt ist) ist hier enthalten, die Ihnen als Einführung in die Policy-Datei dient. Lesen Sie in den Anweisungen in dieser Musterdatei, wie die standardmäßige Policy-Datei bearbeitet wird.

Wenn Sie die Policy-Datei unmittelbar nach der Installation des `Tripwire` Pakets ändern, stellen Sie sicher, dass Sie `/etc/tripwire/twinstall.sh` eingeben, um das Konfigurationsskript auszuführen. Dieses Skript unterzeichnet die geänderte Policy-Datei und benennt sie um in `tw.pol`. Hierbei handelt es sich nun um die effektive Policy-Datei, die das `tripwire` Programm bei seiner Ausführung verwendet.

Wenn Sie das Beispiel der Policy-Datei nach Ausführen des Konfigurationsskripts ändern, lesen Sie in Abschnitt 10.11, *Aktualisieren der Policy-Datei* die Anweisungen, wie Sie die Datei unterzeichnen müssen, um sie in die geforderte `tw.pol` Datei umzuwandeln.

Bitte beachten

Wenn Sie das Beispiel der Policy-Datei ändern, wird diese Datei erst dann von Tripwire verwendet, wenn sie unterzeichnet, verschlüsselt und in die neue `/etc/tripwire/tw.pol` Datei umgewandelt wurde (siehe Abschnitt 10.11, *Aktualisieren der Policy-Datei*).

10.6 Auswählen der Schlüssel

Tripwire Dateien werden mit Site-Schlüsseln oder lokalen Schlüsseln unterzeichnet oder verschlüsselt. Diese Schlüssel verhindern, dass die Konfiguration, die Policy-Datei, die Datenbank und die Berichtdateien von unbefugten Benutzern eingesehen und geändert werden. Mit anderen Worten: auch wenn sich ein Unbefugter als Root in Ihrem System anmeldet, ist er nicht in der Lage, die Tripwire Dateien so zu ändern, dass er seine Spuren verwischen kann (es sei denn, er kennt die Schlüssel). Bei der Auswahl der Schlüssel müssen Sie jeweils mindestens acht alphanumerische und symbolische Zeichen eingeben. Die maximale Länge eines solchen Schlüssels sind 1023 Zeichen. Anführungszeichen sollten dabei nicht verwendet werden. Versichern Sie sich darüber hinaus, dass sich Ihr Schlüssel vollständig vom Root-Passwort Ihres Systems unterscheidet.

Stellen Sie sowohl für den Site-Schlüssel als auch für den lokalen Schlüssel einen eigenen Schlüssel ein. Der Site-Schlüssel dient der Unterzeichnung der Konfigurations- und Policy-Dateien. Der lokale Schlüssel wird für die Unterzeichnung der Tripwire Datenbank und der Berichtdateien verwendet.

Speichern Sie die Schlüssel an einer sicheren Stelle. *Wenn Sie Ihren Schlüssel vergessen, besteht keine Möglichkeit mehr, eine unterzeichnete Datei zu entschlüsseln.* Die Dateien sind daher unbrauchbar und Sie müssen das Konfigurationsskript erneut ausführen, das wiederum die Tripwire Datenbank erneut initialisiert.

10.7 Initialisieren der Datenbank

Bei der Initialisierung der Datenbank erstellt Tripwire auf der Grundlage der Regeln in der Policy-Datei eine Reihe von Dateisystem-Objekten. Diese Datenbank dient als Basis für die Integritätsprüfung.

Geben Sie den folgenden Befehl ein, um die Tripwire Datenbank zu initialisieren:

```
/usr/sbin/tripwire --init
```

Die Ausführung dieses Befehls erfordert einige Minuten.

10.8 Ausführen einer Integritätsprüfung

Bei der Integritätsprüfung vergleicht Tripwire die aktuellen Dateisystem-Objekte mit den in der Datenbank gespeicherten Eigenschaften. Eventuelle Differenzen werden standardmäßig gedruckt und in einer Berichtdatei gespeichert, auf die anschließend über `twprint` zugegriffen werden kann. Weitere Informationen über die Anzeige der Tripwire Berichte finden Sie unter Abschnitt 10.9, *Drucken der Berichte*.

Eine Option der E-Mail-Konfiguration in der Policy-Datei ermöglicht es, dass besondere Mitteilungen an bestimmte E-Mail-Adressen gesendet werden, wenn Differenzen bei der Integritätsprüfung ermittelt wurden. Weiter Informationen hierzu finden Sie unter Abschnitt 10.12, *Tripwire und E-Mail*.

Verwenden Sie den folgenden Befehl, um eine Integritätsprüfung auszuführen:

```
/usr/sbin/tripwire --check
```

In den meisten Fällen erfordert die Ausführung dieses Befehls eine gewisse Zeit. Dies hängt auch von der Anzahl der zu prüfenden Dateien ab.

10.9 Drucken der Berichte

Der Befehl `twprint -m r` zeigt den Inhalt eines Tripwire Berichts in Klartext an. Weisen Sie `twprint` an, welcher Bericht angezeigt werden soll.

Ein `twprint` Befehl für das Drucken von Tripwire Berichten sieht ähnlich wie folgt aus (geben Sie den Befehl auf einer einzigen Zeile ein):

```
/usr/sbin/twprint -m r --twrfile
          /var/lib/tripwire/report/<Name>.twr
```

Die `-m r` Option des Befehls weist `twprint` einen Tripwire Bericht zu dekodieren. Die `--twrfile` Option weist `twprint` an, eine bestimmte Tripwire Berichtdatei zu verwenden.

Der Name des Tripwire Berichts, den Sie anzeigen möchten, enthält den Namen des Rechners, den Tripwire für den Bericht geprüft hat, sowie das Datum und die Uhrzeit des Berichts. Sie können zuvor gespeicherte Berichte jederzeit wieder anzeigen. Geben Sie hierzu einfach `ls /var/lib/tripwire/report` ein. Es erscheint eine Liste der Tripwire Berichte.

Tripwire Berichte können sehr lang sein, was allerdings von der Anzahl der ermittelten Differenzen oder Fehlern abhängt. Ein Beispielbericht startet wie folgt:

```
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            Fri Jan 12 04:04:42 2001
```

```
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================================
Report Summary:
===============================================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --check

===============================================================================
Rule Summary:
===============================================================================
-------------------------------------------------------------------------------
Section: Unix File System
-------------------------------------------------------------------------------
  Rule Name                Severity Level    Added    Removed  Modified
  ---------                --------------    -----    -------  --------
  Invariant Directories    69                0        0        0
  Temporary directories    33                0        0        0
* Tripwire Data Files      100               1        0        0
  Critical devices         100               0        0        0
  User binaries            69                0        0        0
  Tripwire Binaries        100               0        0        0
```

10.9.1 Verwenden von `twprint` zur Anzeige der Tripwire Datenbank

Sie können auch `twprint` verwenden, um die gesamte Datenbank oder Informationen über bestimmte Dateien der Tripwire Datenbank anzuzeigen. Dieser Befehl ist besonders nützlich, wenn Sie kontrollieren möchten, wie viele Informationen Tripwire über Ihr System speichert.

Geben Sie den folgenden Befehl ein, um die gesamte Tripwire Datenbank anzuzeigen:

```
/usr/sbin/twprint -m d --print-dbfile | less
```

Dieser Befehl ruft eine große Menge Informationen ab, wobei die beiden ersten Zeilen etwa wie folgt aussehen:

```
Tripwire(R) 2.3.0 Database

Database generated by:        root
Database generated on:        Tue Jan  9 13:56:42 2001
```

```
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================
Database Summary:
===============================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --init

===============================================================
Object Summary:
===============================================================
---------------------------------------------------------------
# Section: Unix File System
---------------------------------------------------------------
     Mode        UID          Size       Modify Time
     ------      ----------   ---------- ----------
 /
     drwxr-xr-x  root (0)     XXX        XXXXXXXXXXXXXXXXX
 /bin
     drwxr-xr-x  root (0)     4096       Mon Jan  8 08:20:45 2001
 /bin/arch
     -rwxr-xr-x  root (0)     2844       Tue Dec 12 05:51:35 2000
 /bin/ash
     -rwxr-xr-x  root (0)     64860      Thu Dec  7 22:35:05 2000
 /bin/ash.static
     -rwxr-xr-x  root (0)     405576     Thu Dec  7 22:35:05 2000
```

Um die Informationen über eine bestimmte Datei anzuzeigen, die Tripwire überprüft (beispielsweise `/etc/hosts`), geben Sie dagegen den folgenden `twprint` Befehl ein:

```
/usr/sbin/twprint -m d --print-dbfile /etc/hosts
```

Es erscheint in etwa Folgendes:

```
Object name:  /etc/hosts

Property:               Value:
-------------           -----------
Object Type             Regular File
Device Number           773
Inode Number            216991
```

```
Mode                    -rw-r--r--
Num Links               1
UID                     root (0)
GID                     root (0)
```

In den `twprint` man-Seiten finden Sie weitere Optionen.

10.10 Aktualisieren der Datenbank nach einer Integritätsprüfung

Wenn Sie eine Integritätsprüfung ausführen und Tripwire Differenzen ermittelt, müssen Sie zunächst bestimmen, ob diese Differenzen tatsächlich Verletzungen der Sicherheit darstellen oder ob es sich dabei eventuell um berechtigte Änderungen handelt. Wenn Sie kürzlich eine Anwendung installiert oder kritische Systemdateien bearbeitet haben, dann weist Tripwire (korrekterweise) darauf hin. In diesem Fall sollten Sie Ihre Tripwire Datenbank aktualisieren, so dass diese Änderungen nicht mehr als Differenzen angezeigt werden. Wurden jedoch unberechtigte Änderungen an Dateien vorgenommen, die ebenfalls Differenzen generieren, dann müssen Sie die ursprüngliche Datei wiederherstellen, wozu Sie eine Sicherheitskopie benötigen oder aber das Programm neu installieren müssen.

Um Ihre Tripwire dahingehend zu aktualisieren, dass sie die ermittelten Differenzen akzeptiert, müssen Sie den Bericht angeben, der hierzu verwendet werden soll. Bei der Eingabe des Befehls, mit dem diese gültigen Differenzen in Ihre Datenbank integriert werden, müssen Sie sicherstellen, dass Sie den aktuellsten Bericht verwenden. Geben Sie den folgenden Befehl (auf einer einzigen Zeile) ein, wobei *Name* der Name des zu verwendenden Berichts ist:

```
/usr/sbin/tripwire --update --twrfile
          /var/lib/tripwire/report/<Name>.twr
```

Tripwire zeigt den gewünschten Bericht mithilfe des standardmäßigen Texteditors (der in der Tripwire Konfigurationsdatei in der Zeile **EDITOR** angegeben ist) an. An dieser Stelle können Sie Dateien deselektieren, die in der Tripwire Datenbank nicht aktualisiert werden sollen. Achten Sie dabei darauf, das nur berechtigte Differenzen in dieser Datenbank aufgenommen werden.

Alle der Tripwire Datenbank vorgelegten Aktualisierungen sind mit einem `[x]` vor dem Dateinamen gekennzeichnet. Wenn Sie nicht möchten, dass eine gültige Differenz in die Tripwire Datenbank aufgenommen wird, dann entfernen Sie das `x` aus dem Kästchen. Schreiben Sie die Dateien mit einem `x`, die Sie integrieren möchten, in den Editor und beenden Sie den Texteditor. Damit weisen Sie Tripwire an, die Datenbank zu aktualisieren und diese Dateien nicht mehr als Differenzen anzuzeigen.

Der standardmäßige Texteditor für Tripwire ist `vi`. Um die Datei mit `vi` zu schreiben und die Änderungen in der Tripwire Datenbank bei der Aktualisierung mit einem spezifischen Bericht vorzunehmen, geben Sie `:wq` im Befehlsmodus von `vi` ein und drücken Sie die [Eingabetaste]. Sie werden nun aufgefordert, Ihren lokalen Schlüssel einzugeben. Anschließend wird eine neue Datenbankdatei für die gültigen Differenzen geschrieben.

Nachdem eine neue Tripwire Datenbank geschrieben wurde, werden die zuvor berechtigten Differenzen nicht mehr in der Warnmeldung der nächsten Integritätsprüfung angezeigt.

10.11 Aktualisieren der Policy-Datei

Wenn Sie die Dateien, die Tripwire in der Datenbank aufzeichnet, oder die Kriterien, nach denen die Differenzen angezeigt werden, ändern möchten, dann müssen Sie die Tripwire Datei bearbeiten.

Führen Sie zunächst alle notwendigen Änderungen am Beispiel der Policy-Datei (`/etc/tripwire/twpol.txt`) aus. Dabei müssen alle Dateien auskommentiert werden, die nicht in Ihrem System existieren, um zu vermeiden, dass der Fehler `Datei nicht gefunden` in den Tripwire Berichten angezeigt wird. Wenn in Ihrem System beispielsweise die Datei `/etc/smb.conf` nicht existiert, dann können Sie Tripwire durch Auskommentieren der entsprechenden Zeile in `twpol.txt` anweisen, nicht nach dieser Datei zu suchen:

```
#     /etc/smb.conf                     -> $(SEC_CONFIG) ;
```

Anschließend müssen Sie Tripwire anweisen, eine neue, unterzeichnete `/etc/tripwire/tw.pol` Datei und dann eine aktualisierte Datenbankdatei zu erstellen. Wenn zum Beispiel `/etc/tripwire/twpol.txt` die bearbeitete Datei ist, verwenden Sie den folgenden Befehl:

```
/usr/sbin/twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt
```

Sie werden nun aufgefordert, den Site-Schlüssel einzugeben. Anschließend wird die `twpol.txt` Datei analysiert und unterzeichnet.

Es ist sehr wichtig, dass Sie die Tripwire Datenbank aktualisieren, nachdem eine neue `/etc/tripwire/tw.pol` Datei erstellt wurde. Die zuverlässigste Methode ist, Ihre derzeitige Tripwire zu löschen und mithilfe der Policy-Datei eine neue Datenbank zu generieren.

Geben Sie den folgenden Befehl ein, wenn Ihre If your Tripwire Datenbankdatei den Namen `wilbur.domain.com.twd` trägt:

```
rm /var/lib/tripwire/wilbur.domain.com.twd
```

Geben Sie anschließend den Befehl ein, um eine neue Datenbank zu erstellen:

```
/usr/sbin/tripwire --init
```

Auf der Grundlage der Anweisungen in der Policy-Datei wird eine neue Datenbank erstellt. Um sicherzustellen, dass die Datenbank korrekt geändert wurde, sollten Sie die erste Integritätsprüfung starten und den Inhalt des generierten Berichts kontrollieren. Unter Abschnitt 10.8, *Ausführen einer Integritätsprüfung* und Abschnitt 10.9, *Drucken der Berichte* finden Sie genaue Anweisungen hierüber.

10.11.1 Unterzeichnen der Konfigurationsdatei

Die Textdatei mit den Änderungen der Konfigurationsdatei (generell `/etc/tripwire/twcfg.txt`) muss unterzeichnet werden, um `/etc/tripwire/tw.cfg` zu ersetzen und um von Tripwire bei der Integritätsprüfung verwendet zu werden. Tripwire erkennt Änderungen erst dann an, wenn die textbasierte Konfigurationsdatei korrekt unterzeichnet und verwendet wurde, um die `/etc/tripwire/tw.pol` zu ersetzen.

Wenn Ihre geänderte textbasierte Konfigurationsdatei `/etc/tripwire/twcfg.txt` ist, geben Sie den folgenden Befehl ein, um sie zu unterzeichnen und um die aktuelle `/etc/tripwire/tw.pol` Datei zu ersetzen:

```
/usr/sbin/twadmin --create-cfgfile -S site.key /etc/tripwire/twcfg.txt
```

Da die Konfigurationsdatei weder die Policy-Datei von Tripwire noch die von der Anwendung ermittelten Dateien ändert, ist es auch nicht notwendig, die Datenbank der geprüften Systemdateien neu zu generieren.

10.12 Tripwire und E-Mail

Tripwire kann E-Mails versenden, wenn eine bestimmte Regel der Policy-Datei verletzt wurde. Um Tripwire entsprechend zu konfigurieren, benötigen Sie zunächst die E-Mail-Adresse der in einem solchen Fall zu kontaktierenden Person sowie den Namen der Regel, die geprüft werden soll. Beachten Sie, dass es in großen Systemen mit mehreren Administratoren mehrere Personengruppen geben kann, die bei bestimmten Differenzen zu benachrichtigen sind, und dagegen geringfügigere Differenzen niemandem gemeldet werden.

Wenn Sie wissen, wer zu benachrichtigen ist und was gemeldet werden soll, dann fügen Sie eine **emailto=** Zeile in den Abschnitt der Anweisungen jeder einzelnen Regel hinzu. Geben Sie hierzu ein Komma nach der **severity=** Zeile ein und setzen Sie **emailto=** auf die nachfolgende Zeile. Geben Sie hier die E-Mail-Adressen an, die die Berichte für die entsprechende Regel erhalten sollen. Es werden multiple E-Mails gesendet, wenn mehrere Adressen angegeben sind (die Sie durch ein Semikolon trennen müssen).

Wenn Sie zum Beispiel möchten, dass zwei Administratoren (in diesem Beispiel "Karl" und "Otto") benachrichtigt werden, wenn ein Netzwerkprogramm geändert wurde, dann ändern Sie die Anweisung der entsprechenden Regel in der Policy-Datei wie folgt:

```
(
  rulename = "Networking Programs",
  severity = $(SIG_HI),
  emailto = karl@domain.com;otto@domain.com
)
```

Nachdem eine neue, unterzeichnete Policy-Datei aus der `/etc/tripwire/twpol.txt` Datei erstellt wurde, wird eine Meldung mit den Differenzen in Bezug auf die spezifische Regel an die angegebenen E-Mail-Adressen gesendet. Anweisungen über das Unterzeichnen Ihrer Policy-Datei finden Sie unter Abschnitt 10.11, *Aktualisieren der Policy-Datei*.

10.12.1 Senden von Probe-E-Mails

Geben Sie den folgenden Befehl ein, um sicherzustellen, dass die Konfiguration der E-Mails von Tripwire ein korrektes Senden der Meldungen gewährleistet:

```
/usr/sbin/tripwire --test --email Ihre@E-Mail.Adresse
```

Daraufhin sendet `tripwire` sofort eine Probe-E-Mail an die angegebene E-Mail-Adresse.

10.13 Zusätzliche Ressourcen

Tripwire bietet noch mehr als das, was in diesem Kapitel beschrieben wurde. Lesen Sie die Zusatzinformationen, um mehr über Tripwire zu erfahren.

10.13.1 Installierte Dokumentation

- `/usr/share/doc/tripwire-<Version-Nummer>` — Ein idealer Ausgangspunkt um zu erfahren, wie die Konfigurations- und Policy-Dateien im `/etc/tripwire` Verzeichnis an Ihre individuellen Erfordernisse angepasst werden können.
- Lesen Sie auch die man-Seiten für `tripwire`, `twadmin` und `twprint`. Hier wird der Gebrauch dieser Dienstprogramme erläutert.

10.13.2 Nützliche Websites

- http://www.tripwire.org — Die Homepage des Tripwire Open Source Projekts. Hier finden Sie die aktuellsten Neuigkeiten über die Anwendung sowie eine FAQ-Liste.

11 SSH-Protokoll

In diesem Kapitel werden der Nutzen des SSH™-Protokolls, die Abfolge der Vorgänge bei der Erstellung einer sicheren Verbindung zu einem fernen Rechner sowie die verschiedenen SSH-Schichten und die Methoden beschrieben, mit denen Sie sich absichern, dass SSH von den Benutzern, die sich mit Ihrem System verbinden, verwendet werden.

Gebräuchliche Methoden für eine Fernanmeldung an ein anderes System über eine Shell wie (`telnet`, `rlogin` oder `rsh`) oder das Kopieren von Dateien zwischen Rechnern (`ftp` or `rcp`) sind nicht sicher und sollten vermieden werden. Verbinden Sie sich mit einem fernen Rechner grundsätzlich über eine Secure Shell oder ein verschlüsseltes, virtuelles privates Netzwerk. Auf diese Weise werden Sie das Sicherheitsrisiko für Ihr System und das ferne System reduzieren.

11.1 Einführung

SSH (*S*ecure *SH*ell) ist ein Protokoll für die Erstellung einer sicheren Verbindung zwischen zwei Systemen. Anhand von SSH initialisiert der Client-Rechner eine Verbindung mit einem Server-System. SSH gewährleistet dabei Folgendes:

- Nach einer ersten Verbindung prüft der Client, ob er sich auch in der Folge mit dem gleichen Server verbindet.
- Der Client kann die Authentifizierungsinformationen wie Benutzername und Passwort in verschlüsselter Form an den Server übertragen.
- Alle während der Verbindung gesendeten und empfangenen Daten sind so komplex verschlüsselt, dass die Gefahr einer Entschlüsselung extrem gering ist.
- Der Client kann X11[1]Anwendungen verwenden, die von der Shell-Prompt aktiviert werden. Auf diese Weise wird eine sichere graphische Schnittstelle (**X11 forwarding**) geliefert.

Auch der Server nutzt SSH, insbesondere wenn er mehrere Dienste ausführt. Wenn Sie **port forwarding** verwenden, können sonst unverschlüsselte und damit unsichere Protokolle (z.B. POP) zwecks einer sicheren Verbindung mit fernen Rechnern verschlüsselt werden. SSH vereinfacht das Verschlüsseln verschiedener Arten von Meldungen, die normalerweise unverschlüsselt durch öffentliche Netzwerke gesendet werden.

Red Hat Linux 7.1 enthält die Pakete für den OpenSSH-Server (`openssh-server`) und den Client (`openssh-clients`) sowie das allgemeine OpenSSH-Paket (`openssh`), das in beiden Fällen installiert werden muss. Weitere Informationen über die Installation und den Gebrauch von OpenSSH

[1] X11 bezieht sich auf das X11R6 Anzeigesystem, das gewöhnlich als X bezeichnet wird. Red Hat Linux enthält XFree86, ein sehr gebräuchliches Open Source X Window System auf der Grundlage von X11R6.

in Ihrem Red Hat Linux System finden Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration.*

Die OpenSSH-Pakete erfordern das OpenSSL-Paket (`openssl`). OpenSSL installiert verschiedene wichtige kryptographische Bibliotheken, die OpenSSH bei der Erstellung mit verschlüsselten Meldungen unterstützt. Bevor Sie irgendeines der OpenSSH-Pakete installieren, müssen Sie `openssl` installieren.

Eine große Anzahl an Client- und Serverprogrammen können das SSH-Protokoll verwenden, einschließlich vieler Open-Source und kostenlos erhältlicher Anwendungen. Für fast alle der heute gebräuchlichsten Betriebssystem stehen verschiedene SSH Client-Versionen zur Verfügung. Selbst wenn die Benutzer, die sich mit Ihrem System verbinden, Red Hat Linux nicht verwenden, können sie doch einen SSH-Ursprungsclient für ihr Betriebssystem benutzen.

11.1.1 Wozu dient SSH?

Gefahren im Rahmen der Netzwerkkommunikation schließen unerlaubte Zugriffe auf Pakete und das "spoofing" [2]von DNS- und IP-Adressen sowie die Verbreitung von falschen Informationen ein. Diese Gefahren können generell wie folgt klassifiziert werden:

- *Abfangen von Mitteilungen zwischen zwei Systemen* — In diesem Fall gibt es irgendwo im Netzwerk zwischen den miteinander kommunizierenden Systemen einen Dritten, der die Informationen, die zwischen den beiden Systemen ausgetauscht werden, kopiert. Der Dritte kann dabei die Informationen abfangen und aufbewahren oder sie auch ändern und an den eigentlichen Empfänger weiterleiten.
- *Imitation eines bestimmten Rechners* — Diese Strategie bedeutet, dass ein drittes System vorgibt, der Empfänger einer Mitteilung zu sein. Ist sie erfolgreich, so bemerkt der Client die Manipulation nicht und kommuniziert weiterhin mit diesem System, als ob es sich um den ursprünglichen Empfänger handele.

Bei beiden Methoden werden Informationen mit sehr wahrscheinlich unlauteren Absichten abgefangen. Hieraus kann ein enormer Schaden entstehen, unabhängig davon, ob die Pakete auf einem LAN- oder einem DNS-Server abgesucht werden.

Dank der digitalen Unterschrift des Servers können diese Sicherheitsrisiken erheblich gemindert werden, wenn SSH für Fernanmeldungen über eine Shell und für das Kopieren von Dateien verwendet wird. Die Mitteilungen zwischen Client und Server sind, auch wenn sie abgefangen werden, wertlos, da jedes Paket verschlüsselt ist. Dabei nutzen auch Versuche, sich als das eine oder andere System auszugeben, nichts, da der Schlüssel hierfür nur dem Client- und dem Server-System bekannt ist.

[2] "Spoofing" bedeutet, dass sich ein Benutzer als ein bestimmtes System präsentiert, es aber in Wirklichkeit nicht ist.

11.2 Die Abfolge der Vorgänge einer SSH-Verbindung

Bestimmte Vorgänge tragen zu einer unversehrten SSH-Kommunikation zwischen zwei Rechnern bei.

Zunächst wird eine sichere **Transportschicht** geschaffen, die dem Client-System anzeigt, dass es mit dem korrekten Server in Verbindung steht. Anschließend werden die Mitteilungen zwischen den beiden Rechnern mit einer symmetrischen Ziffer verschlüsselt.

Nachdem eine auf diese Weise verschlüsselte Verbindung mit dem Server hergestellt wurde, kann sich der Client gegenüber dem Server identifizieren, ohne dass die Gefahr einer Manipulation der entsprechenden Informationen besteht. Für die standardmäßige Authentifizierung verwendet OpenSSH von Red Hat Linux DSA- oder RSA-Schlüssel sowie die Version 2.0 des SSH-Protokolls.

Sobald sich der Client gegenüber dem Server identifiziert hat, können verschiedene Dienste auf sichere Weise über diese Verbindung verwendet werden. Darunter: interaktive Shell-Sessionen, X11-Anwendungen und Kommunikationen von TCP/IP-Ports über Tunnel.

Vom lokalen System erfordert dieser gesamte Verbindungsprozess einen nur geringen Arbeitsaufwand mehr. SSH funktioniert sehr gut, da es den Benutzern geläufig ist, die bereits mit weniger sicheren Verbindungsmethoden vertraut sind.

Im folgenden Beispiel initialisiert der Benutzer user1 auf dem Client-System eine Verbindung zu einem Server. Die IP-Adresse des Servers lautet 10.0.0.2, könnte aber auch der Domänenname sein. Der Name, mit dem sich user1 am Server anmeldet, ist user2. Der Befehl `ssh` sieht daher wie folgt aus:

```
[user1@machine1 user1]$ ssh user2@10.0.0.2
```

Der OpenSSH-Client wird nun den Benutzer auffordern, den persönlichen Schlüssel einzugeben, der der Authentifizierung dient. Dieser Schlüssel wird jedoch nicht über die - inzwischen sichere - Verbindung zwischen Client und Server gesendet, sondern benutzt, um die Datei `id_dsa` zu öffnen und eine Unterschrift zu erstellen, die anschließend an den Server übertragen wird. Wenn der Server eine Kopie des allgemeinen Benutzerschlüssels besitzt, die für die Kontrolle der Unterschrift verwendet werden kann, dann wird der Benutzer authentifiziert.

In diesem Beispiel verwendet der Benutzer einen DSA-Schlüssel (es können aber auch RSA-Schlüssel etc. benutzt werden). Es erscheint die folgende Prompt:

```
Enter passphrase for DSA key '/home/user1/.ssh/id_dsa':
```

Sollte die allgemeine Authentifizierung fehlschlagen (weil der falsche Text für den Schlüssel eingegeben wurde oder die Informationen für die Authentifizierung auf dem Server nicht vorhanden sind), wird gewöhnlich ein weiterer Versuch zur Authentifizierung eingeleitet. In unserem Beispiel erlaubt es OpenSSH dem Benutzer user1, sich mit dem Passwort von user2 zu authentifizieren, da die gesendete Unterschrift nicht mit einem allgemeinen, von user2 gespeicherten Schlüssel übereinstimmt:

```
user2@machine2's password:
```

Wenn das korrekte Passwort eingegeben wurde, erscheint ein Shell-Prompt. Benutzer user2 muss natürlich bereits einen Account auf dem Rechner 10.0.0.2 besitzen, damit die Authentifizierung des Passworts erfolgen kann.

```
Last login: Mon Apr 15 13:27:43 2001 from machine1
[user2@machine2 user2]$
```

Der Benutzer kann nun die Shell analog zu `telnet` oder `rsh` verwenden. Der einzige Unterschied besteht darin, dass die Kommunikation verschlüsselt ist.

Andere SSH-Tools (`scp` and `sftp`) funktionieren auf ähnliche Weise wie die unsicheren `rcp` und `ftp`. Anweisungen und Beispiele für den Gebrauch dieser und anderer SSH-Befehle finden Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*.

11.3 Schichten der SSH-Sicherheit

Das SSH-Protokoll ermöglicht es allen Client- und Serverprogrammen, die nach den Angaben des Protokolls erstellt wurden, auf sichere Weise zu kommunizieren und untereinander ausgetauscht zu werden.

Derzeit gibt es zwei verschiedene SSH-Protokolle: SSH-Version 1 enthält verschiedene patentierte Verschlüsselungsalgorithmen (mehrere Patente sind jedoch bereits abgelaufen) und eine Sicherheitslücke, die es potentiell ermöglicht, dass Daten in den Datenfluss eingegeben werden. Wenn möglich, wird empfohlen, Clients und Server zu verwenden, die mit SSH Version 2 kompatibel sind.

OpenSSH enthält den Support für Version 2 (sowie kostenlose DSA-Verschlüsselungen). Zusammen mit den OpenSSL-Verschlüsselungsbibliotheken bietet OpenSSH eine umfassende Bandbreite an Sicherheitsfunktionen.

Beide Versionen des SSH-Protokolls (1 und 2) verwenden ähnliche Sicherheitsschichten, um einen Rundum-Schutz der Kommunikation zu gewährleisten. Jede Schicht bedeutet eine bestimmte Schutzfunktion, die in Kombination mit den anderen die gesamte Sicherheit des Systems sowie die Benutzerfreundlichkeit verbessert.

11.3.1 Transportschicht

Die wichtigste Aufgabe der Transportschicht ist es, die sichere und verschlüsselte Kommunikation zwischen zwei Rechnern bei und nach der Authentifizierung zu gewährleisten. Die gewöhnlich über TCP/IP ausgeführte Transportschicht verwaltet zu diesem Zweck die Verschlüsselung und Entschlüsselung der Daten und prüft, ob der Server der korrekte Rechner ist. Darüber hinaus sorgt sie dafür, dass die Datenpakete während des gesamten Übertragungsflusses geschützt sind. Weiterhin kann diese Schicht die Daten komprimieren und damit die Übertragungsgeschwindigkeit erheblich erhöhen.

Sobald ein Client über ein SSH-Protokoll mit einem Server in Verbindung tritt, erfolgen verschiedene wichtige Vorgänge, die dazu dienen, dass die beiden Systeme die Transportschicht korrekt aufbauen:

- Austausch des Schlüssels
- Zu verwendender Algorithmus für den allgemeinen Schlüssel
- Zu verwendender Algorithmus für die symmetrische Verschlüsselung
- Zu verwendender Algorithmus für die Authentifizierung der Mitteilungen
- Zu verwendender Hash-Algorithmus

Beim Austausch der Schlüssel identifiziert sich der Server gegenüber dem Client mithilfe von **Rechnerschlüssel**. Wenn nie zuvor eine Verbindung zwischen dem Client und diesem Server bestanden hatte, erkennt er den Server als 'unbekannt' an. OpenSSH löst dieses Problem, indem es dafür sorgt, dass der Client den Rechnerschlüssel akzeptiert, wenn zum ersten Mal eine SSH-Verbindung hergestellt wird. Bei den nachfolgenden Verbindungen wird dieser Schlüssel mit der gespeicherten Version des Clients verglichen und auf diese Weise sichergestellt, dass der Client tatsächlich mit dem gewünschten Server kommuniziert.

Die von OpenSSH verwendete Kontrolle des Rechnerschlüssels ist nicht perfekt. Ein Hacker könnte sich zum Beispiel bei der ersten Verbindung als Server ausgeben, da der lokale Rechner zu diesem Zeitpunkt den gewünschten Server von einem unerlaubten Zugriff noch nicht unterscheiden kann. Bis eine verbesserte Methode zur Verfügung steht, ist jedoch diese Methode besser als nichts.

Das SSH-Protokoll wurde konzipiert, um mit fast allen Algorithmen oder Formaten für allgemeine Schlüssel verwendet werden zu können. Nachdem ein erster Schlüsselaustausch zwei Werte erstellt hat (einen Hash-Wert für den Austausch und einen gemeinsam genutzten, geheimen Wert), berechnen die beiden Systeme sofort neue Schlüssel und Algorithmen, um die Authentifizierung und die in der Folge über die Verbindung gesendeten Daten zu schützen.

11.3.2 Authentifizierung

Nachdem die Transportschicht einen sicheren Tunnel geschaffen hat, in dem die Informationen zwischen den beiden Systemen übertragen werden, teilt der Server dem Client die verschiedenen unterstützten Authentifizierungsmethoden mit (beispielsweise eine private, verschlüsselte Unterschrift oder die Eingabe eines Passworts). Der Client wird anschließend versuchen, sich anhand einer der unterstützten Methoden gegenüber dem Server zu identifizieren.

Server können konfiguriert werden, um verschiedene Arten der Authentifizierung zu ermöglichen. Diese Methode bietet daher jeder Seite das ideale Maß an Kontrolle. Der Server kann entscheiden, welche Verschlüsselungsmethoden er auf der Grundlage seines Sicherheitsmodells unterstützen möchte, und der Client kann festlegen, in welcher Reihenfolge er die verschiedenen verfügbaren Authentifizierungsmethoden verwendet. Dank der Sicherheit der SSH-Transportschicht sind auch scheinbar unsichere Authentifizierungsmethoden (z.B. die rechnerbasierte Authentifizierung) sicher.

Die meisten Benutzer mit einer Secure Shell werden sich mithilfe eines Passworts authentifizieren. Im Gegensatz zu anderen Authentifizierungsmethoden wird das Passwort hierbei als normaler Text an den Server übertragen. Da das gesamte Passwort jedoch bei der Übertragung über die Transportschicht verschlüsselt wird, wird es auch sicher über jedes Netzwerk gesendet.

11.3.3 Verbindung

Nach der erfolgreichen Authentifizierung über die SSH- Transportschicht werden multiple **Kanäle**[3]geöffnet, wobei die einzelne Verbindung zwischen den beiden Systemen mehrfach genutzt wird. Jeder der Kanäle bearbeitet die Mitteilungen für eine andere Terminalsession, gesendete X11-Informationen oder jedes andere Gerät, das die SSH-Verbindung verwenden möchte.

Sowohl Clients als auch Server können einen neuen Kanal erstellen, wobei jedem Kanal an jedem Ende eine unterschiedliche Nummer zugewiesen wird. Wenn eine Seite einen neuen Kanal öffnen möchte, wird die Nummer der entsprechenden Seite des Kanals mit der Anforderung übermittelt. Diese Information wird von der anderen Seite gespeichert und verwendet, um eine bestimmte Mitteilung an diesen Kanal weiterzuleiten. Ziel ist zu vermeiden, dass sich verschiedene Arten Sessionen beeinflussen und die Kanäle geschlossen werden können, ohne die primäre SSH-Verbindung zwischen den beiden Systemen zu unterbrechen.

Kanäle unterstützen auch die Datenflusskontrolle, was es ihnen ermöglicht, Daten geordnet zu senden und zu empfangen. Auf diese Weise werden Daten erst dann über den Kanal gesendet, wenn der Host-Rechner die Meldung erhält, dass der Kanal empfangsbereit ist.

Kanäle sind insbesondere für das X11-Forwarding und das TCP/IP- Forwarding mit SSH von großem Nutzen. Es ist dabei möglich, separate Kanäle verschieden zu konfigurieren, beispielsweise um eine unterschiedliche maximale Paketgröße zu verwenden oder einen bestimmten Datentyp zu übertragen. Auf diese Weise ist SSH flexibel genug, um verschiedene Arten Fernverbindungen (z.B. Onlinedienste über öffentliche Netzwerke oder Hochgeschwindigkeit-LAN-Verbindungen) ohne die grundlegende Infrastruktur des Protokolls zu verändern. Der Client und der Server bearbeiten automatisch die Konfiguration jedes Kanals innerhalb der SSH-Verbindung für den Benutzer.

[3] Eine Multiplex-Verbindung besteht aus verschiedenen Signalen, die über ein gemeinsam genutztes Medium gesendet werden. Mit SSH werden verschiedene Kanäle über eine gemeinsame, verschlüsselte Verbindung gesendet.

11.4 OpenSSH Konfigurationsdateien

OpenSSH verfügt über zwei verschiedene Arten Konfigurationsdateien: eine für Clientprogramme (`ssh`, `scp` und `sftp`) und eine andere für den Serverdienst (`sshd`), die in zwei verschiedenen Bereichen abgelegt sind.

Die SSH-Konfigurationsinformationen für das gesamte System sind im Verzeichnis `/etc/ssh` gespeichert:

- `primes` — Hier sind Diffie-Hellmann Gruppen für den Austausch des Diffie-Hellmann Schlüssels enthalten. Dieser Austausch erstellt einen gemeinsam genutzten, geheimen Wert, der von keiner Seite allein erstellt werden kann und für die Rechnerauthentifizierung verwendet wird. Diese Datei ist ausschlaggebend für den Aufbau einer sicheren Transportschicht.
- `ssh_config` — Hierbei handelt es sich um eine Datei für die Konfiguration des SSH-Clients, die verwendet wird, um den SSH-Client zu verwalten. Wenn einem Benutzer eine eigene Konfigurationsdatei in seinem Home-Verzeichnis zur Verfügung steht, dann überschreiben die hier enthaltenen Werte die in `/etc/ssh/ssh_config` gespeicherten Werte.
- `sshd_config` — Dies ist die Konfigurationsdatei für `sshd`.
- `ssh_host_dsa_key` — Der individuelle DSA-Schlüssel, der von `sshd` verwendet wird.
- `ssh_host_dsa_key.pub` — Der allgemeine DSA-Schlüssel, der von `sshd` verwendet wird.
- `ssh_host_key` — Der individuelle RSA- Schlüssel, der von `sshd` für Version 1 des SSH-Protokolls verwendet wird.
- `ssh_host_key.pub` — Der öffentliche RSA- Schlüssel, der von `sshd` für Version 1 des SSH-Protokolls verwendet wird.
- `ssh_host_rsa_key` — Der individuelle RSA- Schlüssel, der von `sshd` für Version 2 des SSH-Protokolls verwendet wird.
- `ssh_host_rsa_key.pub` — Der allgemeine RSA-Schlüssel, der von `sshd` für Version 2 des SSH-Protokolls verwendet wird.

Die benutzerspezifischen SSH-Konfigurationsinformationen werden im Home-Verzeichnis des Benutzers im Unterverzeichnis `.ssh` gespeichert:

- `authorized_keys2` — In dieser Datei ist eine Liste der "authorisierten" allgemeinen Schlüssel enthalten. Wenn ein sich verbindender Benutzer nachweisen kann, dass er den individuellen Schlüssel kenn, der einem dieser allgemeinen Schlüssel entspricht, dann wird er authentifiziert. Beachten Sie, dass es sich hierbei um eine fakultative Authentifizierungsmethode handelt.
- `id_dsa` — Diese Datei enthält die DSA-Authentifizierungs-ID des Benutzers.
- `id_dsa.pub` — Der allgemeine DSA- Schlüssel des Benutzers.

- known_hosts2 — In dieser Datei können die DSA-Rechnerschlüssel der Server gespeichert werden, mit denen sich der Benutzer über SSH anmeldet. Wenn ein Server seine Rechnerschlüssel auf korrekte Weise geändert hat (beispielsweise bei einer Neuinstallation von Red Hat Linux), wird dem Benutzer gemeldet, dass der Rechnerschlüssel, der in der Datei known_hosts2 gespeichert ist, nicht mit diesem Rechner übereinstimmt. Der Benutzer muss daraufhin diesen Schlüssel aus der Datei known_hosts2 löschen, um den neuen Rechnerschlüssel für das System speichern zu können. Die Datei known_hosts2 gewährleistet, dass sich der Client mit dem korrekten Server verbindet. Wenn ein Rechnerschlüssel geändert wurde und Sie sich nicht absolut sicher sind, warum, dann sollten Sie den Systemadministrator kontaktieren, um sicherzustellen, dass der Rechner nicht auf irgendeine Weise manipuliert wurde.

Auf den man-Seiten von ssh und sshd finden Sie weitere Informationen über die verschiedenen Anweisungen in den SSH-Konfigurationsdateien.

11.5 Mehr als eine Secure Shell

Eine sichere Befehlszeilenschnittstelle stellt nur eine der vielen Arten und Weisen dar, wie SSH verwendet werden kann. Mit einer angemessenen Bandbreite können X11-Sessionen über einen SSH-Kanal verwaltet werden. Mithilfe von TCP/IP-Forwarding können bisher unsichere Port-Verbindungen zwischen Systemen auf spezifische SSH-Kanäle gemapped werden.

11.5.1 X11-Forwarding

Eine X11-Session über eine bestehende SSH-Verbindung zu öffnen ist so einfach wie das Ausführen eines X-Programms, während Sie bereits einen X-Client auf Ihrem Rechner ausführen. Wird ein X-Programm von einer Secure Shell Prompt ausgeführt, erstellen der SSH-Client und -Server einen neuen, verschlüsselten Kanal in der aktuellen SSH- Verbindung, und die Daten des X-Programms werden über diesen Kanal auf Ihren Client-Rechner gesendet, als ob Sie über ein lokales Terminal mit dem X-Server verbunden wären.

Sie können sich sicherlich vorstellen, wie nützlich X11-Forwarding sein kann. Sie können hiermit zum Beispiel eine sichere, interaktive Session mithilfe der up2date GUI auf dem Server erstellen, um bestimmte Pakete zu aktualisieren (sofern die notwendigen Red Hat Network Pakete auf dem Server installiert sind). Verbinden Sie sich hierzu über ssh mit dem Server und geben Sie Folgendes ein:

```
up2date
```

Sie werden nun aufgefordert, das Root-Passwort für den Server einzugeben. Anschließend erscheint Red Hat Update Agent, und Sie können Ihre Pakete auf dem Server aktualisieren, als ob Sie direkt vor Ihrem Rechner sitzen würden.

Die zusätzlichen Bearbeitungsinformationen, die für das Verschlüsseln und Entschlüsseln der über den Kanal gesendeten Informationen notwendig sind, sowie die für das Übertragen der verschlüsselten Daten des X-Programms erforderliche zusätzliche Bandbreite können jedoch von großer Bedeutung

sein. Es müssen entsprechende Tests durchgeführt werden, um sicherzustellen, dass das X-Programm mit Ihrer speziellen Hardware und Bandbreite verwendet werden kann.

11.5.2 TCP/IP-Forwarding

TCP/IP-Forwarding funktioniert mit dem SSH-Client, der anfordert, dass ein bestimmter Port beim Client oder Server über die bestehende Verbindung gemapped wird.

Um einen lokalen Port des Clients auf den Port des Servers zu mappen, müssen Sie zunächst die Portnummern beider Rechner kennen. Es ist auch möglich, zwei nicht-standardmäßige unterschiedliche Ports miteinander zu mappen.

Verwenden Sie den folgenden Befehl (auf einer einzigen Zeile), um einen TCP/IP-Forwarding-Kanal zu erstellen, der auf Verbindungen auf dem lokalen Rechner wartet:

```
ssh -L <local-port>:<remote-hostname>:<remote-port>
        <username>@<hostname>
```

Bitte beachten

Für das Einrichten von TCP/IP-Forwarding-Kanälen für Ports mit weniger als 1024 Zylindern - wie auch für das Starten von Diensten an solchen Ports - müssen Sie als Root angemeldet sein.

Wenn Sie zum Beispiel Ihre E-Mails auf einem Server mit dem Namen mail.domain.com mithilfe von POP abrufen möchten und SSH auf diesem Server zur Verfügung steht, können Sie den folgenden Befehl verwenden, um TCP/IP-Forwarding einzurichten:

```
ssh -L 1100:mail.domain.com:110 mail.domain.com
```

Nachdem TCP/IP-Forwarding zwischen den beiden Rechnern eingerichtet wurde, können Sie Ihren POP-Mail-Client anweisen, localhost als POP-Server und 1100 als Port für das Abrufen neuer E-Mails zu verwenden. Alle an Ihren Port 1100 gesendeten Anforderungen werden auf diese Weise sicher an den Server mail.domain.com weitergeleitet.

Wenn mail.domain.com keinen SSH-Serverdämon ausführt, Sie sich jedoch über SSH (und eventuell mit einer Firewall) an einem nahen Rechner anmelden können, können Sie dennoch SSH verwenden, um den Teil der POP-Verbindung zu sichern, der über öffentliche Netzwerke läuft. Hierzu ist ein Befehl notwendig:

```
ssh -L 1100:mail.domain.com:110 other.domain.com
```

In diesem Beispiel leiten Sie Ihre POP-Anforderung von Port 1100 Ihres Rechners über die SSH-Verbindung auf Port 22 an other.domain.com weiter. Anschließend verbindet sich other.domain.com mit Port 110 auf mail.domain.com, so dass Sie neue E-Mails abrufen können. Nur die Verbindung

zwischen Ihrem System und other.domain.com ist sicher. In den meisten Fällen reicht dies jedoch aus, um Ihre Informationen sicher über öffentliche Netzwerke zu senden.

In diesem und im vorigen Beispiel müssen Sie sich allerdings gegenüber dem SSH-Server identifizieren, um das TCP/IP-Forwarding vornehmen zu können. Versichern Sie sich, dass Sie die normalen SSH-Befehle ausführen können, bevor Sie TCP/IP-Forwarding einrichten.

TCP/IP-Forwarding kann sehr nützlich sein, wenn Sie Informationen sicher über Netzwerk-Firewalls übertragen möchten. Wenn die Firewall so konfiguriert ist, dass SSH-Kommunikationen über den Standardport (22) erfolgen, die Übertragung über andere Ports jedoch gesperrt ist, ist eine Verbindung zwischen zwei Rechnern mit gesperrten Ports weiterhin möglich, indem die Meldungen über eine festgesetzte SSH-Verbindung zwischen diesen Rechnern übermittelt werden.

Bitte beachten

Dies stellt jedoch ein großes Risiko dar. TCP/IP-Forwarding für das Weiterleiten von Verbindungen ermöglicht es jedem Benutzer des Client-Servers, sich mit dem Dienst zu verbinden, an den Sie Verbindungen weiterleiten. Dies ist besonders dann gefährlich, wenn Ihr Client-System auf irgendeine Art und Weise beschädigt ist.

Prüfen Sie mit dem Systemadministrator, wer Ihre Firewall verwaltet, bevor Sie TCP/IP-Forwarding verwenden. Der Grund hierfür ist, dass Systemadministratoren diese Anwendung auf dem Server deaktivieren können, indem sie auf der **AllowTcpForwarding**-Zeile `No` in `/etc/ssh/sshd_config` eingeben und `sshd` neu starten.

11.6 Anfordern von SSH für Fernverbindungen

Damit SSH Ihre Netzwerkverbindungen effektiv schützt, dürfen Sie keine unsicheren Verbindungsprotokolle wie `telnet` und `rsh` mehr verwenden. Andernfalls wird das Passwort eines Benutzers mithilfe von `ssh` an einem Tag zwar geschützt, kann jedoch an dem Tag, an dem `telnet` verwendet wird, erfasst werden.

Deaktivieren Sie unsichere Verbindungsmethoden Ihres Systems mithilfe von `ntsysv` oder `chkconfig`. Auf diese Weise stellen Sie sicher, dass die entsprechenden Dienste nicht beim Booten des Systems gestartet werden. Geben Sie den folgenden Befehl ein, um `ntsysv` für die Konfiguration von Diensten zu verwenden, die auf den Runlevels 2, 3 und 5 starten.

```
/usr/sbin/ntsysv 235
```

In `ntsysv` können Sie Dienste durch einfaches Deselektieren deaktivieren. Mit der [Leertaste] können Sie den Dienst auf aktiv oder nicht aktiv einstellen. Sie sollten hier auf jeden Fall `telnet`, `rsh`,

`ftp` und `rlogin` deselektieren. Wählen Sie anschließend **OK**, um Ihre Änderungen in `ntsysv` zu speichern. Weitere Informationen hierüber finden Sie auf der man-Seite von `ntsysv`.

Änderungen mit `ntsysv` sind erst dann gültig, wenn entweder das System neu gestartet oder die Runlevel geändert werden. Wenn Sie Dienste deaktiviert haben, die mit `xinetd` verwendet werden, dann müssen Sie `xinetd` neu starten. `rlogin`, `rsh` und `telnet` werden standardmäßig von `xinetd` geprüft. Geben Sie Folgendes ein, um `xinetd` neu zu starten.

```
/sbin/service xinetd restart
```

Dienste, die nicht mit `xinetd` verwendet werden, müssen von Ihnen angehalten werden, es sei denn, Sie starten Ihr System nach Verwendung von `ntsysv` neu. Um einen Dienst anzuhalten, verwenden Sie einen Befehl wie den folgenden:

```
/sbin/service <service-name> stop
```

Nachdem `xinetd` neu gestartet und alle anderen Dienste angehalten wurden, die Sie so konfiguriert haben, dass sie nicht automatisch starten, akzeptiert Ihr System keine deaktivierten Verbindungsmethoden mehr. Wenn Sie alle Fernverbindungsmethoden außer dem `sshd` Dienstdämon deaktivieren, müssen sich die Benutzer über eine SSH-Client-Anwendung mit dem Server verbinden.

12 Kontrolle von Zugriff und Privilegien

Die Systemsicherheit ist im großen Maße darauf zurückzuführen, dass Benutzer oder Gruppen nur das machen können, was die Sicherheitsbestimmungen zulassen. Die meisten der täglichen Änderungen werden vorgenommen, um die Zugriffe und Privilegien zu kontrollieren, die Benutzer und Gruppen haben. (Unter Kapitel 2, *Benutzer und Gruppen* erhalten Sie mehr Informationen über das korrekte Erstellen und Konfigurieren von Benutzern und Gruppen.)

Viele Organisationen, die Red Hat Linux verwenden, haben bestimmte Richlinien oder Arbeitsumgebungen, die eine höhere Sicherheit oder spezielle Konfigurationen für erweiterten oder eingeschränkten Zugriff auf Anwendungen oder Systemgeräte erfordern. Dieser Abschnitt behandelt einige Möglichkeiten wie Sie Ihr System bearbeiten können, um einen geeigneten Level von Zugriffen und Privilegien für Ihre Benutzer zur Verfügung zu haben.

12.1 Shadow Dienstprogramme

Wenn Sie sich in einer Mehrbenutzer-Umgebung befinden und weder PAM noch Kerberos benutzen, sollten Sie in Erwägung ziehen, Shadow-Dienstprogramme (auch als **Shadow-Passwörter** bekannt) zu verwenden, um den verbesserten Schutz zu nutzen, der Ihnen dadurch für Ihre Authentifizierungsdateien in Ihrem System zur Verfügung gestellt wird. Der Shadow-Passwortschutz für Ihr System ist standardmäßig bei der Installation von Red Hat Linux aktiviert, wie z.B. **MD5-Passwörter** (eine alternative und sichere Methode zum Verschlüsseln von Passwörtern, die in Ihrem System gespeichert werden).

Shadow-Passwörter bieten zusätzlich zum standardmäßigen Speichern von Passwörten auf UNIX und Linux-Systemen noch einige deutliche Vorteile:

- 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.
- Sie liefern Informationen über ältere Passwörter (wann ein Passwort das letzte Mal geändert wurde).
- Kontrolle, wie lange das Passwort noch verwendet werden kann, bis es geändert werden muss.
- Die Möglichkeit unter Verwendung der Datei `/etc/login.defs` die Sicherheitsbestimmungen besonders im Bezug auf ältere Passwörter umzusetzen.

Das Paket `Shadow-Dienstprogramme` enthält Dienstprogramme, die Folgendes unterstützen:

- Umwandeln von normalen Passwörtern in Shadow-Passwörter und umgekehrt (`pwconv`, `pwunconv`)

- Überprüfen der Passwort-, Gruppen- und der dazugehörigen Shadow-Dateien (`pwck`, `grpck`)
- Industriestandard-Methoden zum Hinzufügen, Löschen und Modifizieren von Benutzerzugriffen (`useradd`, `usermod` und `userdel`)
- Industriestandard-Methoden zum Hinzufügen, Löschen und Modifizieren von Benutzergruppen (`groupadd`, `groupmod` und `groupdel`)
- Industriestandard-Methoden zum Verwalten der `/etc/group` Datei, die `gpasswd` verwendet.

Bitte beachten

Weitere interessante, diese Dienstprogramme betreffende Punkte sind:

- Die Dienstprogramme arbeiten ordnungsgemäß, unabhängig davon, ob der Shadow-Effekt aktiviert ist oder nicht.
- Die Dienstprogramme wurden leicht verändert, um die Red Hat Linux Benutzer privater Gruppenschemata zu unterstützen. Diese Änderungen finden Sie in der man-Seite `useradd` beschrieben. Weitere Informationen über die Benutzer privater Gruppen finden Sie unter Abschnitt 2.4, *Benutzereigene Gruppen*
- Das `adduser` Skript wurde durch eine symbolische Link nach `/usr/sbin/useradd` ersetzt.
- Die Tools im Paket `shadow-utils` sind für Kerberos oder LDAP nicht aktiviert. Neue Benutzer haben nur lokalen Zugriff. Weitere Informationen über Kerberos oder LDAP finden Sie unter Kapitel 9, *Verwenden von Kerberos 5 in Red Hat Linux* und Kapitel 4, *Lightweight Directory Access Protocol (LDAP)*.

12.2 Konfigurieren des Zugriffs auf die Konsole

Wenn sich normale Benutzer (nicht Root) an einem Computer lokal anmelden, werden ihnen zwei spezielle Berechtigungen zugeteilt:

1. Sie können bestimmte Programme ausführen, die Sie normalerweise nicht ausführen können.
2. Sie haben 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 gleichen 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.

12.2.1 Deaktivieren der Möglichkeit, mit der Tastenkombination Strg-Alt- Entf herunterzufahren

Standardmäßig ist durch `/etc/inittab` festgelegt, dass Ihr System mit der Tastenkombination [Strg]-[Alt]-[Entf] der Konsole sowohl heruntergefahren als auch neu gebootet werden kann. Wenn Sie diese Möglichkeit komplett deaktivieren wollen, müssen Sie die folgende Zeile aus `/etc/inittab` herauskommentieren:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Sie können auch bestimmten Nicht-Root Benutzern erlauben, das System von der Konsole aus mit der Tastenkombination [Strg]-[Alt]-[Entf] herunterzufahren. Sie können diese Berechtigung auf bestimmte Benutzer beschränken, indem Sie folgende Schritte durchführen:

1. Fügen Sie die Option `-a` in die oben angezeigte Zeile `/etc/inittab` ein, so dass sie wie folgt aussieht:

   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```

   Die Anzeige `-a` weist `shutdown` an nach der Datei `/etc/shutdown.allow` zu suchen, die Sie im nächsten Schritt erstellen:

2. Erstellen Sie in `/etc` die Datei `shutdown.allow`. Die Datei `shutdown.allow` sollte alle Namen der Benutzer beinhalten, die das System mit der Tastenkombination [Strg]-[Alt]-[Entf] herunterfahren dürfen. Das Dateiformat sieht dann wie folgt aus:

   ```
   Stephen
   Jack
   Sophie
   ```

Gemäß diesem Beispiel für die Datei `shutdown.allow` dürfen somit Stephen, Jack und Sophie das System von der Konsole aus mit der Tastenkombination [Strg]-[Alt]-[Entf] herunterfahren. Sobald diese Tastenkombination verwendet wird, überprüft `shutdown -a` (in `/etc/ inittab` abgelegt), ob alle Benutzer (oder Root) von `/etc/shutdown.allow` auf einer virtuellen Konsole angemeldet

sind. Ist dies der Fall, wird das System weiter heruntergefahren, andernfalls wird eine Fehlermeldung auf die Systemkonsole geschrieben.

Weitere Informationen über `shutdown.allow` finden Sie unter der `shutdown` man-Seite.

12.2.2 Deaktivieren des Zugriffs auf Programme über die Konsole

Wenn Sie den Zugriff auf Programme über die Konsole deaktivieren wollen, sollten Sie folgenden Befehl als Root ausführen:

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

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/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

12.2.3 Deaktivieren aller Zugriffe über die Konsole

Das PAM-Modul `pam_console.so` verwaltet Konsolen-Datei-Berechtigungen und Authentifikationen. (Mehr Informationen über die Konfiguration von PAM erhalten Sie unter Kapitel 8, *Pluggable Authentication Modules (PAM)*). 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
```

12.2.4 Definieren der Konsole

Das Modul `pam_console.so` verwendet `/etc/security/console.perms` zum Festlegen der Berechtigungen für Benutzer der Systemkonsole. 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
```

12.2.5 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]* \
    /dev/floppy/*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
    /dev/mixer* /dev/sequencer \
    /dev/sound/*
<cdrom>=/dev/cdrom* /dev/cdwriter*
```

Sie können auch eigene Zeilen hinzufügen. Stellen Sie sicher, dass sich alle Zeilen, die Sie hinzufügen, auf das entsprechende Gerät beziehen. Sie können zum Beispiel folgende Zeile hinzufügen:

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

(Natürlich muss `/dev/sga` 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 <Sound>  0640 root
<Konsole> 0600 <CD-ROM>  0600 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).

12.2.6 Aktivieren des Zugriffs auf andere Anwendungen über die Konsole

Um Konsolenbenutzern neben `shutdown`, `reboot` und `halt` Zugriff auf weitere Anwendungen zu geben, ist etwas mehr Aufwand notwendig.

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. Nachdem Sie das überprüft haben, führen Sie folgende Schritte aus:

1. Erstellen Sie einen Link vom Namen Ihrer Anwendung mit der Anwendung `/usr/bin/consolehelper`. (Wie unser Beispielprogramm *`foo`*):

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

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

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

3. 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/halt /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.

12.3 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 fred zur Gruppe `floppy` hinzufügen können:

```
[root@bigdog root]# gpasswd -a fred floppy
```

```
Adding user fred to group floppy
[root@bigdog root]#
```

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

Teil III Apache

13 Verwendung von Apache als Secure Web-Server

13.1 Einführung

Dieses Kapitel enthält grundlegende Informationen über die Installation des Apache World Wide Web (WWW oder Web)-Servers mit dem mod_ssl-Sicherheitsmodul sowie der OpenSSL-Bibliothek und dem Toolkit. Die Kombination dieser drei mit Red Hat Linux gelieferten Komponenten wird in diesem Handbuch als secure Web server bezeichnet (oder kurz Secure 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. 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/).

Der Apache-Web-Server hat eine modulare Struktur. Er besteht aus verschiedenen "Teilcodes", die für die unterschiedlichen Aspekte oder Funktionen des Web-Servers gelten. Diese Modularität wurde so eingerichtet, dass jeder Entwickler seine eigenen Teilcodes für seine speziellen Bedürfnisse erstellen kann. Diese Codes, auch Module genannt, können dann relativ einfach in den Apache-Web-Server integriert werden.

Das Modul mod_ssl ist ein Sicherheitsmodul für den Apache Web-Server. Es 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 gelesen 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 wird die Installation dieser Programme beschrieben. Weiterhin werden die Schritte beschrieben, die notwendig sind, um ein eigensigniertes Zertifikat zu erstellen sowie ein Zertifikat zu installieren, das Sie für Ihren Secure Web-Server verwenden können.

13.2 Danksagungen

Der secure Web server enthält folgende Komponenten:

- Von der Apache Group entwickelte Software für die Verwendung im Apache HTTP-Server-Projekt (http://httpd.apache.org)
- 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.

13.3 Überblick über die Pakete für die Sicherheit

Für die Installation eines Secure Servers müssen Sie mindestens drei Pakete installieren:

`Apache`

Das Paket `Apache` enthält den Dämon `httpd` und dazugehörige Dienstprogramme, Konfigurationsdateien, Symbole, Apache-Module, man-Seiten und andere Dateien, die vom Apache-Web-Server verwendet werden.

`mod_ssl`

Das Paket `mod_ssl` enthält das mod_ssl-Modul, in dem die Protokolle Secure Sockets Layer (SSL) und Transport Layer Security (TLS) zur wirksamen Verschlüsselung des Apache-Web-Servers enthalten sind.

`openssl`

Das Paket `openssl` enthält das OpenSSL- Toolkit. Dieses Toolkit implementiert die Protokolle SSL und TLS und enthält eine universelle Verschlüsselungsbibliothek.

Zusätzlich können andere, in Red Hat Linux enthaltene Softwarepakete einige Sicherheitsfunktionen enthalten (sind aber für den Secure Server nicht erforderlich):

`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 secure Web server mit der DSO-Funktionalität von Apache finden Sie in Abschnitt 14.3, *Hinzufügen von Modulen zu Ihrem Server*.

Wenn Sie keine weiteren Module in den 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.

OpenSSH Pakete

Die Pakete OpenSSH enthalten einen Satz von OpenSSL-Netzwerk- Verbindungstools zum Anmelden und Ausführen von Befehlen auf einem Remote-Rechner. OpenSSH-Tools verschlüsseln den gesamten Datenverkehr (einschließlich der Passwörter), um das Mithören, den Missbrauch der Verbindungen und andere Angriffe auf die Kommunikation zwischen Ihrem Rechner und einem Remote-Rechner zu verhindern.

Das Paket `openssh` enthält die Haupt-Dateien, die sowohl von den OpenSSH-Client-Programmen als auch vom OpenSSH-Server benötigt werden. Es enthält außerdem `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 entsprechenden Dateien. 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, einschließlich der folgenden: `ssh`, ein sicheres Programm zum Erstatz von `rsh` sowie `slogin`, ein sicheres Programm zum Ersatz von `rlogin` (Remote-Anmeldung) und `telnet` (Kommunikation mit einem anderen Rechner über das TELNET-Protokoll).

Weitere Informationen zu OpenSSH finden Sie in Kapitel 11, *SSH-Protokoll* und auf der OpenSSH-Website unter http://www.openssh.com.

`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.

`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.

Tabelle 13–1, *Sicherheitspakete* zeigt die Speicherstelle des Secure Server-Pakets und zusätzlich sicherheitsbezogene Pakete innerhalb der von Red Hat Linux zur Verfügung gestellten Paketgruppen. Diese Tabelle gibt an, ob jedes Paket für die Installation eines Secure Web-Servers optional ist oder nicht.

Tabelle 13–1 Sicherheitspakete

Paketbezeichnung	Enthalten in Gruppe	Optional?
`apache`	Systemumgebungen/Dämonen	Nein
`mod_ssl`	Systemumgebungen/Dämonen	Nein
`openssl`	Systemumgebungen/Bibliotheken	Nein
`apache-devel`	Entwicklung/Bibliotheken	Ja
`apache-manual`	Dokumentation	Ja
`openssh`	Anwendungen/Internet	Ja
`openssh-askpass`	Anwendungen/Internet	Ja

Paketbezeichnung	Enthalten in Gruppe	Optional?
`openssh-askpass-gnome`	Anwendungen/Internet	Ja
`openssh-clients`	Anwendungen/Internet	Ja
`openssh-server`	Systemumgebung/Dämonen	Ja
`openssl-devel`	Entwicklung/Bibliotheken	Ja
`stunnel`	Anwendungen/Internet	Ja

13.4 Installieren des Secure Servers

Sie können secure Web server auf folgende Weise installieren:

- *Während einer Neuinstallation von Red Hat Linux* — da der 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 Secure Server auf diese Weise installieren. Weitere Informationen zur Installation von secure Web server im Zusammenhang mit einer Neuinstallation von Red Hat Linux finden Sie in Abschnitt 13.5, *Installieren des Secure Servers mit Red Hat Linux*.
- *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 7.1 aktualisieren möchten, müssen Sie die Pakete für den Secure Server während des Aktualisierungsprozesses installieren. Wichtige Informationen darüber, was bei der Aktualisierung von Red Hat Linux zu beachten ist, finden Sie in Abschnitt 13.6, *Aktualisieren einer älteren Version von Red Hat Linux*.
- *Installation des Secure Servers nach der Installation von Red Hat Linux 7.1* — wenn Sie Red Hat Linux 7.1 vorher installiert haben und zu einem späteren Zeitpunkt die Funktionalität des Secure Servers nutzen möchten, können Sie die Pakete für den Secure Server mit RPM), GNOME-RPM oder mit Kpackage von einer Red Hat Linux-CD installieren. Informationen über die Installation des Secure Servers nach der Installation von Red Hat Linux finden Sie unter Abschnitt 13.7, *Installieren des Secure Servers nach der Installation von Red Hat Linux* .

Aktualisieren von Apache

Wenn Sie den secure Web server installieren, während Sie eine frühere Version von Apache aktualisieren (einschließlich aller früheren Versionen von secure Web server), benötigen Sie außerdem bestimmte Informationen zum Aktualisierungsprozess. Informieren Sie sich dazu in Abschnitt 13.8, *Aktualisieren einer älteren Version von Apache*, bevor Sie den Installationsprozess beginnen, wenn Sie Apache aktualisieren.

13.5 Installieren des Secure Servers mit Red Hat Linux

Wenn Sie Red Hat Linux und den secure Web server gleichzeitig installieren, folgen Sie bitte den auf Ihre Architektur abgestimmten Anleitungen im Installationshandbuch. Wenn Sie Ihr Red Hat Linux System als Secure Server verwenden möchten, sollten Sie sich für Server- oder benutzerdefinierte Installation entscheiden. Sie können aus folgenden Installationsklassen wählen:

- Installationsklasse Server: wenn Sie sich hierfür entscheiden, werden die Pakete für den Secure Server (`apache`, `mod_ssl` und `openssl`) automatisch ausgewählt. Die Pakete `stunnel` und `openssh` enthalten sicherheitsrelevante Funktionen und werden ebenfalls mit ausgewählt.
- Installationsklasse Workstation (oder Laptop-Installation, falls vorhanden): wenn Sie sich hierfür entscheiden, werden die Pakete für den Secure Server und sicherheitsrelevanten Pakete nicht automatisch für die Installation ausgewählt, Sie können diese jedoch während des benutzerdefinierten Paketauswahlprozesses installieren.
- Benutzerdefinierte Installation: wenn Sie sich hierfür entscheiden, müssen Sie die zu installierenden Pakete für den Secure Server und die 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 Secure 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 13.3, *Überblick über die Pakete für die Sicherheit* beschriebenen zusätzlichen sicherheitsrelevanten Pakete installieren möchten, müssen Sie dies im Installationsprogramm angeben. Wählen Sie dazu **Auswahl einzelner Pakete** im Bildschirm **Paketgruppenauswahl**.

Wählen Sie die zu installierenden sicherheitsrelevanten Pakete aus. Gehen Sie dazu nach den Anleitungen in Ihrem Installationshandbuch vor. Für die Auswahl steht Ihnen die Tabelle Tabelle 13–1, *Sicherheitspakete* mit den entsprechenden Verzeichnissen zur Verfügung.

Überprüfen Sie noch einmal, ob die richtigen Pakete ausgewählt sind, und fahren Sie dann mit dem Installationsprozess fort. Wenn die Installation von Red Hat Linux und des Secure Servers abgeschlossen ist, lesen Sie Abschnitt 13.9, *Ein Überblick über Zertifikate und Sicherheit*.

13.6 Aktualisieren einer älteren Version von Red Hat Linux

Wenn auf Ihrem System bereits eine frühere Version von Red Hat Linux vorhanden ist, können Sie statt einer kompletten Installation ein Upgrade von Red Hat Linux 7.1 vornehmen. Wenn Sie sich also für die Aktualisierung entscheiden, müssen Sie **Upgrade** an Stelle der Installationsklasse wählen. Folgen Sie den Anweisungen des auf Ihre Architektur abgestimmten Installationshandbuches. Stellen Sie sicher, dass bei einem Upgrade die Pakete für den Secure Server vom Installationsprogramm ausgewählt wurden.

Wenn Sie ein Upgrade Ihres Red Hat Linux Systems durchführen, überprüft das Installationsprogramm, welche Pakete bereits installiert sind. Diese Pakete werden während des Aktualisierungsprozesses automatisch auf die Version von Red Hat Linux7.1 aktualisiert. Ist ein bestimmtes Paket jedoch nicht installiert, wird auch vom Installationsprogramm keine neue Version dieses Paketes installiert — es sei denn, Sie passen Ihre Aktualisierung entspechend an.

Wenn Sie ein Upgrade von Red Hat Linux 7.0 oder einer späteren Version durchführen wollen und das Paket secure Web server installiert ist, wird das Secure Server-Paket aktualisiert. Ist das secure Web server Paket jedoch nicht installiert, müssen Sie während des benutzerdefinierten Paketauswahlprozesses die Pakete `apache`, `mod_ssl` und `openssl` auswählen. In Abschnitt 13.6.1, *Anpassung der Aktualisierung für die Installation des Secure Servers* erhalten Sie weitere Informationen über die auszuwählenden Pakete.

Wenn Sie ein Upgrade einer US- oder kanadischen Version von Red Hat Linux Professional durchführen, müssen Sie das Upgrade anpassen und das Secure Server-Paket wählen. Auch wenn Sie `apache` installiert haben, sind `mod_ssl` und `openssl` nicht installiert, da sie in den Red Hat Linux- Versionen vor Red Hat Linux 7.0 nicht enthalten sind. Sie müssen das Upgrade anpassen, um `mod_ssl` und `openssl` doch auswählen zu können. Abschnitt 13.6.1, *Anpassung der Aktualisierung für die Installation des Secure Servers* enthält weitere Informationen über die zu wählenden Pakete.

Wenn Sie ein Upgrade einer internationalen Version von Red Hat Linux Professional durchführen und die Pakete `apache`, `mod_ssl` und `openssl` installiert sind, werden sie vom Installationsprogramm automatisch ausgewählt und aktualisiert.

Wenn Sie ein Upgrade einer internationalen Version von Red Hat Linux Professional durchführen und die Pakete `apache`, `mod_ssl` und `openssl` nicht installiert sind, müssen Sie Ihre Aktualisierung anpassen und diese Pakete für die Installation auswählen. Abschnitt 13.6.1, *Anpassung der Aktualisierung für die Installation des Secure Servers* enthält Anweisungen, wo die auszuwählenden Pakete zu finden sind.

13.6.1 Anpassung der Aktualisierung für die Installation des Secure Servers

Wenn Sie den Aktualisierungsprozess anpassen müssen, folgen Sie bitte den Aktualisierungsanleitungen Ihres Installationshandbuches. Im Prinzip ist **Upgraden** als **Installationstyp** und dann **Zu aktualisierende Pakete auswählen** auszuwählen. Anschließend müssen Sie, wie in Ihrem Installationshandbuch beschrieben, die zu aktualisierenden Pakete auswählen. Zur Erleichterung der Auswahl ist in Tabelle 13–1, *Sicherheitspakete* angegeben, wo jedes Server-relevante Paket abgelegt ist und ob es optional ist.

Wenn die Aktualisierung aller Apache-Versionen abgschlossen ist, lesen Sie Abschnitt 13.8, *Aktualisieren einer älteren Version von Apache*. Haben Sie Apache nicht aktualisiert, fahren Sie fort unter Abschnitt 13.9, *Ein Überblick über Zertifikate und Sicherheit*.

13.7 Installieren des Secure Servers nach der Installation von Red Hat Linux

Wenn Sie Red Hat Linux 7.1 ohne die Pakete für den Secure Server installiert haben, können Sie den Secure Server auch später installieren. Die einfachste Möglichkeit dafür ist die Installation der auf der Red Hat Linux-CD enthaltenen RPM-Pakete mit RPM, GNOME-RPM oder Kpackage.

13.7.1 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 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
```

13.7.2 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 Secure Server verwenden.

Weitere Informationen zur Verwendung von GNOME-RPM finden Sie im *Offiziellen Red Hat Linux Handbuch Erste Schritte* 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/.

Nachdem Sie die erforderlichen Pakete installiert haben, besteht der nächste Schritt darin, Ihren Schlüssel zu erstellen und ein Zertifikat zu beantragen. Fahren Sie dazu mit Abschnitt 13.9, *Ein Überblick über Zertifikate und Sicherheit* fort.

13.7.3 Verwenden von RPM

Die secure Web server-Pakete stehen im RPM-Format zur Verfügung, so dass Sie die Pakete unter Verwendung von RPM installieren können. Im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration* finden Sie weitere Informationen über RPM. Wenn Sie sich nicht sicher sind, welche Pakete Sie installieren sollen, erhalten Sie entsprechende Hilfe unter Tabelle 13–1, *Sicherheitspakete*.

Nachdem Sie die Pakete für den Secure Server installiert haben und Sie alle Versionen von Apache aktualisieren, lesen Sie Abschnitt 13.8, *Aktualisieren einer älteren Version von Apache*. Wenn Sie Apache nicht aktualisieren, fahren Sie mit Abschnitt 13.9, *Ein Überblick über Zertifikate und Sicherheit* fort.

13.8 Aktualisieren einer älteren Version von Apache

Wenn Sie die Secure Server-Pakete, bei einer Aktualisierung von Apache installieren, müssen Sie zwei wichtige Punkte beachten:

- In der in Red Hat Linux 7.1 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.

13.8.1 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 14.2.28, *`DocumentRoot`* eine detailliertere Erklärung.

Vor der Version 7.0 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, dass in Red Hat Linux 7.1 die Standardeinstellung für `DocumentRoot` jetzt `/var/www/html` ist.

Ist das für Sie von Bedeutung? Es ist dann von Bedeutung, wenn Sie Apache mit einer anderen `DocumentRoot` verwenden, und Sie die gleichen Web-Seiten mit Ihrer neuen Konfiguration von Apache nutzen. Alle Web-Seiten, die vorher in einer anderen `DocumentRoot` untergebracht waren, werden von dem mit Red Hat Linux 7.1 ausgelieferten Apache in der Standardkonfiguration nicht mehr gefunden. Deshalb müssen Sie eine der folgenden Aktionen durchführen:

Verschieben Sie alle Dateien 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 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.

13.8.2 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 Konfigurationsdatei für den Secure Server übertragen. Bitte beachten Sie, wenn Sie das Apache Configuration Tool verwenden, dass Sie `httpd.conf` nicht manuell bearbeiten müssen. Im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration* finden Sie weitere Informationen über Apache Configuration Tool.

13.9 Ein Überblick über Zertifikate und Sicherheit

Die von secure Web server zur Verfügung gestellte Sicherheit ist eine Kombination aus dem Secure Sockets Layer (SSL)-Protokoll und (meistens) einem digitalen Zertifikat von der Zertifizierungsstelle (ZS). SSL verwaltet die verschlüsselte Kommunikation und die gegenseitige Authentifizierung zwischen Browsern und Ihrem secure Web server. Die durch die ZS zugelassenen digitalen Zertifikate stellen die Authentifizierung für secure Web server bereit (die ZS stellt nach der Zertifizierung Ihrer Organisation ihre Reputation zur Verfügung). Wenn Ihr Browser unter Verwendung der SSL- Verschlüsselung kommuniziert, erscheint im Balken zum Navigieren, am Anfang des Uniform Resource Locators (URL) das Präfix https://.

Die Verschlüsselung ist von den verwendeten Schlüsseln abhängig (Sie können sie sich als eine Art Sicherheitsring zur Verschlüsselung und Entschlüsselung im Datenformat vorstellen). Konventionelle oder symmetrische Kryptografie: beide Transaktionen haben am Ende den gleichen Schlüssel, mit dem sie gegenseitig ihre Übertragungen entschlüsseln können. In der öffentlichen oder asymmetrischen Kryptografie bestehen gleichzeitig zwei Schlüssel: ein öffentlicher Schlüssel und ein privater Schlüssel. Eine Person oder Organisation hält ihren privaten Schlüssel geheim und veröffentlicht den öffentlichen Schlüssel. Mit dem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem privaten Schlüssel entschlüsselt, und mit dem privaten Schlüssel verschlüsselte Daten können nur mit dem öffentlichen Schlüssel entschlüsselt werden.

Für die Einstellung Ihres Secure Servers müssen Sie unter Verwendung der öffentlichen Kryptografie ein Paar öffentlicher und privater Schlüsseln erstellen. In den meisten Fällen müssen Sie Ihren Antrag für ein Zertifikat (einschließlich dem öffentlichen Schlüssel), einen Nachweis der Identität Ihres Unternehmens und die Zahlung an die ZS verschicken. Die ZS überprüft Ihren Antrag und Ihre Identität und schickt dann ein Zertifikat für Ihren secure Web server zurück.

Ein Secure Server benutzt ein Zertifikat, um sich für den Web- Browser zu identifizieren. Sie können sowohl Ihr eigenes Zertifikat erstellen (eigensigniertes Zertifikat genannt) als auch ein Zertifikat von einer Zertifizierungsstelle oder ZS erhalten. Ein Zertifikat, das Sie von der ZS erhalten haben, garantiert, dass eine Web-Site mit einem bestimmten Unternehmen oder Organisation in Verbindung steht.

Alternativ dazu können Sie Ihr eigensigniertes Zertifikat erstellen. Diese Zertifikate sollen jedoch nicht in Produktionsumgebungen verwendet werden. Eigensignierte Zertifikate werden nicht automatisch vom Browser eines Benutzers akzeptiert — der Benutzer wird vom Browser gefragt, ob er das Zertifikat akzeptieren und eine sichere Verbindung herstellen möchte. Mehr Informationen über den Unterschied zwischen eigensignierten und ZS-Zertifikaten finden Sie unter Abschnitt 13.11, *Arten von Zertifikaten*.

Nachdem Sie ein eigensigniertes Zertifikat erstellt oder ein ZS-Zertifikat ausgewählt haben, müssen Sie es in secure Web server installieren.

13.10 Verwendung bereits vorhandener Schlüssel und Zertifikate

Wenn Sie bereits Schlüssel oder Zertifikate haben (z.B. wenn Sie secure Web server installieren, um einen Secure Web-Server eines anderen Unternehmens dadurch zu ersetzen), können Sie wahrscheinlich diese vorhandenen Schlüssel und Zertifikate für secure Web server verwenden. In den folgenden zwei Situationen wird angezeigt, dass Sie die vorhandenen Schlüssel und Zertifikate nicht verwenden können:

- *Wenn Sie Ihre IP-Adresse oder Ihren Domänennamen ändern* — Sie können die vorhandenen Schlüssel und Zertifikate nicht verwenden, wenn Sie Ihre IP-Adresse oder Ihren Domänennamen ändern. Da sich die Zertifikate auf eine bestimmte IP-Adresse und Domänennamen beziehen, müssen Sie bei der Änderung der IP-Adresse und des Domänennamens ein neues Zertifikat beantragen.
- *Wenn Sie ein Zertifikat von VeriSign haben und Ihre Serversoftware ändern* — VeriSign ist eine sehr verbreitete ZS. Wenn Sie bereits ein Zertifikat von VeriSign zu einem anderen Zweck haben, würde es sich anbieten, dieses für Ihren neuen secure Web server zu verwenden. Dies ist jedoch nicht möglich, da VeriSign die Zertifikate für eine bestimmte Serversoftware und eine Kombination aus der IP-Adresse und Domänennamen erteilt.

  Wenn Sie eines dieser Parameter ändern (z.B. wenn Sie einen Secure Web-Server eines anderen Unternehmens verwendet haben und jetzt secure Web server benutzen möchten), können Sie das VeriSign-Zertifikat, das Sie für die vorherige Konfiguration genutzt haben, für die neue Konfiguration nicht mehr verwenden. Sie müssen ein neues Zertifikat beantragen.

Wenn Sie bereits einen Schlüssel und ein Zertifikat haben, das Sie verwenden können, müssen Sie weder einen neuen Schlüssel noch ein neues Zertifikat erstellen. Sie müssen jedoch die Dateien, die Ihren Schlüssel und Ihr Zertifikat enthalten, verschieben und umbenennen.

Verschieben Sie Ihre vorhandene Schlüsseldatei in das Verzeichnis:

```
/etc/httpd/conf/ssl.key/server.key
```

Verschieben Sie Ihre vorhandene Zertifikatdatei in das Verzeichnis:

```
/etc/httpd/conf/ssl.crt/server.crt
```

Nachdem Sie Ihren Schlüssel und Ihr Zertifikat verschoben haben, gehen Sie zu Abschnitt 13.15, *Testen Ihres Zertifikats*.

Wenn Sie die Version 1.0 oder 2.0 des Red Hat Secure Web-Servers aktualisieren, wird Ihr alter Schlüssel (`httpsd.key`) und das Zertifikat (`httpsd.crt`) im Verzeichnis `/etc/httpd/conf/` abgelegt. Damit sie von secure Web server verwendet werden können, müssen Sie die Schlüssel- und Zertifikatdatei verschieben und umbenennen. Führen Sie dazu die folgenden zwei Befehle aus:

```
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 danach den secure Web server, wie in Abschnitt 14.1, *Starten und Anhalten von* `httpd` beschrieben. Wenn Sie eine frühere Version von secure Web server aktualisieren, brauchen Sie kein neues Zertifikat.

13.11 Arten von Zertifikaten

Wenn Sie secure Web server mit dem Red Hat Linux Installationsprogramm installiert haben, wird ein willkürlicher Schlüssel und ein Testzertifikat erstellt und in die entsprechenen Verzeichnisse abgelegt. Bevor Sie Ihren Secure Server verwenden, müssen Sie jedoch Ihren eigenen Schlüssel und Ihr eigenes Zertifikat mit den korrekten Angaben Ihres Servers erstellen.

Um mit secure Web server arbeiten zu können, benötigen Sie einen Schlüssel und ein Zertifikat — das bedeutet, dass Sie entweder ein eigensigniertes Zertifikat erstellen oder ein durch ZS-signiertes (auch offizielles) Zertifikat erhalten. Worin besteht der Unterschied zwischen diesen beiden Zertifikaten?

Ein ZS-signiertes Zertifikat liefert zwei wichtige Fähigkeiten für Ihren Server:

- Browser erkennen das Zertifikat in der Regel automatisch an. Die gesicherte Verbindung wird ohne zusätzliche Bestätigung durch den Benutzer hergestellt.
- Wenn die ZS ein signiertes Zertifikat ausstellt, wird die Identität der Organisation garantiert, die die Web-Seiten für den Browser zur Verfügung stellt.

Wenn auf Ihren Secure Server im Allgemeinen öffentlich zugegriffen werden kann, benötigt secure Web server ein ZS-signiertes Zertifikat, so dass die Personen, die Ihre Website anschauen, sicher sein können, dass diese Website tatsächlich Eigentum der Organisation ist, die dies behauptet. Bevor die ZS ein Zertifikat signiert, wird überprüft, ob die Organisation, die das Zertifikat beantragt, auch die Organisation ist für die sie sich ausgibt.

Die meisten Web-Browser, die SSL unterstützen, haben eine Liste von ZSs, deren Zertifikate automatisch akzeptiert werden. Wenn ein Browser auf ein Zertifikat trifft, dessen ZS-Authorisierung nicht in der Liste aufgeführt ist, wird der Benutzer vom Browser aufgefordert, die Verbindung entweder anzunehmen oder zu abzulehnen.

Sie können für Red Hat Linux ein eigensigniertes Zertifikat erstellen, sollten aber bedenken, dass diese Zertifikate nicht die gleichen Funktionen zur Verfügung stellen wie ZS-signierte Zertifikate. Ein eigensigniertes Zertifikat wird nicht nicht automatisch vom Browser des Benutzers erkannt und kann auch nicht die Identität der Organisation garantieren, die eine Website zur Verfügung stellt. Ein ZS-signiertes Zertifikat dagegen liefert beide Fähigkeiten. Wenn Ihr Secure Server in einer Produktionsumgebung eingebunden ist, benötigen Sie wahrscheinlich ein ZS-signiertes Zertifikat.

Die Beantragung eines Zertifikates von einer Zertifizierungsstelle ist denkbar einfach, wie der kurze Überblick zeigt:

1. Erstellen Sie einen privaten und einen öffentlichen Schlüssel.
2. Erstellen Sie einen Zertifikatsantrag, der auf dem öffentlichen Schlüssel basiert. Der Antrag enthält Informationen über Ihren Server und Ihr Unternehmen.
3. Senden Sie das gewünschte Zertifikat zusammen mit den Dokumenten, die Ihre Identität belegen, an eine ZS. Da die Wahl des Zertifikats wahrscheinlich auf eigenen Erfahrungen oder Erfahrungen von Freunden oder Kollegen beruht, können wir Ihnen keinen Vorschlag machen, für welche Zertifizierungsstelle Sie sich entscheiden sollten.

   Um die Liste anzuzeigen, klicken Sie auf den Button **Sicherheit** Ihres Navigator- Balkens oder auf Vorhängeschloss-Symbol unten links in Ihrem Bildschirm. Klicken Sie danach auf **Unterzeichner** und Sie sehen die Liste der Unterzeichner der Zertifikate, von denen Ihr Browser Zertifikate annimmt. Sie können auch im Web Informationen über ZSs finden. Wenn Sie sich für eine ZS entschieden haben, müssen Sie der in der ZS enthaltenen Anweisung folgen, um ein Zertifikat zu erhalten.
4. Nach Überprüfung der Identität und Echtheit Ihres Unternehmens sendet die Zertifizierungsstelle Ihnen ein digitales Zertifikat.
5. Installieren Sie dieses Zertifikat auf Ihrem Web-Server, und Ihre Transaktionen sind nun gegen unerlaubten Zugriff geschützt.

Ob Sie von einer ZS ein Zertifikat erhalten oder ein eigensigniertes Zertifikat erstellen - der erste Schritt ist die Erstellung eines Schlüssels. Unter Abschnitt 13.12, *Erstellen eines Schlüssels* finden Sie Anweisungen über die Erstellung eines Schlüssels.

13.12 Erstellen eines Schlüssels

Geben Sie als Erstes den Befehl `cd` ein, um in das Verzeichnis `/etc/httpd/conf` zu gelangen. Entfernen Sie den falschen Schlüssel und das Zertifikat, die während der Installation erstellt wurden, mit den folgenden Befehlen:

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

Danach müssen Sie Ihren eigenen Zufallsschlüssel erstellen. Geben Sie dazu folgenden Befehl ein:

```
make genkey
```

Ihr System wird folgende (oder eine ähnliche) Mitteilung anzeigen:

```
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:
```

Sie müssen jetzt ein Passwort eingeben. Zur Sicherheit sollte Ihr Passwort mindestens acht Zeichen enthalten, einschließlich Ziffern und Satzzeichen. Es sollte kein Wort aus einem Wörterbuch sein. Sie sollten Ihr Passwort gut auswählen.

Bitte beachten

Sie müssen bei jedem Start von secure Web server Ihr Passwort eingeben. Sie sollten es also nicht vergessen.

Sie werden aufgefordert, Ihr Passwort zur Bestätignung ein zweites Mal einzugeben. Dadurch wird sichergestellt, dass es korrekt ist. Nach der korrekten Eingabe wird die Datei `server.key` erstellt, die Ihren Schlüssel enthält.

Wenn Sie nicht bei jedem Start von secure Web server Ihr Passwort eingeben möchten, können Sie die folgenden zwei Befehle statt `make genkey` für die Erstellung eines Schlüssels eingeben. Beide Befehle sollten auf einer Zeile eingegeben werden:

Verwenden Sie die folgenden Befehle:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

Für die Erstellung des Schlüssels verwenden Sie dann den folgenden Befehl:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

um sicherzustellen, dass die Berechtigungen für Ihren Schlüssel korrekt gesetzt sind.

Nachdem Sie für die Erstellung Ihres Schlüssels die oben aufgeführten Befehle verwendet haben, brauchen Sie für den Start von secure Web server kein Passwort einzugeben.

Die Deaktivierung der Passwort-Funktion für Ihren Secure Server ist ein Sicherheitsrisiko. Aus diesem Grund empfehlen wird Ihnen, die Passwort-Funktion für Ihren secure Web server NICHT außer Kraft zu setzen.

Die Probleme, die auftreten, wenn das Passwort nicht benutzt wird, haben direkten Einfluss auf die Sicherheit des Rechners. Wenn zum Beispiel jemand die reguläre UNIX-Sicherheit eines Rechners

überwindet, kann diese Person Ihren privaten Schlüssel (die Inhalte Ihrer `server.key` Datei) abrufen. Der Schlüssel kann benutzt werden, um falsche Web-Seiten zu erstellen, die scheinbar von Ihrem Web-Server stammen.

Wenn die UNIX-Sicherheitsregeln strikt eingehalten und gewartet werden (d.h. alle Betriebssystem-Patches und -aktualisierungen werden bei Verfügbarkeit installiert, es werden keine unnötigen oder risikoreichen Dienste in Anspruch genommen usw.) erscheint das secure Web server-Passwort unnötig. Da der secure Web server jedoch nicht oft neu gebootet 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 ZS wird Ihnen nicht helfen können. Die einzige Möglichkeit wäre dann das Beantragen (und Bezahlen) eines neuen Zertifikats.

Wenn Sie ein Zertifikat von einer ZS erwerben, fahren Sie bei Abschnitt 13.13, *Erzeugen von Zertifikatsanträgen für die ZS* fort. Möchten Sie Ihr eigensigniertes Zertifikat erstellen, fahren Sie unter Abschnitt 13.14, *Erstellen eines eigensignierten Zertifikats* fort.

13.13 Erzeugen von Zertifikatsanträgen für die ZS

Sobald Sie einen Schlüssel erstellt haben, müssen Sie als Nächstes das gewünschte Zertifikat bei einer ZS Ihrer Wahl beantragen:

```
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 für die Erstellung Ihres Schlüssels gewählt haben. Ihr System wird einige Anweisungen anzeigen und Sie werden aufgefordert, eine Reihe von Fragen zu beantworten. Ihre Eingaben werden in den Antrag für das Zertifikat integriert. 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]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:Durham
Organization Name (eg, company) [Internet Widgits]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.mydomain.com
Email Address []:admin@mydomain.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`). Folgen Sie dazu diesen Richtlinien:

- Schreiben Sie den Namen der Stadt und des Landes aus und kürzen Sie ihn nicht ab (z.B. St. Augustin wird Sankt Augustin geschrieben).
- Wenn Sie diese Anforderung an eine ZS schicken, stellen Sie sicher, dass alle Informationen in allen Dialogfeldern vollständig und richtig sind, im Besonderen `Organization Name` und `Common Name`. Die ZS überprüft die Angaben und weist solche, die als ungültig erkannt werden, zurück.
- Stellen Sie bei der Eingabe des `Common Name` sicher, dass Sie den *wirklichen* Namen Ihres secure Web server (ein gültiger DNS-Name) und keinen Alias-Namen eingegeben haben.
- Die `Email Address` sollte mit der E-Mail-Adresse des Webmasters oder des Systemadministratos übereinstimmen.

- Vermeiden Sie jegliche Sonderzeichen wie @, #, &, !, etc. Einige Zertifizierungsstellen weisen Zertifikatanträge, die Sonderzeichen enthalten, zurück. Wenn also der Name Ihrer Firma ein Und-Zeichen (&) enthält, schreiben Sie es aus, so dass Sie statt "&", "und" eingeben.
- Die zusätzlichen Attribute (`A challenge password` und `An optional company name`) müssem Sie nicht ausfüllen. Drücken Sie einfach die [Eingabetaste], um die in der Voreinstellung leeren Felder zu akzeptieren.

Wenn die Eingabe von Informationen abgeschlossen ist, wird die Datei `server.csr` erstellt. Diese Datei ist Ihre Zertifikatanfrage, die Sie an die ZS verschicken.

Nachdem Sie sich entschieden haben, welche ZS Sie verwenden möchten, folgen Sie den Anweisungen, die in der Web-Site der ZS enthalten sind. Diese Anweisungen enthalten Informationen darüber, wie Sie Ihren Zertifikatantrag verschicken, ob es andere Dokumentationen gibt, und über die Zahlungsmodalitäten.

Das Zertifikat von der ZS erhalten Sie üblicherweise per E-Mail. Sichern Sie das Zertifikat mit dem Namen `/etc/httpd/conf/ ssl.crt/server.crt` (Sie können es auch ausschneiden und einfügen).

13.14 Erstellen eines eigensignierten Zertifikats

Sie können Ihr eigensigniertes Zertifikat erstellen. Beachten Sie, dass diese Zertifikate nicht die Sicherheitsgarantien enthalten, wie die ZS-signierten Zertifikate. Weitere Einzelheiten über Zertifikate finden Sie unter Abschnitt 13.11, *Arten von Zertifikaten*.

Wenn Sie Ihr eigensigniertes Zertifikat erstellen möchten, müssen Sie als Erstes einen Zufallsschlüssel erstellen, wie unter Abschnitt 13.12, *Erstellen eines Schlüssels* angegeben ist. Sobald Sie diesen Schlüssel haben, geben Sie folgenden Befehl ein:

```
make testcert
```

Sie erhalten folgende Mitteilung und werden aufgefordert, Ihr Passwort einzugeben (es sei denn, Sie haben einen Schlüssel ohne Passwort erstellt):

```
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:
```

Nachdem Sie Ihr Passwort eingegeben haben (die entsprechende Eingabeaufforderung wird nicht ausgegeben, wenn die Passwortfunktion deaktiviert ist, werden Sie aufgefordert, weitere Angaben zu machen. Die Computerausgaben sowie die Eingaben sehen wie folgt aus (Sie müssen korrekte Angaben über Ihre Organisation und Ihren Rechner machen):

```
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]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:Durham
Organization Name (eg, company) [Internet Widgits]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.mydomain.com
Email Address []:myemail@mydomain.com
```

Im Anschluss daran wird ein eigensigniertes Zertifikat erstellt und in der Datei `/etc/httpd/conf/ssl.crt/server.crt` abgelegt. Nach der Erstellung des Zertifikats müssen Sie Ihren Secure Server erneut starten. Unter Abschnitt 14.1, *Starten und Anhalten von `httpd`* finden Sie Anweisungen über den Neustart Ihres Secure Servers.

13.15 Testen Ihres Zertifikats

Bei der Installation des Secure Servers mit Red Hat Linux werden ein Zufallsschlüssel und ein allgemeines Zertifikat zu Testzwecken installiert. Mit diesem Zertifikat können Sie eine Verbindung zu Ihrem Secure 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 13.11, *Arten von Zertifikaten*.

Wenn Sie ein Zertifikat von einer ZS erworben haben oder Sie haben ein Zertifikat mit eigener Signatur, verfügen Sie über die Datei `/etc/httpd/conf/ssl.key/server.key`, die Ihren Schlüssel enthält und die Datei `/etc/httpd/conf/ssl.crt/ server.crt`, die Ihr Zertifikat enthält. Wenn Schlüssel und Zertifikat in irgendwo anders abgelegt sind, verschieben Sie diese in die Verzeichnisse. Wenn Sie die Standardverzeichnisse oder Dateinamen für den 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 14.1, *Starten und Anhalten von `httpd`* 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 secure Web server entspricht der folgenden:

```
https://your_domain
```

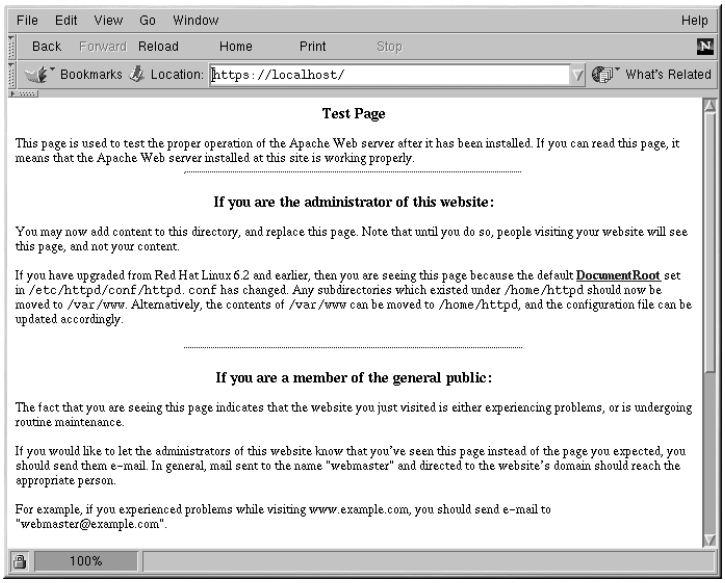
Bitte beachten

Beachten Sie, dass auf "http" ein "s" folgt. https: wird für sichere HTTP-Transaktionen verwendet.

Wenn Sie ein ZS-signiertes Zertifikat von 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 secure Web server eine Standard-Home-Page, die der in Abbildung 13–1, *Die Standard-Home-Page* entspricht.

Abbildung 13–1 Die Standard-Home-Page



13.16 Zugriff auf den Secure Server

Um auf Ihren Secure Server zuzugreifen, verwenden Sie die folgende URL:

```
https://your_domain
```

Beachten Sie, dass die URLs, die auf den secure Web server zugreifen sollen, mit dem Protokollkennzeichner https: und nicht dem gängigeren Kennzeichner http: beginnen müssen.

Auf Ihren nicht gesicherten 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 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 URLs, die in diesem Handbuch verwendet werden, müssen eventuell geändert werden. Das hängt davon ab, ob Sie auf Ihren secure Web server oder auf einen ungesicherten Web-Server zugreifen wollen. Betrachten Sie also alle in diesem Handbuch verwendeten URLs als allgemeine Beispiele und nicht auszuführende Anweisungen.

13.17 Zusätzliche Ressourcen

Wenn Sie den Schritten in der Gliederung in Kapitel 13, *Verwendung von Apache als Secure Web-Server* folgen, dabei jedoch Probleme auftreten, sollten Sie als Erstes in der Red Hat Errata der Red Hat Web-Site unter http://www.redhat.com/support/errata nachschauen.

Wenn Sie ein offizielles Red Hat Produkt einschließlich Support erworben haben, haben Sie Anspruch auf technischen Support. Stellen Sie sicher, dass Sie sich unter der Web-Site http://www.redhat.com/support für den Support registriert haben lassen.

Sie können sich in die Redhat-Secure-Server-Adressliste unter http://www.redhat.com/mailing-lists einschreiben.

Sie können sich auch per E-Mail `redhat-secure-server-request@redhat.com` in diese Liste einschreiben und dafür das Wort "subscribe" ohne Anführungszeichen in die Objektzeile eingeben.

13.17.1 Installierte Dokumentationen

Wenn Sie das Paket `apache-manual` installiert haben, können Sie auf Apache-Dokumentationen im HTML-Format in Ihrem Computer mit folgender URL zugreifen: http://localhost/manual/.

Die mod_ssl Dokumentation finden Sie unter folgender URL: http://localhost/manual/mod/mod_ssl/.

13.17.2 Hilfreiche Websites

Tips, FAQ und HOWTO-Dokumentationen finden Sie auf der Red Hat Website: http://www.redhat.com/support/docs/howto.

Die Apache Centralized Knowledgebase ist verfügbar unter http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html .

Die Apache-Website enthält eine vollständige Dokumentation für den Apache-Web-Server unter http://httpd.apache.org/docs.

Die mod_ssl Website (http: //www.modssl.org) ist die maßgebliche Quelle für Informationen über mod_ssl. Die Website enthält eine Fülle von Dokumentationen, einschließlich dem *Benutzerhandbuch* unter http: //www.modssl.org/docs.

13.17.3 Zusätzliche Literatur

Apache: The Definitive Guide, zweite Edition, von Ben Laurie und Peter Laurie, O'Reilly & Associates, Inc.

14 Apache - Anweisungen und Module

Die Standardkonfiguration von Apache 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.

WARNUNG

Wenn Sie das Konfigurationstool von Apache (ein GUI-Dienstprogramm, das zum Lieferumfang von Red Hat Linux gehört) verwenden möchten, dürfen Sie keine Änderungen an der Konfigurationsdatei `httpd.conf` Ihres Apache Web-Servers vornehmen. Wenn Sie `httpd.conf` editieren möchten, so verwenden Sie das Konfigurationstool von Apache nicht.

Weitere Informationen über das Konfigurationstool von Apache finden Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*.

Nach der Installation Ihres Web-Servers finden Sie die Dokumentation zum Apache Web-Server unter http://*your_domain*/manual/ oder Sie können die Apache Dokumentation im Web unter http://www.apache.org/docs/ einsehen. 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 Ihren 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 (Secure 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 14.4, *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.

14.1 Starten und Anhalten von `httpd`

Während des Installationsprozesses wurde das Bourne Shell-Skript `httpd` in der Datei `/etc/rc.d/init.d` gespeichert. Um Ihren Server zu starten und herunterzufahren, führen Sie `httpd` mit den Argumenten `stop` oder `start` aus.

Geben Sie folgenden Befehl ein, um Ihren Server zu starten:

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

Wenn Sie Apache als Secure Server ausführen, werden Sie aufgefordert, Ihr Passwort einzugeben. Anschließend wird Ihr Server starten.

Geben Sie folgenden Befehl ein, um Ihren Server herunterzufahren:

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

Der Befehl `restart` stellt die direkteste Möglichkeit zum Starten und Anhalten dar. Beim Neustart werden Sie aufgefordert, Ihr Passwort einzugeben, wenn Sie Apache als Secure Server verwenden. Der Befehl `restart` stellt sich wie folgt dar:

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

Auch wenn Sie Änderungen in Ihrer Datei `httpd.conf` vorgenommen haben, ist es nicht nötig, dass Sie Ihren Server anhalten und neu starten: zu diesem Zweck können Sie den Befehl `reload` verwenden. In diesem Fall müssen Sie Ihr Passwort nicht mehr eingeben (das erforderlich ist, wenn Sie Apache als Secure Server verwenden). Während der Ladevorgänge bleibt Ihr Passwort gespeichert, nicht jedoch beim Herunterladen und Starten. Dieser Befehl stellt sich wie folgt dar:

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

Standardmäßig wird `httpd` beim Booten des Rechners aktiviert. Wenn Sie Apache als Secure Server ausführen, werden Sie nach dem Booten aufgefordert, das Passwort des Secure Servers einzugeben, es sei denn, Sie haben einen Schlüssel ohne Passwort für Ihren Secure Server eingestellt.

14.2 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 Ihres Web-Servers 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 Web-Server konfigurieren müssen, ist lediglich die Datei `httpd.conf` zu editieren und anschließend der Web-Server neu zu laden oder anzuhalten und neu zu starten. Das Neuladen, Anhalten und Starten des Servers wird in Abschnitt 14.1, *Starten und Anhalten von `httpd`* 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 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 Ihres Web-Servers 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 darüber 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://*your_domain*/manual/ oder in 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:// *your_domain*/manual/mod/mod_ssl/ bzw. im mod_ssl-*User Manual* (Benutzerhandbuch) unter http://www.modssl.org/docs/2.6/.

14.2.1 `ServerType`

Die Einstellung für `ServerType` kann entweder `inetd` oder `standalone` sein. Die Standardeinstellung für Ihren Web-Server ist `ServerType standalone`.

`ServerType standalone` bedeutet, dass der Server ein Mal 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 7.1 `xinetd` verwendet, sind zusätzliche Konfigurationsarbeiten erforderlich, um über `xinetd` den Server zu starten. Aus diesen Gründen sollten Sie die Einstellung von `ServerType` Ihres Web-Servers auf `standalone` belassen.

14.2.2 ServerRoot

`ServerRoot` ist das oberste Verzeichnis, das die Serverdateien enthält. Sowohl der Server mit Verschlüsselung (Secure Server) als auch der Server ohne Verschlüsselung sind auf die Verwendung von `/etc/httpd` als `ServerRoot` eingestellt.

14.2.3 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.

14.2.4 PidFile

`PidFile` gibt die Datei an, in der der Server seine Prozess-ID (pid) ablegt. Ihr Web-Server ist so konfiguriert, dass er seine pid in `/var/run/httpd.pid` ablegt.

14.2.5 ScoreBoardFile

Im `ScoreBoardFile` werden interne Serverprozessinformationen gespeichert, die für die Kommunikation zwischen dem Eltern-Serverprozess und seinen Kind-Prozessen verwendet wird. Das `ScoreBoardFile` Ihres Web-Servers ist auf `/var/run/httpd.scoreboard` eingestellt.

14.2.6 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.

14.2.7 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.

14.2.8 Timeout

`Timeout` gibt die Zeit in Sekunden an, die der Server bei 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 PUT-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.

14.2.9 KeepAlive

`KeepAlive` kann verwendet werden, um zu verhindern, dass ein einzelner Client zu viele der Serverressourcen verbraucht. Die Standardeinstellung für `KeepAlive` ist `on`, d.h. 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 14.2.10, *`MaxKeepAliveRequests`* .

14.2.10 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.

14.2.11 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`.

14.2.12 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.

14.2.13 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.

14.2.14 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.

14.2.15 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`.

14.2.16 Listen

Der Befehl `Listen` kennzeichnet den Port, an dem Ihr Web-Server ankommende Anforderungen annimmt. Der Web-Server ist so konfiguriert, dass auf Port 80 auf unverschlüsselte Web-Kommunikation und (in Virtual Host-Tags, die den Secure 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.

14.2.17 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 standardmäßig auskommentiert.

14.2.18 LoadModule

`LoadModule` wird in Dynamic Shared Object (DSO)-Modulen zum Laden verwendet. Weitere Informationen zur DSO-Unterstützung von Apache einschließlich der genauen Verwendung der Anweisung `LoadModule` finden Sie in Abschnitt 14.3, *Hinzufügen von Modulen zu Ihrem Server*. Beachten Sie, dass die Reihenfolge der Module wichtig ist. Sie sollten daher die Reihenfolge nicht verändern.

14.2.19 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 Ihr 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 Secure Server. <IfDefine HAVE_SSL>-Tags umschließen außerdem auch die Anweisungen LoadModule und AddModule für das ssl_module.

14.2.20 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.

14.2.21 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 14.3, *Hinzufügen von Modulen zu Ihrem Server*.

14.2.22 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 14.2.71, *Location* .

14.2.23 Port

Normalerweise definiert Port den Port, an dem der Server auf Anforderungen wartet. Ihr 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 14.2.39, *`UseCanonicalName`*.

14.2.24 `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 Codes ausführen dürfen, die zur Beantwortung von HTTP-Anforderungen vorgesehen sind.

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 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.

14.2.25 `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`.

14.2.26 `ServerAdmin`

`ServerAdmin` sollte auf die E-Mail-Adresse Ihres 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@your_domain.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 den neuen Alias hinzuzufügen.

14.2.27 `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.your_domain.com einrichten, obwohl der wirkliche Name Ihres Servers foo.your_domain.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.

14.2.28 `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 Secure Web-Server `/var/www/html`. Zum Beispiel könnte der Server eine Anforderung für folgendes Dokument empfangen:

```
http://your_domain/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 14.4, *Virtuelle Rechner verwenden* entsprechende Informationen.

14.2.29 `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 14.2.30, *`Options`*) und `AllowOverride` (siehe Abschnitt 14.2.31, *`AllowOverride`*) sehr restriktive Parameter vorgegeben. Bei dieser Konfiguration müssen für jedes Verzeichnis die Einstellungen explizit vergeben werden, wenn weniger restriktive Einstellungen erforderlich sind.

Mit Directory-Tags werden für DocumentRoot 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/my_cgi_directory>
    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 14.2.65, *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.

14.2.30 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 standardmäßig 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 serverseitige 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 <Directory "/var/www/html"> 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>
```

14.2.31 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.

14.2.32 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.

14.2.33 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.

14.2.34 Deny

`Deny` funktioniert genauso wie `allow`, wobei angegeben wird, wem der Zugriff nicht erlaubt ist. In Ihrer `DocumentRoot` sind keine `deny`-Anweisungen enthalten.

14.2.35 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://your_domain/~username/foo.html
```

Der Server sucht daraufhin die Datei:

```
/home/username/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.

14.2.36 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://*your_domain*/*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.

14.2.37 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).

14.2.38 CacheNegotiatedDocs

Standardmäßig fordert Ihr 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.

14.2.39 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.

14.2.40 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.

14.2.41 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.

14.2.42 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 14.3, *Hinzufügen von Modulen zu Ihrem Server* Hinweise zum Hinzufügen von Modulen zu Ihrem Server.

14.2.43 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. Wenn Sie `HostnameLookups` auf `double` einstellen, stellt Ihr Server einen doppelt-umgekehrten DNS aus. Mit anderen Worten: nach einem umgekehrten

Lookup wird ein Vorwärts-Lookup ausgeführt. Mindestens eine der IP-Adressen im Vorwärts-Lookup muss der Adresse des ersten umgekehrten Lookup entsprechen.

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.

14.2.44 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.

14.2.45 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 Web-Server ist auf `warn` eingestellt.

14.2.46 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.

14.2.47 CustomLog

`CustomLog` bestimmt die Protokolldatei und das Protokolldateiformat. In der Standardkonfiguration Ihres Web-Servers 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

Der Name 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.

14.2.48 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.

14.2.49 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/`.

14.2.50 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 14.2.65, *`AddHandler`* und Abschnitt 14.2.29, *`Directory`* .

14.2.51 Redirect

Wenn eine Web-Seite verschoben wird, kann mit `Redirect` die Zuordnung der alten URL auf eine neue URL erfolgen. Hier das Format:

```
Redirect /path/foo.html http://new_domain/path/foo.html
```

Wenn also eine HTTP-Anforderung für eine Seite empfangen wird, die früher unter http://*your_domain* /*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.

14.2.52 `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 14.2.30, *`Options`*), kann Ihr Web-Server eine Verzeichnisliste erstellen, wenn er eine HTTP-Anforderung wie die Folgende empfängt:

http://*your_domain*/*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.

14.2.53 `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`.

14.2.54 `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.

14.2.55 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.

14.2.56 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`.

14.2.57 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"
```

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.

14.2.58 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.

14.2.59 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.

14.2.60 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.

14.2.61 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.

14.2.62 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.

14.2.63 LanguagePriority

`LanguagePriority` ermöglicht die Einstellung, in welchen Sprachen Dateien geliefert werden sollen, falls vom Client keine Angabe zur Sprache vorliegt.

14.2.64 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.

14.2.65 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 14.2.29, *`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.

14.2.66 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.

14.2.67 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.

14.2.68 MetaSuffix

`MetaSuffix` gibt das Dateinamensuffix für die Datei an, die die Metainformationen enthält (zusätzliche HTTP-Header), die im Verzeichnis `MetaDir` abgelegt sein sollten.

14.2.69 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.

14.2.70 `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.

14.2.71 `Location`

Die Tags `<Location>` und `</Location>` ermöglichen die Angabe von Zugangsberechtigungen auf URL-Basis.

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 14.3, *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:

```
#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>
```

Weiterhin müssen Sie die folgenden Zeilen am Anfang von `httpd.conf` auskommentieren, so dass das Modul mod_put in Apache geladen werden kann:

```
#LoadModule put_module          modules/mod_put.so
#AddModule mod_put.c
```

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 .your_domain.com
#</Location>
```

Dabei muss `.your_domain.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://*your_domain*/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.

14.2.72 `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 14.3, *Hinzufügen von Modulen zu Ihrem Server*.

14.2.73 `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`.

14.2.74 Cache-Anweisungen

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.

14.2.75 `NameVirtualHost`

Wenn Sie namensbasierte virtuelle Rechner einrichten, müssen Sie die Anweisung `NameVirtual-Host` 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 Secure 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 Secure Server verwendet werden, weil der SSL-Handshake (der Zeitpunkt, wenn der Browser das Authentifizierungszertifikat des Secure 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 erfolgt. Virtuelle Rechner müssen IP-Adressen-basiert sein, um sie gemeinsam mit dem Secure Server verwenden zu können.

Wenn Sie namensbasierte virtuelle Rechner verwenden, sind für die Konfigurationsanweisung `Name-VirtualHoHallst` 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.

14.2.76 `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 14.4, *Virtuelle Rechner verwenden*.

14.2.77 `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.

14.2.78 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 außerdem unter http://www.modssl.org/docs/2.7/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/2.7/ 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 13, *Verwendung von Apache als Secure Web-Server*.

Bitte beachten

Nehmen Sie keine Veränderungen an Ihren SSL-Anweisungen vor, es sei denn, Sie wissen genau, was Sie tun. In den meisten Fällen sind die SSL-Anweisungen in der installierten Form völlig ausreichend.

14.3 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 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://*your_domain*/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 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 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 secure Web server das Modul `mime_magic_module` lädt, kommentieren Sie die folgende Zeile aus:

```
#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
```

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 14.1, *Starten und Anhalten von `httpd`* beschrieben. Nach dem Start sollten die Module in Ihren 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 13, *Verwendung von Apache als 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.

WARNUNG

Wenn Sie das Apache-Konfigurationstool, ein mit Red Hat Linux geliefertes GUI-Dienstprogramm, verwenden möchten, kompilieren Sie Ihre eigenen Module nicht in den Apache Web-Server und bearbeiten Sie auch die Konfigurationsdatei `httpd.conf` des Apache Web-Servers nicht. Wenn Sie Apache Module hinzufügen oder `httpd.conf` bearbeiten möchten, verwenden Sie dagegen nicht das Apache-Konfigurationstool.

Weitere Informationen über das Apache-Konfigurationstool finden Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*.

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 14.1, *Starten und Anhalten von `httpd`* 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.

14.3.1 Das mod_ssl-Sicherheitsmodul

Der mod_ssl-Sicherheitsteil Ihres Web-Servers 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 [userflags] --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.

14.4 Virtuelle Rechner verwenden

WARNUNG

Wenn Sie das Apache-Konfigurationstool, ein mit Red Hat Linux geliefertes GUI-Dienstprogramm, verwenden möchten, kompilieren Sie Ihre eigenen Module nicht in den Apache Web-Server und bearbeiten Sie auch die Konfigurationsdatei `httpd.conf` des Apache Web-Servers nicht. Wenn Sie Apache Module hinzufügen oder `httpd.conf` bearbeiten möchten, verwenden Sie dagegen nicht das Apache-Konfigurationstool.

Weitere Informationen über das Apache-Konfigurationstool finden Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*.

Apache bietet die Möglichkeit zur Verwendung von virtuellen Rechnern, um verschiedene Server für verschiedene IP-Adressen, verschiedene Rechnernamen oder verschiedene Ports auf demselben Rechner zu benutzen. Wenn Sie virtuelle Rechner verwenden möchten, so finden Sie detaillierte Informationen in der Apache-Dokumentation oder unter http://httpd.apache.org/docs/vhosts/.

Bitte beachten

Namensbasierte virtuelle Rechner können nicht zusammen mit dem Web-Server verwendet werden, weil der SSL-Handshake (der Zeitpunkt, wenn der Browser das Authentifizierungszertifikat des Secure 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 14.2, *Konfigurationsanweisungen in `httpd.conf`* beschrieben. Bitte lesen Sie dort nach, bevor Sie die Konfiguration der virtuellen Rechner auf Ihrem Rechner ändern.

14.4.1 Der virtuelle Rechner des Secure Web-Servers

In der Standardkonfiguration Ihres secure Web server wird ein unverschlüsselter und Secure 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 Secure Servers für unverschlüsselten Web-Datenverkehr ist daher nicht zu empfehlen.

Die Konfigurationsanweisungen für Ihren Secure Server sind innerhalb von Virtual Host-Tags in der Datei `httpd.conf` untergebracht. Wenn Sie die Konfiguration Ihres Secure Servers ändern möchten, müssen Sie die Konfigurationsanweisungen innerhalb der Virtual Host-Tags in der Datei `httpd.conf` anpassen. Wenn Sie bestimmte Funktionen für Ihren Secure Server aktivieren möchten (z.B. serverseitige Includes), müssen diese innerhalb der Virtual Host-Tags aktiviert werden, die Ihren Secure 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 Secure Server definieren, so definiert diese (offensichtlich) Ihren Secure 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.

Nachdem diese zwei Schritte ausgeführt sind, nimmt Ihr 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.

14.4.2 Einrichten von virtuellen Rechnern

Die meisten Benutzer verwenden 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 Secure 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
```

Starten Sie `httpd` neu, um einen neuen virtuellen Rechner zu starten. Weitere Informationen hierüber finden Sie unter Abschnitt 14.1, *Starten und Anhalten von `httpd`*.

Vollständigere Informationen zum Erstellen und Konfigurieren von namensbasierten 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 IV Anhang

A Allgemeine Parameter und Module

Dieser Anhang soll *einige* der möglichen Parameter erklären, die von bestimmten Treibern für bestimmte Hardware-Devices benötigt werden.[1] In den meisten Fällen sind diese zusätzlichen Parameter nicht notwendig, da der Kernel das Gerät bereits ohne sie vewenden kann. Sie sollten die in diesem Anhang beschriebenen Einstellungen nur verwenden, wenn bei der Anwendung eines bestimmten Gerätes Probleme mit Red Hat Linux auftreten, oder wenn Sie die Standardparameter für das Gerät ausser Kraft setzen möchten.

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.

Bitte beachten

Da Red Hat Linux die Installation auf vielen verschiedenen Hardware-Typen unterstützt, sind viele Treiber (einschließlich der Treiber für SCSI-Adapter, Netzwerkkarten und viele CD-ROMs) 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.

Zum Festlegen der Modulparameter während des Ladevorgangs geben Sie **`linux expert`** am `boot:` Prompt ein und legen die Treiberdiskette ein, wenn Sie vom Installationsprogramm dazu aufgefordert werden. Nachdem das Installationsprogramm die Treiberdiskette gelesen hat, werden Sie nach dem Gerätetyp gefragt, den Sie konfigurieren. In diesem Bildschirm können Sie ein Modulparameter auswählen. Dann erscheint ein Bildschirm, in den Sie die korrekten Parameter eingeben können, die auf dem Gerätetyp basieren, den Sie konfigurieren möchten.

Nach Abschluss der Installation möchten Sie möglicherweise einen neuen Kernel erstellen, der Ihre Hardware-Konfiguration unterstützt. In den meisten Fällen ist ein solcher benutzerdefinierter Kernel jedoch nicht notwendig. Im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration* finden Sie weitere Informationen über das Neuerstellen eines Kernels.

[1] Ein **Treiber** ist eine Art von Software, die Ihr System bei der Verwendung bestimmter Hardware-Devices unterstützt. Ohne den Treiber kann der Kernel das Gerät nicht korrekt verwenden.

A.1 Spezifizieren der Modulparameter

Wenn Sie Parameter für das Laden eines Moduls aufführen, können Sie diese auf zwei verschiedene Arten spezifizieren:

- Sie können einen vollständigen Satz von Parametern mit einer Anweisung spezifizieren. Zum Beispiel kann der Parameter `cdu31=0x340,0` mit einem Sony CDU 31 oder 33 an Port 340 kein IRQ verwendet werden.
- Sie können die Parameter individuell spezifizieren. Diese Methode wird benutzt, wenn ein oder mehrere Parameter aus dem ersten Satz nicht benötigt werden. Zum Beispiel kann `cdu31=0x340,0` als Parameter für die gleiche CD-ROM verwendet werden, die als Beispiel für die erste Methode verwendet wurde. Ein *OK* in den CD-ROM-, SCSI- und Ethernettabellen zu diesem Anhang zeigt an, wo die erste Methode endet und die zweite beginnt.

Bitte beachten

Verwenden Sie nur eine der beiden Methoden zum Laden eines Moduls mit bestimmten Parametern.

Wenn ein Parameter über Kommas verfügt, achten Sie darauf, nach einem Komma *keinen* Punkt zu setzen.

A.2 CD-ROM Modulparameter

Bitte beachten

Nicht alle aufgeführten CD-ROM-Treiber werden unterstützt. Prüfen Sie bitte die Hardware-Kompatibilitätsliste aus der Website http://hardware.redhat.com, um sich zu vergewissern, dass Ihr CD-ROM-Treiber unterstützt wird.

Selbst wenn die Parameter nach dem Laden der Treiberdiskette spezifiziert sind und das Gerät angegeben wurde, *kann* der am häufigsten verwendete Parameter (`hdX =cdrom`) während der Installation

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		hd*X*=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 CD-ROM	`cdu31a.o`	cdu31a=*io_port,IRQ ODER* 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-Interface (OPTi 82C928 und OPTi 82C929) mit Sanyo/Panasonic, Sony, oder Mitsumi-Laufwerken	`isp16.o`	isp16=*io_port,IRQ,dma, drive_type ODER* 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*
Optics storage 8000 AT "Dolphin"-Laufwerk, Lasermate CR328A	`optcd.o`	

Hardware	Modul	Parameter
Parallel-Port IDE CD-ROM	`pcd.o`	
SB Pro 16-kompatibel	`sbpcd.o`	sbpcd=*io_port*
Sanyo CDR-H94A	`sjcd.o`	sjcd=*io_port ODER* sjcd_base=*io_port*
Sony CDU-535 & 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 zweiten 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 *ODER* cdu31_port=0x340 cdu31a_irq=0
Aztech CD-ROM at port 220	aztcd=0x220
Panasonic CD-ROM an einem SoundBlaster-Interface an Port 230	sbpcd=0x230,1
Phillips/LMS cm206 und cm260 an E/A 340 und IRQ 11	cm206=0x340,11
Goldstar R420 an IO 300	gscd=0x300
Mitsumi-Laufwerk an einer MAD16-Soundkarte an E/A Addr 330 und IRQ 1, DMA-Erkennung	isp16=0x330,11,0,Mitsumi
Sony CDU 531 an E/A-Adresse 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 `hd`*X* Parameter.

A.3 SCSI-Parameter

Tabelle A–3 SCSI-Parameter

Hardware	Modul	Parameter
3ware Storage Controller	`3w-xxxx.o`	
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
AM53/79C974 (PC-SCSI) Treiber	`AM53C974.o`	
Die meisten Buslogic- (jetzt Mylex-) Karten mit "BT"-Teilenummer	`BusLogic.o`	BusLogic_Options=*option,option,…*
Mylex DAC960 RAID Controller	`DAC960.o`	
MCR53c406a-based SCSI	`NCR53c406a.o`	
Initio INI-9100UW	`a100u2w.o`	a100u2w=*io,IRQ,scsi_id*
Adaptec AACRAID	`aacraid.o`	
Advansys SCSI-Karten	`advansys.o`	
Adaptec AHA-152x	`aha152x.o`	aha152x=*io,IRQ,scsi_id*
Adaptec AHA 154x amd 631x-based	`aha1542.o`	
Adaptec AHA 1740	`aha1740.o`	

Hardware	Modul	Parameter
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*
ACARD ATP870U PCI SCSI Controller	`atp870u.o`	
Compaq Smart Array 5300 Controller	`cciss.o`	
Compaq Smart/2 RAID Controller	`cpqarray.o`	
Compaq FibreChannel Controller	`cpqfc.o`	
Domex DMX3191D	`dmx3191d.o`	
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 ODER* eata io_port=*port0,port1,port2,…* option=*value*
DTP SCSI Adapters 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`	
Sun Enterprise Network Array (FC-AL)	`fcal.o`	
Future Domain TMC-16*xx* SCSI	`fdomain.o`	
NCR5380 (generic driver)	`g_NCR5380.o`	
ICP RAID Controller	`gdth.o`	
I2O Block-Treiber	`i2o_block.o`	
IOMEGA MatchMaker SCSI-Adapter für Parallelport	`imm.o`	
Always IN2000 ISA SCSI Karte	`in2000.o`	in2000=*setup_string*:*value* *ODER* in2000 *setup_string=value*
Initio INI-9X00U/UW SCSI-Host-Adapter	`initio.o`	
IBM ServeRAID	`ips.o`	
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	

Hardware	Modul	Parameter
NCR SCSI-Controller mit den Chipsätzen 810/810A/815/ 825/825A/860/875/876/895	`ncr53c8xx.o`	ncr53c8xx=*option1*:*value1*,*option2*:*value2*,… *ODER* ncr53c8xx="*option1*:*value1 option2*:*value2*…"
Pro Audio Spectrum/Studio 16	`pas16.o`	
PCI-2000 IntelliCache	`pci2000.o`	
PCI-2220I EIDE RAID	`pci2220i.o`	
SparcSTORAGE Array	`pluto.o`	
IOMEGA PPA3 SCSI-Host-Adapter für Parallelport	`ppa.o`	
Perceptive Solutions PSI-240I EIDE	`psi240i.o`	
Qlogic 1280	`qla1280.o`	
Qlogic 2*x*00	`qla2x00.o`	
QLogic Fast SCSI FASXXX ISA/VLB/PCMCIA	`qlogicfas.o`	
QLogic ISP2100 SCSI-FCP	`qlogicfc.o`	
QLogic ISP1020 Intelligent SCSI cards IQ-PCI, IQ-PCI-10, IQ-PCI-D	`qlogicisp.o`	
Qlogic ISP1020 SCSI SBUS	`qlogicpti.o`	
Seagate ST-01/02, Future Domain TMC-8*xx*	`seagate.o`	
Future Domain TMC-885, TMC-950	`seagate.o`	controller_type=2 base_address=*base_addr* irq=*IRQ*
Karten mit dem sym53c416-Chipsatz	`sym53c416.o`	sym53c416=*PORTBASE,[IRQ] ODER* sym53c416 io=*PORTBASE* irq=*IRQ*

Hardware	Modul	Parameter
Trantor T128/T128F/T228 SCSI-Host-Adapter	`t128.o`	
Tekram DC-390(T) PCI	`tmscsim.o`	
UltraStor 14F/34F (nicht 24F)	`u14-34f.o`	
UltraStor 14F, 24F, und 34F	`ultrastor.o`	
WD7000 Series	`wd7000.o`	

Es folgen einige Beispiele, wie diese Module verwendet werden:

Tabelle A–4 Konfigurationsbeispiele für SCSI-Parameter

Konfiguration	Beispiele
Adaptec AHA1522 at port 330, IRQ 11, SCSI ID 7	aha152x=0x330,11,7
Adaptec AHA1542 at port 330	bases=0x330
Future Domain TMC-800 at CA000, IRQ 10	controller_type=2 base_address=0xca000 irq=10

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 ODER* 3c503 io=*io_port_1,io_port_n* irq=*IRQ_1,IRQ_n*
3Com EtherLink Plus (3c505)	`3c505.o`	3c505=*io_port,IRQ ODER* 3c505 io=*io_port_1,io_port_n* irq=*IRQ_1,IRQ_2*
3Com EtherLink 16	`3c507.o`	3c507=*io_port,IRQ ODER* 3c507 io=*io_port* irq=*IRQ*
3Com EtherLink III	`3c509.o`	3c509=*IRQ*

Hardware	Modul	Parameter
3Com ISA EtherLink XL "Corkscrew"	`3c515.o`	
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	
RTL8139, SMC EZ Card Fast Ethernet	`8139too.o`	
Apricot 82596	`82596.o`	
Ansel Communications Model 3200	`ac3200.o`	ac3200=*io_port,IRQ ODER* ac3200 io=*io_port_1,io_port_n* irq=*IRQ_1,IRQ_n*
Alteon AceNIC Gigabit	`acenic.o`	
Aironet Arlan 655	`arlan.o`	
Aironet 4500 PCI-ASI-i365 wireless	`aironet4500_card.o`	
Allied Telesis AT1700	`at1700.o`	at1700=*io_port,IRQ ODER* 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 ODER* cops io=*io_port* irq=*IRQ*
Modularer Treiber für dei synchrone serielle COSA oder SRP-Karte	`cosa.o`	cosa=*io_port,IRQ,dma*
Crystal Semiconduc-torCS89[02]0	`cs89x0.o`	

Hardware	Modul	Parameter
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 cards with DC21040 (no SROM), DC21041[A], DC21140[A], DC21142, DC21143 chipsets	`de4x5.o`	de4x5=*io_port ODER* de4x5 io=*io_port* de4x5 args='eth*X[fdx]* autosense=*MEDIA_STRING*'
D-Link DE-600 Ethernet Pocket Adapter	`de600.o`	
D-Link DE-620 Ethernet Pocket Adapter	`de620.o`	
DIGITAL DEPCA & EtherWORKS DEPCA, DE100, DE101, DE200 Turbo, DE201Turbo DE202 Turbo TP/BNC, DE210, DE422 EISA	`depca.o`	depca=*io_port,IRQ ODER* depca io=*io_port* irq=*IRQ*
Digi Intl. RightSwitch SE-X EISA und PCI	`dgrs.o`	
Davicom DM9102(A)/DM9132/ DM9801 Fast Ethernet	`dmfe.o`	
Intel EtherExpress/1000 Gigabit	`e1000.o`	
Cabletron E2100	`e2100.o`	e2100=*io_port,IRQ,mem ODER* e2100 io=*io_port* irq=*IRQ* mem=*mem*

Hardware	Modul	Parameter
Intel EtherExpress Pro10	`eepro.o`	eepro=*io_port,IRQ ODER* eepro io=*io_port* irq=*IRQ*
Intel i82557/i82558 PCI EtherExpressPro Treiber	`eepro100.o`	
Intel EtherExpress 16 (i82586)	`eexpress.o`	eexpress=*io_port,IRQ ODER* eexpress io=*io_port* irq=*IRQ*
SMC EtherPower II 9432 PCI (83c170/175 EPIC series)	`epic100.o`	
Racal-Interlan ES3210 EISA	`es3210.o`	
ICL EtherTeam 16i/32 EISA	`eth16i.o`	eth16i=*io_port,IRQ ODER* eth16i ioaddr=*io_port* IRQ=*IRQ*
EtherWORKS 3 (DE203, DE204 und DE205)	`ewrk3.o`	ewrk=*io_port,IRQ ODER* ewrk io=*io_port* irq=*IRQ*
Fujitsu FMV-181/182/183/184	`fmv18x.o`	fmv18x=*io_port,IRQ ODER* fmv18x io=*io_port* irq=*IRQ*
Packet Engines GNIC-II Gigabit	`hamachi.o`	
Modularer Treiber für den Comtrol Hostess SV11	`hostess_sv11.o`	hostess_sv11=*io_port,IRQ, DMABIT ODER* hostess_sv11 io=*io_port* irq=*IRQ* dma=*DMABIT*
HP PCLAN/plus	`hp-plus.o`	hp-plus=*io_port,IRQ ODER* hp-plus io=*io_port* irq=*IRQ*
HP LAN Ethernet	`hp.o`	hp=*io_port,IRQ ODER* hp io=*io_port* irq=*IRQ*

Hardware	Modul	Parameter
100VG-AnyLan Network Adapters HP J2585B, J2585A, J2970, J2973, J2573 Compex ReadyLink ENET100-VG4, FreedomLine 100/VG	`hp100.o`	hp100=*io_port,name ODER* hp100 hp100_port=*io_port* hp100_name=*name*
IBM Token Ring 16/4	`ibmtr.o`	ibmtr=*io_port,IRQ,mem ODER* ibmtr io=*io_port* irq=*IRQ* mem=*mem*
AT1500, HP J2405A, most NE2100/clone	`lance.o`	
Mylex LNE390 EISA	`lne390.o`	
	`ltpc.o`	ltpc=*io_port,IRQ ODER* ltpc io=*io_port* irq=*IRQ*
MyriCOM MyriNET SBUS	`myri_sbus.o`	
NatSemi DP83815 Fast Ethernet	`natsemi.o`	
NE1000 / NE2000 (non-pci)	`ne.o`	ne=*io_port,IRQ ODER* 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	`ne3210.o`	
MiCom-Interlan NI5010	`ni5010.o`	
NI5210 card (i82586 Ethernet chip)	`ni52.o`	ni52=*io_port,IRQ ODER* ni52 io=*io_port* irq=*IRQ*
NI6510 Ethernet	`ni65.o`	

Hardware	Modul	Parameter
Older DEC 21040, meistens 21*40 Ethernet	`old_tulip.o`	old_tulip=*io_port ODER* old_tulip io=*io_port*
AMD PCnet32 und AMD PCnetPCI	`pcnet32.o`	
RedCreek Communications PCI	`rcpci.o`	
RealTek-Karten mmit dem Chipsatz RTL8129 oder RTL8139 Fast Ethernet	`rtl8139.o`	
Sangoma S502/S508 Multi-Protocol FR	`sdla.o`	
Sangoma S502A, ES502A, S502E, S503, S507, S508, S509	`sdladrv.o`	
SysKonnect SK-98*XX* Gigabit	`sk98lin.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 ODER* sktr io=*io_port* irq=*IRQ* mem=*mem*
SMC Ultra und SMC EtherEZ ISA ethercard (8K, 83c790)	`smc-ultra.o`	smc-ultra=*io_port,IRQ ODER* 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 ODER* smc9194 io=*io_port* irq=*IRQ* ifport=*[0,1,2]*
Sun BigMac Ethernet	`sunbmac.o`	
Sundance ST201 Alta	`sundance.o`	

Hardware	Modul	Parameter
Sun Happy Meal Ethernet	`sunhme.o`	
Sun Quad Ethernet	`sunqe.o`	
ThunderLAN	`tlan.o`	
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`	
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 (für NCR) WaveLan ISA-Karte	`wavelan.o`	wavelan=*[IRQ,0],io_port,NWID*
WD8003 und WD8013-kompatible Ethernet-Karten	`wd.o`	wd=*io_port,IRQ,mem, mem_end ODER* wd io=*io_port* irq=*IRQ* mem=*mem* mem_end=*end*
Compex RL100ATX-PCI	`winbond.o`	
Packet Engines Yellowfin	`yellowfin.o`	
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 Adresse 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 im *Offiziellen Red Hat Linux Handbuch Benutzer-definierte Konfiguration*.

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).

Weitere Informationen über die Verwendung mehrerer Ethernt- Karten finden Sie im *Linux Ethernet-HOWTO* unter http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

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.

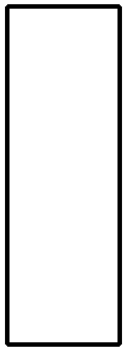
Wenn Sie mit Festplattenpartitionen bereits vertraut sind, fahren Sie fort mit Abschnitt B.1.4, *Verfügbarmachen von Festplattenspeicher für Red Hat Linux*. Hier erfahren Sie, wie Sie als Vorbereitung für eine Red Hat Linux Installation Festplattenspeicher freigeben. In diesem Abschnitt werden auch verwandte 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

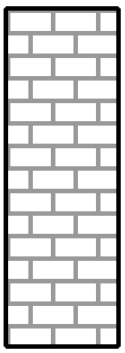


Es ist nicht gerade viel zu sehen, aber für eine einfache Erklärung von Festplatten reicht es aus. Angenommen, wir möchten Daten auf diesem Laufwerk speichern. So wie die Festplatte im Moment aussieht, kann das nicht funktionieren. Wir müssen zuerst noch etwas tun…

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]

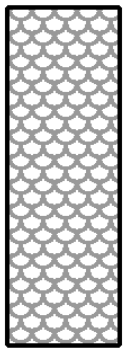
In Anbetracht der Tatsache, dass Dateisysteme Verzeichnisse und Dateien erst möglich machen, fallen diese kleinen Abweichungen nicht allzu sehr ins Gewicht.

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 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

[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.

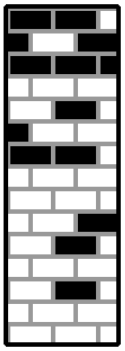
Hat Linux unterstützt z.B. eine Vielzahl von Dateisystemen (darunter viele Dateisysteme anderer Betriebssysteme). Das erleichtert den Datenaustausch.

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

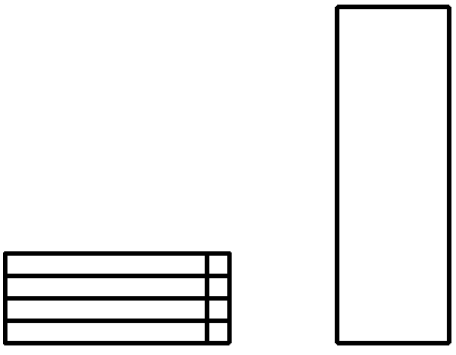
noch für mehr Unordnung sorgte. Rein technisch gesehen waren manche Dateisysteme für die Unterstützung größerer Festplatten einfach nicht ausgelegt. Manche Dateisysteme *unterstützten* zwar größere Festplatten, aber ein übermäßiger Verwaltungsaufwand war die Folge.

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. Der "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.

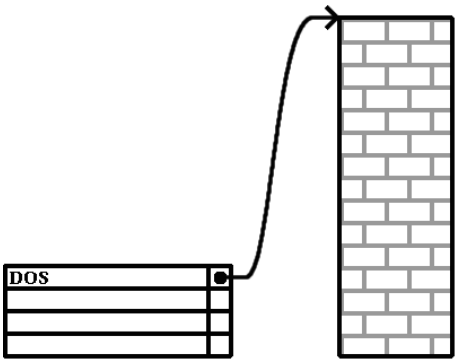
Tabelle B–1 Partitionstypen

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 <=32M	04	Linux swap	82
Extended	05	Linux native	83
DOS 16-bit >=32	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

Partitionstyp	Wert	Partitionstyp	Wert
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
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.

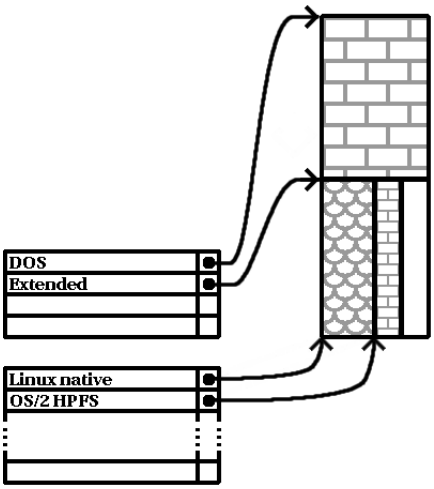
B.1.3 Partitionen innerhalb von Partitionen – Ein Überblick über erweiterte Partitionen

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 Reihr nach an.

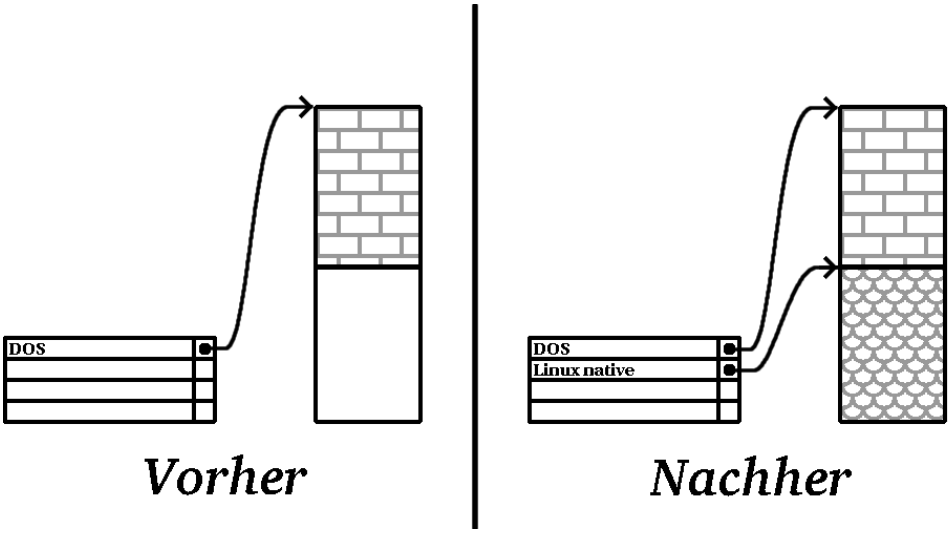
Bitte beachten

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.

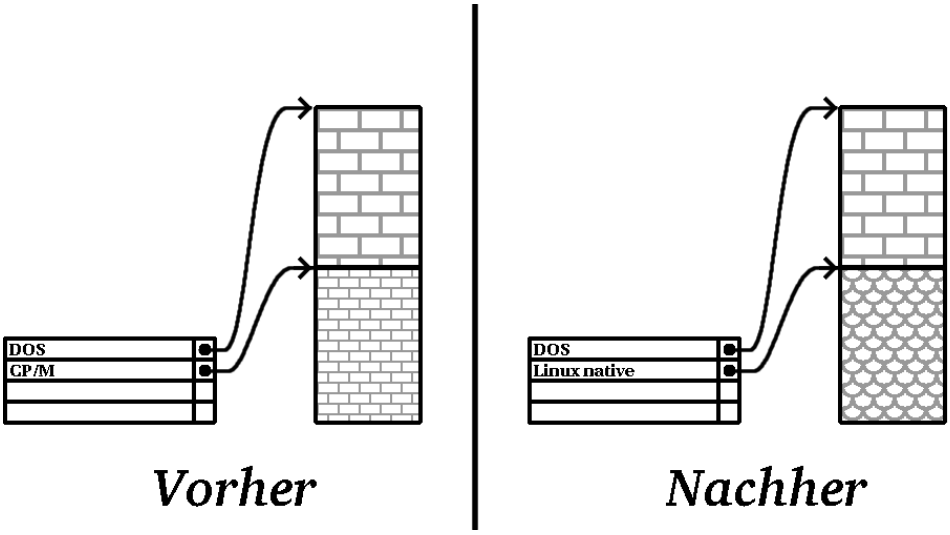
Auf jeden Fall können Sie einfach die notwendigen Partitionen auf dem unbenutzten Festplattenspeicher erstellen. Leider ist es sehr unwahrscheinlich, dass Sie dieses sehr einfache Szenario vorfinden (es sei denn, Sie haben extra für Red Hat Linux eine neue Festplatte gekauft). Die meisten vorinstallierten Betriebssysteme sind so konfiguriert, dass sie den gesamtem Festplattenspeicher beanspruchen (siehe *Freier Festplattenspeicher auf einer aktiven Partition* in Abschnitt B.1.4.

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:

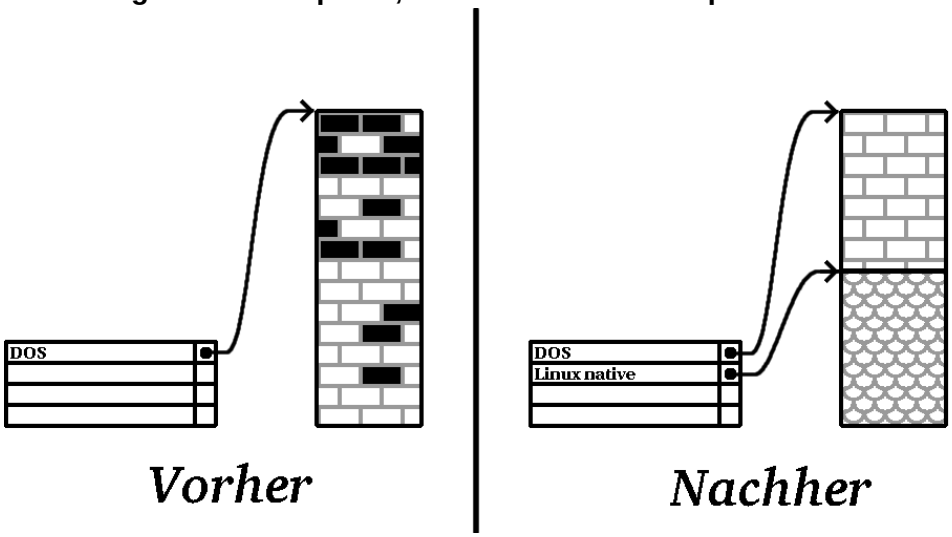
Neupartitionieren mit Datenverlust

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. Bedenken Sie, dass bei einigen Computern mit vorinstallierten Betriebssystemen keine CD-ROM Medien für das erneute Installieren des originalen Betriebssystems vorhanden sind. Sie sollten feststellen, ob das für Ihr System zutrifft, *bevor* Sie Ihre Originalpartition und das entsprechende Betriebssystem zerstören.

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



VORSICHT

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

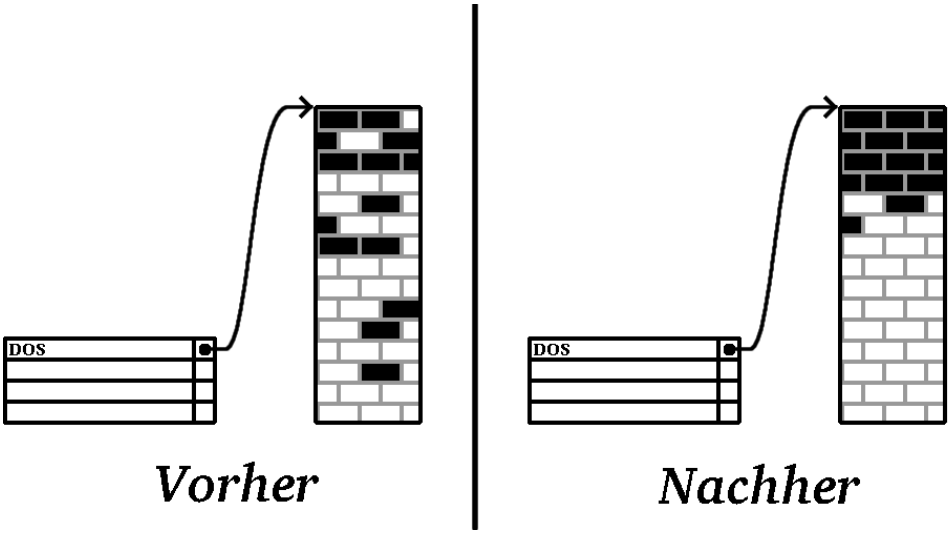
- Erstellen neuer Partition(en)

Betrachten wir die einzelnen Schritte einmal näher.

Komprimieren vorhandener Dateien

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

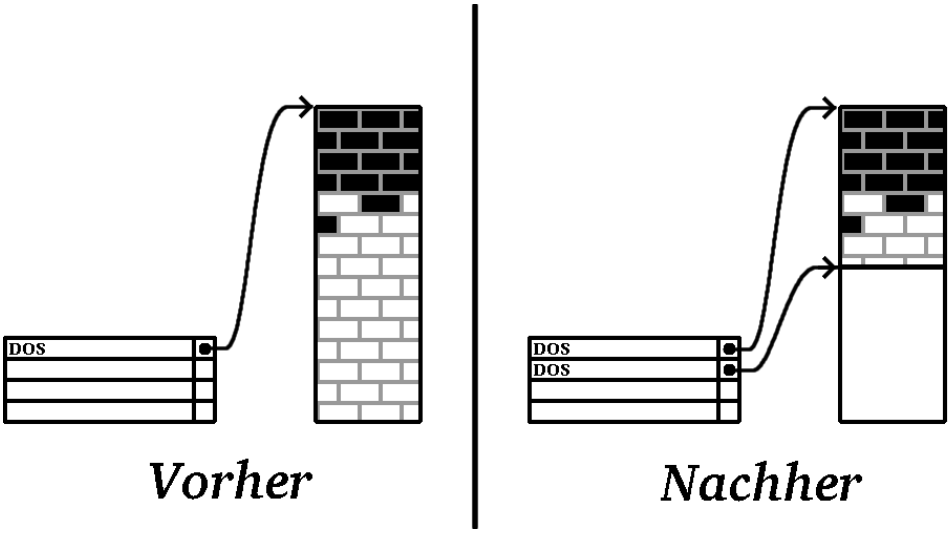


Dieser Schritt ist entscheidend. Wenn er ausgelassen wird, kann die Position der Daten verhindern, dass die Partition auf die gewünschte Größe gebracht werden kann. Beachten Sie auch, dass, aus welchen Gründen auch immer, manche Daten nicht verschoben werden können. Wenn dies der Fall ist (und dadurch 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

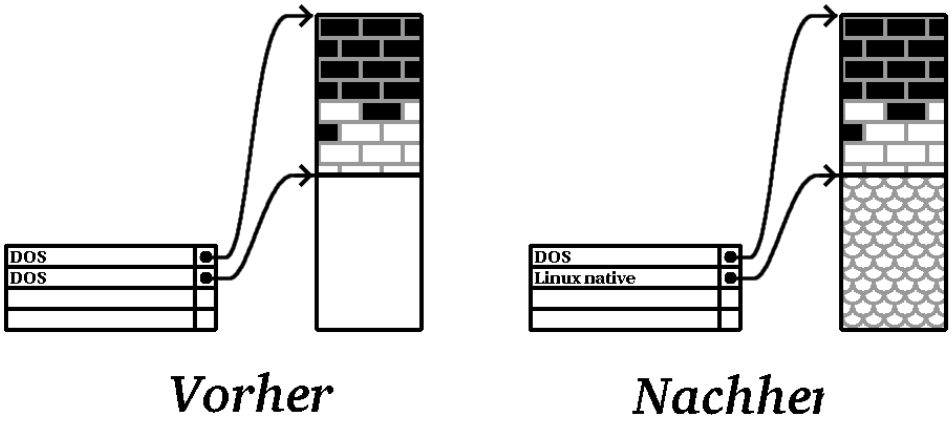


Wichtig ist, dass Sie verstehen, was die Größenänderungs-Software mit dem freigegebenen Platz macht, damit Sie die geeigneten Schritte durchführen können. In dem dargestellten Fall wäre es das Beste, die neue DOS-Partition zu löschen und (eine) geeignete Linux-Partition(en) zu erstellen.

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



Bitte beachten

Die folgenden Informationen gelten nur für Intel-basierte Computer.

Um Red Hat Linux Kunden die Arbeit zu erleichtern, bieten wir das DOS-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/x86 CD-ROM im Verzeichnis `dosutils` .

WARNUNG

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/x86 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 füe 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.

Note

Wenn Red Hat Linux/x86 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` physisch 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 32 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 32 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.

  Lesen Sie bitte Abschnitt B.1.9, *Verwenden von LILO* — Die dort angegebenen Informationen gelten für die `/boot`-Partition!

  Wegen der Einschränkungen der meisten PC-BIOS-Versionen sollten Sie zur Aufnahme dieser Dateien nur eine kleine Partition erstellen. Sie sollte nicht größer als 32 MB sein.
- *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 1.2 GB erlaubt den Umfang einer Workstation-Installation (mit *sehr* wenig freiem Festplattenspeicher), während Sie in einer Root-Partition von 2.4 GB alle Pakete installieren können. Selbstverständlich ist es besser, der Root-Partition den größtmöglichen Platz zur Verfügung zu stellen.

Im *Offiziellen Red Hat Linux Installationshandbuch* erhalten Sie Angaben darüber, wielviel Platz Sie den verschienden Partitionen einräumen müssen.

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 des Zylinders 1023 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

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 Support 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 Treiberdiskete wird nur dann benötigt, wenn Sie für die Installation von Red Hat Linux ein spezielles Gerät benötigen. Im Allgemeinen handelt es sich dabei um Treiberdisketten für nicht standardisierte oder sehr neue CD-ROM-Laufwerke, SCSI-Adapter oder NICs. Das sind die einzigen Geräte, die bei der Installation eine Treiberdiskette benötigen, da die benötigten Treiber nicht auf den Red Hat Linux CD-ROMs enthalten sind (oder Floppy-Disk, wenn Sie eine Boot-Floppy erstellen, um die Installation zu starten).

Bitte beachten

Wenn für die nstallation von Red Hat Linux kein nichtunterstütztes Gerät benötigt wird, fahren Sie mit der normalen Installation fort und fügen Sie dann den Support für das neue Gerät im Anschluss an die Installation hinzu.

C.1.2 Wie sind Treiberdisketten erhältlich?

Die Red Hat Linux CD-ROM 1 enthält ein Treiberdisketten-Image (`images/drivers.img`) das viele selten verwendete Treiber enthält. Wenn Sie feststellen, dass Ihr System einen dieser Treiber benötigt, können Sie fortfahren und die Floppy-Treiberdiskette erstellen, bevor die Installation von Red Hat Linux beginnt.

Eine weitere Möglichkeit, Informationen über spezielle Treiberdisketten zu erhalten, bietet die Red Hat Linux Website: http://www.redhat.com/ support/errata im Abschnitt **Bug Fixes**. Gelegentlich wird aufgrund einer Version von Red Hat Linux sehr bekannte Hardware zur Verfügung, die nicht mit Treibern im Installationsprogramm arbeitet oder auf dem Treiberdisketten-Image der Red Hat Linux CD-ROM enthalten ist. Die Red Hat Linux Website könnte ein Link für ein Treiberdisketten-Image enthalten, das Sie zum Installieren von Red Hat Linux auf dieser Hardware verwenden können.

Erstellen einer Treiberdiskette von einer Image-Datei

Wenn Sie ein Treiberdisketten-Image haben, das auf eine Floppy- Disk geschrieben werden muss, kann dies innerhalb von DOS oder Red Hat Linux durchgeführt werden.

Erstellen einer Treiberdiskette von einem Treiberdisketten-Image, mit Red Hat Linux:

1. Legen Sie eine leere, formatierte Floppy-Diak in das erste Diskettenlaufwerk ein.
2. Geben Sie `cat`*`dd.img`* `> /dev/fd0` als Root in das Verzeichnis (z.B *`dd.img`*) ein, das das Treiberdisketten-Image enthält.

Erstellen einer Treiberdiskette von einem Treiberdisketten-Image, mit DOS:

1. Legen Sie eine leere, formatierte Floppy-Disk in das Laufwerk a ein.
2. Geben Sie `rawrite`*`dd.img`* `a:` in die Befehlszeile des Verzeichnisses (z.B *`dd.img`*) ein, das das Treiberdisketten-Image enthält.

C.1.3 Verwenden einer Treiberdiskette während der Installation

Die Treiberdiskette nur zu haben, reicht nicht. Sie müssen dem Red Hat Linux Installationsprogramm mitteilen, dass es die Treiberdiskette laden und während des Installationsprozesses verwenden soll.

Bitte beachten

Eine Treiberdiskette unterscheidet sich von einer Bootdiskette. Wenn Sie eine Boot-Floppy verwenden, um die Red Hat Linux Installation in Ihrem System zu starten, müssen Sie diese Floppy erstellen, von der Sie dann booten, bevor Sie Ihre Treiberdiskette verwenden.

Wenn Sie keine Installations-Floppy-Disk haben und Ihr System das Booten von der CD-ROM unterstützt, erstellen Sie unter Verwendung des korrekten *Dateinamen* `.img` eine Bootdiskette (z.B. `boot.img`) im Verzeichnis `Images` der Red Hat Linux CD-RROM 1. Anweisungen für die Erstellung einer Bootdiskette finden Sie im *Offiziellen Red Hat Linux Installationshandbuch* im Abschnitt *Installationsdisketten erstellen*.

Sobald Sie Ihre Treiberdiskette erstellt haben, können Sie den Installationsprozess mit der Red Hat Linux CD-ROM 1 (oder der Installations- Boot-Floppy, die Sie erstellt haben, weil Sie aus irgendeinem Grund nicht von der CD-ROM aus booten konnten) starten. Geben Sie dann am `boot:` Prompt entweder **`linux expert`** oder **`linux dd`** ein.

Das Red Hat Linux Installationsprogramm wird Sie auffordern, die Treiberdiskette einzulegen. Sobald die Treiberdiskette vom Installer gelesen wurde, können anschließend diese Treiber auf der Hardware angewendet werden, die in Ihrem System gefunden wurde.

D RAID (Redundant Array of Independent Disks)

D.1 Was verbirgt sich hinter RAID?

Das grundlegende Konzept 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 einzigen großen und teuren Festplatte. Diese Festplattengruppe wird durch den Computer wie eine einzige logische Speichereinheit oder Festplatte angesprochen.

Bei dieser Methode werden Daten unter Verwendung von Techniken wie **disk striping** (RAID Level 0), **disk mirroring** (Raid Level 1), und **disk striping with parity** (RAID Level 5) auf mehrere Festplatten 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 einheitlich auf jedes Laufwerk innerhalb der Laufwerkgruppe auf 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.

D.1.1 Wer sollte Raid verwenden?

Wer mit großen Datenmengen umgeht (z.B. ein Administrator), kann von der RAID-Technologie profitieren. Zu den Hauptgründen für die Verwendung von RAID gehören:

- höhere Geschwindigkeit
- größere Speicherkapazität
- höhere Effizienz beim Wiederherstellen von Daten nach einem Festplattenausfall

D.1.2 RAID: Hardware oder Software

Es gibt zwei mögliche Ansätze für RAID: Hardware-RAID und Software-RAID.

Hardware-RAID

Das hardwarebasierte 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 ist 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-Level im Kernel-Disk-(Blockgeräte-) Code implementiert. Dieser Ansatz ist die preiswerteste Lösung: Es werden keine teuren Festplattencontroller oder Hot-Swap-Chassis [1]benötigt und Software-RAID funktioniert mit günstigeren 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 softwarebasierten Arrays ist sehr stark abhängig von Leistung und Auslastung der Server-CPU.

Für weitere Informationen über Software RAID im Red Hat Linux Installationsprogramm lesen Sie das *Offizielle Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*.

Für alle, die sich für Software-RAID interessieren, geben wir hier eine kurze Liste einiger Funktionsmerkmale an:

- Wiederherstellungsprozess mit Threads
- Vollständig kernelbasierte Konfiguration
- Portabilität von Arrays zwischen Linux-Rechnern ohne Reorganisation
- Reorganisation von Arrays im Hintergrund unter Verwendung ungenutzter Systemressourcen
- Unterstützung von hotswapfähigen Laufwerken
- Automatische CPU-Erkennung zur vollen Ausnutzung bestimmter CPU-Ausnutzungen

[1] Ein Hot-Swap-Chassis ermöglicht es, ein Festplattenlaufwerk zu entfernen, ohne das System ausschalten zu müssen

D.1.3 RAID Level and linearer Support

RAID bietet außerdem die Level 0, 1, 4, 5 und linearen Support. 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 einen parallelen Zugriff für hohe Datenübertragungsgeschwindigkeiten zum Lesen bieten, 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]Die Speicherkapazität des Level 1 Arrays entspricht der Kapazität einer einzelnen Festplatte im Hardware RAID oder einer der gespiegelten Partitionen in einem Software-RAID.
- *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 größerer 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 Speicherkapazität des Hardware-RAID Level 4 entspricht der Kapazität der Festplatten abzüglich der Größe einer der zugehörigen Festplatten. Die Speicherkapazität des Hardware-RAID Level 4 entspricht der Kapazität der Partitionen abzüglich der Größe einer der zugehörigen Partitionen, wenn sie gleich groß sind.

[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 40 GB-Festplatten verteilt ist, sind insgesamt 80 GB im Einsatz, wobei Sie aber nur auf 40 GB dieser 80 GB zugreifen können. Die weiteren 40 GB werden als eine Art Spiegel der ersten 40 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 den gleichen 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.

- *Level 5* — Das ist der am meisten 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 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 PowerTools

E.1 Was sind PowerTools?

PowerTools sind eine Sammlung von Software-Paketen, die für das Betriebssystem Red Hat Linux 7.1 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.

Sind sie ein Systemadministrator? Die PowerTools enthalten eine große Auswahl an Tools, die Ihnen die Dinge erleichtern und auch verschiedene teure Programme durch eine gemeinsame Anwendung ersetzen. Beispiele hierfür sind Anwendungen wie Ethereal für die Analyse der Netzwerkprotokolle, Ethereal um das Lesen der Ports auf dem Netzwerk zu verhindern, oder Postfix als Alternative zu Sendmail.

Spielen Sie gerne? PowerTools enthält zahlreiche amüsante, einfache Spiele wie SpeedX, XFrisk und Amphetamine.

Da das Installieren und Deinstallieren von Software-Paketen auf Red Hat Linux dank Anwendungen wie RPM oder Gnome-RPM sehr einfach ist, können Sie diverse gleiche Anwendungen ausprobieren, bevor Sie die wählen, die Sie für die geeignetste halten.

E.2 PowerTools-Pakete

Wenn Sie schon wissen, welche PowerTools-Pakete Sie installieren wollen, lesen Sie unter Abschnitt E.3, *Das Installieren von PowerTools-Paketen* die Informationen zur Installation.

Dennoch ist es aufgrund der zahlreichen erhältlichen PowerTools-Paketen hilfreich, die Beschreibungen durchzulesen, um zu verstehen, welche die für Sie am besten geeigneten sind.

E.2.1 Lesen des Inhalts der CD-ROM

Den Inhalt einer PowerTools CD können Sie von einem Shell Prompt aus lesen (sowohl in einem Terminalfenster als auch im Konsolenmodus). Zuerst müssen Sie das CD-ROM Laufwerk mounten.

Mounten der PowerTools CD-ROM

Wenn Ihr System nicht so eingestellt ist, dass es automatisch das CD-ROM-Laufwerk mounted, wenn Sie eine CD einlegen, dann legen Sie die PowerTools CD in Ihr CD-ROM-Laufwerk. Geben Sie als Root Folgendes an:

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

Bitte beachten

Vielleicht räumt der Systemadministrator bereits allen Benutzern (nicht nur den Root-Benutzern) die Möglichkeit ein, das CD-ROM-Laufwerk zu mounten. Benutzer haben diese Berechtigung, wenn die Option `user` in der Zeile `/dev/cdrom` in der Datei `etc/fstab` inbegriffen ist. Beachten Sie jedoch, dass Sie als Root angemeldet sein müssen, um PowerTools RPMs installieren zu können.

Die Datei `CONTENTS` lesen

Nachdem Sie das Laufwerk gemountet haben, wechseln Sie das Verzeichnis mithilfe des folgenden Befehls:

```
cd /mnt/cdrom
```

Geben Sie zuletzt `less CONTENTS` ein, um die verfügbaren Anwendungen anzuzeigen. Die Datei `CONTENTS` enthält jedes Programm der PowerTools CD-ROM in alphabetischer Reihenfolge.

Angesichts der großen Anzahl an verfügbaren Anwendungen kann es anstrengend sein, die Datei `CONTENTS` auf der PowerTools CD-ROM zu lesen. Hierzu einige Tricks, wie Sie ein besonderes Programm finden können, ohne alle Beschreibungen lesen zu müssen.

- *Benutzen Sie die Gruppennamen* — Jede Anwendung gehört zu einer besonderen Gruppe. Zum Beispiel befindet sich FaxMail, ein Dienstprogramm für das Verschicken von Faxmitteilungen, in der Gruppe Applications/Communication, und Icecast, ein MP3 Internet Broadcasting System, gehört zur Gruppe Applications/Multimedia. Indem Sie bereits unter den Gruppennamen wählen, brauchen Sie nicht die Beschreibung jedes Paketes zu lesen.
- *Suchen Sie mit Hilfe von Schlüsselworten* — Der Befehl `ls` vereinfacht die Suche. Wenn Sie einen IRC-Client suchen, geben Sie `less CONTENTS` ein, um `CONTENTS` zu finden. Geben Sie dann **`/IRC`** ein, und drücken Sie die [Eingabetaste]. Der erste IRC-Client auf der Liste wird erscheinen. Wenn Sie nicht an diesem interessiert sind, wählen Sie wiederholt [n], bis Sie das Paket finden, das Sie interessiert.

Wenn Sie Schwierigkeiten mit dem Befehl `less` command haben, wählen Sie `man less`, um Hilfe aufzurufen.

Unmounten der PowerTools CD-ROM

Wenn Sie die Installation Ihrer Pakete mit der PowerTools CD abgeschlossen haben, können Sie die CD aus dem Laufwerk nehmen. Wenn Sie die CD-ROM im Verzeichnis `/mnt/cdrom` gespeichert haben, tun Sie Folgendes:

1. Wechseln Sie mit dem Befehl `cd /mnt` solange die Verzeichnisse, bis Sie sich eine Stufe über dem Verzeichnis `/mnt/cdrom` befinden.
2. Geben Sie `umount /mnt/cdrom` ein, um die CD-ROM zu unmounten.
3. Geben Sie `eject /dev/cdrom` ein, um das CD-ROM-Laufwerk zu öffnen, damit Sie die CD-ROM entnehmen können.

E.3 Das Installieren von PowerTools-Paketen

E.3.1 Das Installieren von PowerTools unter einer graphischen 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-Programm automatisch (je nach GUI-Umgebung) und kann zum Installieren der PowerTools verwendet werden.

Genaue Anweisungen zur Verwendung von Gnome-RPM finden Sie im *Offiziellen Red Hat Linux Handbuch Erste Schritte*. Für Anweisungen zur Verwendung von Kpackage wenden Sie sich an die Adresse http://www.general.uwa.edu.au/u/toivo/kpackage

Wenn Sie nicht mit Gnome oder KDE arbeiten, müssen Sie die PowerTools von der Shell Prompt aus installieren.

E.3.2 Das Installieren von PowerTools von der Shell Prompt aus

Zuerst müssen Sie die PowerTools CD-ROM in Ihrem CD-ROM-Laufwerk mounten und den Befehl `ls` eingeben, um den Inhalt anzuzeigen. Wenn Sie nicht wissen, wie man eine CD-ROM unmounted, lesen Sie unter *Mounten der PowerTools CD-ROM* in Abschnitt E.2.1 nach.

Folgende Verzeichnisse werden angezeigt: `SRPMS` und `RedHat`. Das Verzeichnis `SRPMS` enthält PowerTools Quell-RPMs. Das Verzeichnis `RedHat/RPMS` enthält die RPMs fü r die drei vorgegebenen Betriebssystemarchitekturen.

Der Pfad RedHat/RPMS wird 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 wollen Sie mehr Informationen über ein spezielles Paket, bevor Sie entscheiden, 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 im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration.*

Andernfalls können Sie in der Datei CONTENTS nach Paketen suchen, die Sie interessieren. Weitere Informationen finden Sie unter *Die Datei CONTENTS lesen* in Abschnitt E.2.1.

Nachdem Sie sich für ein bestimmtes Paket entschieden haben, können Sie die Installation mit RPM durchführen. RPM ist ein leistungsfähiges Paketverwaltungssystem, das von der Befehlszeile aus bedient wird. Weitere Informationen zur Benutzung von RPM für die Installation und Verwaltung von PowerTools-Paketen finden Sie im *Offiziellen Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*

Wenn Sie die Installation Ihrer Pakete abgeschlossen haben, müssen Sie Ihre CD-ROM unmounten. Wenn Sie Schwierigkeiten mit dem Unmounten Ihrer CD-ROM haben, lesen Sie *Unmounten der PowerTools CD-ROM* in Abschnitt E.2.1 für weitere Informationen.

E.4 Deinstallieren der PowerTools

Um PowerTools-Pakete zu deinstallieren, müssen Sie so vorgehen wie bei allen anderen RPM-installierten Paketen auch.

Zuerst benötigen Sie den Namen des Paketes, das Sie deinstallieren wollen. Wenn Sie beispielsweise thrust-0.83c-11 aus Ihrem System deinstallieren möchten, wählen Sie Folgendes als Root:

```
rpm -e thrust
```

Allgemein dient rpm -e <*Paketnamen*> dazu, das Paket und die dazugehörigen Dateien von Ihrem System zu löschen. Die PowerTools CD-ROM ist nicht notwendig für diesen Vorgang.

Für weitere Informationen zur Verwendung von RPM lesen Sie das *Offizielle Red Hat Linux Handbuch Benutzerdefinierte Konfiguration*.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z