Red Hat Linux 9

Red Hat Linux Referenzhandbuch

Red Hat Linux 9: Red Hat Linux Referenzhandbuch


Red Hat, Inc.

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

rhl-rg(DE)-9-Print-RHI (2003-02-13T19:20)

Inhaltsverzeichnis

Einführung

Willkommen im *Red Hat Linux Referenzhandbuch*.

Das *Red Hat Linux Referenzhandbuch* enthält nützliche Informationen über Ihr Red Hat Linux-System. Für grundlegende Konzepte, wie z.B. die Struktur des Red Hat Linux-Dateisystems bis hin zu den Details, wie z.B. die Systemsicherheits- und Authentifizierungskontrolle, hoffen wir, dass dieses Buch zu einem wertvollen Nachschlagewerk für Sie wird.

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

- Struktur des Dateisystems
- Boot-Prozess
- Das X Window System
- Sicherheits-Tools
- Netzwerkleistungen

1. Änderungen an diesem Handbuch

Dieses Handbuch wurde zur besseren Übersicht neu angeordnet und mit den neuesten Merkmalen von Red Hat Linux 9 aktualisiert. Zu den Änderungen gehören u.a.:

Aktualisierung des Kapitels Das X Window System

> *Das X Window System* wurde komplett umgeschrieben und für eine bessere Klarheit neu organisiert. Weiterhin wurden Anleitungen zur Font-Konfiguration hinzugefügt.

Ein neues Kapitel `sysconfig` wurde hinzugefügt

> Der Abschnitt `sysconfig` des Kapitels *Boot, Init und Shutdown* wurde erweitert und in ein eigenes Kapitel ausgelagert.

Das Kapitel TCP Wrappers und `xinetd` wurde aktualisiert.

> Das aktualisierte Kapitel *TCP Wrappers und `xinetd`* wurde komplett umgestellt, um die Klarheit zu erhöhen.

Das Kapitel Benutzer und Gruppen wurde aktualisiert.

> Das Kapitel *Benutzer und Gruppen* wurde aktualisiert, neu organisiert und bietet eine verbesserte Klarheit.

Das Kapitel Netzwerkschnittstellen wurde aktualisiert.

> Das Kapitel *Netzwerkschnittstellen* wurde umgeschrieben und neu organisiert.

Das Kapitel Apache HTTP-Server wurde aktualisiert.

> Es steht nun ein Leitfaden zur Migration von Version 1.3 nach Version 2.0 von Apache HTTP-Server zur Verfügung. Außerdem wurde die Liste der Serverkonfigurations-Optionen auf den neuesten Stand gebracht. Ein besonderer Dank geht an **Gary Benson** und **Joe Orton** für ihre harte Arbeit am Apache HTTP-Server-Migrationsleitfaden.

Bevor Sie dieses Handbuch lesen, sollten Sie den Inhalt des *Red Hat Linux Installationshandbuchs* über Installationsfragen und des *Red Hat Linux Handbuchs Erster Schritte* über grundlegende Linux-Konzepte sowie des *Red Hat Linux Handbuchs benutzerdefinierter Konfiguration* für allgemeine An-

weisungen or zur benutzerdefinierten Einstellung durchlesen. Das *Red Hat Linux Referenzhandbuch* enthält Informationen zu fortgeschrittenen Themen, die vielleicht nicht jeden Benutzer betreffen, was jedoch davon abhängt, wie Sie Ihr Red Hat Linux-System benutzen.

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

Anmerkung

Auch wenn dieses Handbuch die bis heute aktuellsten Informationen enthält, sollten Sie zusätzlich auch die Red Hat Linux *Release Notes* lesen, die auch Informationen enthalten, die eventuell erst nach der Beendigung dieser Dokumentation zur Verfügung standen. Die *Release Notes* finden Sie auf der Red Hat Linux CD #1 und Online unter:

```
http://www.redhat.com/docs/manuals/linux
```

2. So finden Sie die geeignete Dokumentation

Es ist wichtig, daß Sie sich die Dokumentation beschaffen, die für Ihren Kenntnisstand in Sachen Linux geeignet ist. Andernfalls könnten Sie sich schnell überfordert fühlen oder nicht an die Informationen gelangen, mit deren Hilfe Sie Ihre Probleme lösen können. Das *Red Hat Linux Referenzhandbuch* beschäftigt sich mit den eher technischen Aspekten und Optionen Ihres Red Hat Linux-Systems. Dieser Abschnitt wird Ihnen dabei helfen, zu entscheiden, ob Sie dieses Handbuch als Informationsquelle benutzen wollen oder ob Sie andere Handbücher, einschließlich der Online-Quellen, bei Ihrer Suche zu Rate ziehen wollen.

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

Linux-Einsteiger

Dieser Benutzertyp hat bislang noch kein Linux- oder Linux-ähnliches Betriebssystem verwendet oder verfügt über nur geringe Kenntnisse in Linux. Möglicherweise sind bereits gewisse Kenntnisse im Umgang mit anderen Betriebssystemen vorhanden (beispielsweise Windows) Trifft dies auf Sie zu? Falls ja, sollten Sie sich Abschnitt 2.1 durchlesen.

Bereits einige Erfahrungen mit Linux

Dieser Benutzertyp hat Linux (aber nicht Red Hat Linux) zuvor bereits erfolgreich installiert und verwendet. Er verfügt unter Umständen auch über vergleichbare Erfahrungen mit anderen Betriebssystemen, die Linux ähneln. Trifft das auf Sie zu? Falls ja, sollten Sie sich Abschnitt 2.2 durchlesen.

Alter Hase

Dieser Benutzertyp hat Red Hat Linux bereits zuvor erfolgreich installiert und verwendet. Sind Sie ein alter Hase in Sachen Linux? Falls ja, sollten Sie sich Abschnitt 2.3 durchlesen.

2.1. Dokumentation für Linux-Einsteiger

Ein Linux-Einsteiger könnte von den vielen Informationen, die über jedes Argument, wie z.B. Drucken und Starten, zur Verfügung stehen, überfordert sein. Bevor Sie sich mit diesen Fortgeschrittenen-Themen auseinandersetzen, ist es sicher eine gute Idee, einen Schritt zurückzugehen, um zunächst einmal genügend Informationen über die Funktionsweise von Linux zu sammeln.

Ihr erstes Ziel sollte es zunächst sein, sich die notwendige Dokumentation zu beschaffen. Die Wichtigkeit dieses Schritts kann gar nicht oft genug betont werden. Ohne die erforderlichen Informationen können Sie Ihr Red Hat Linux-System nämlich auch nicht nach Ihren Wünschen einrichten.

Sie sollten sich die folgende Linux-Dokumentation beschaffen:

- *Ein kurzer Überblick über die 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, den Ansprüchen und Erfordernissen zusammenhängt. Wenn Sie sich zumindest ein bißchen mit der Entstehungsgeschichte von Linux auskennen, werden Sie im voraus herausfinden, wie Sie viele Ihrer potentiellen Probleme lösen können, bevor sie überhaupt auftreten.
- *Eine Erklärung der Funktionsweise von Linux* — Auch wenn es sicherlich 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 Betriebssysteme können möglicherweise nicht direkt auf Linux übertragen werden.
- *Eine einführende Befehlsübersicht (mit Beispielen)* — Dies ist unter Umständen. der wichtigste Punkt bei Ihrer Suche nach einer geeigneten Linux-Dokumentation. Die grundlegende Philosophie hinter Linux besteht darin, daß die Kombination von kleineren Befehlen mit eingeschränktem Funktionsumfang der Verwendung einiger weniger großer (aber damit auch komplizierteren) Befehle vorzuziehen ist. Wenn Sie sich nicht anhand der Beispiele mit dem von Linux vertretenen Ansatz für das Erledigen von Aufgaben vertraut machen können, liegt dies möglicherweise daran, daß Sie von der Vielzahl der auf Ihrem Red Hat Linux-System zur Verfügung stehenden Befehle schier überwältigt werden.

  Denken Sie aber bitte immer daran, daß Sie sich nicht an alle Ihnen 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 also lediglich ganz grob darüber Bescheid wissen, wie Linux funktioniert und wie Sie den Zugang zu dem Tool finden, das Ihnen genaue Anweisungen dazu gibt, wie Sie den Befehl ausführen müssen.

Das *Red Hat Linux Installationshandbuch* ist eine hervorragende Informationsquelle und hilft Ihnen dabei, Ihr Red Hat Linux-System erfolgreich zu installieren und grundlegend zu konfigurieren. Das *Red Hat Linux Handbuch Erster Schritte* behandelt auch die Entwicklungsgeschichte von Linux, die die wichtigsten Systembefehle, GNOME, KDE, RPM und informiert auch über viele andere grundlegende Themen. Sie sollten also mit diesen beiden Büchern beginnen, Ihr Grundlagenwissen über Red Hat Linux dann vertiefen. Früher oder später werden Ihnen auch kompliziertere Konzepte sinnvoll erscheinen, weil Sie die Grundgedanken dahinter bereits verstanden haben.

Außer den Red Hat Linux-Handbüchern stehen Ihnen auch viele andere hervorragende Dokumentationsquellen zur Verfügung, die - sofern sie nicht gratis sind - auch nicht viel kosten:

2.1.1. Einführung in Linux Webseiten

- http://www.redhat.com — Auf der Red Hat Website finden Sie Links 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 — Auf der Linux Headquarters-Website finden Sie leicht verständliche schrittweise Anweisungen zu einer Vielzahl von Linux-Tasks.

2.1.2. 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 selbst aktiv Fragen stellen oder beantworten. Erfahrene Linux-Benutzer sind dafür bekannt, daß Sie Einsteigern gerne bei Ihren unterschiedlichen Fragen zu Linux unter die Arme greifen — vor allem, wenn Sie Ihre Fragen vor dem richtigem Publikum stellen. Sollten Sie allerdings keinen Zugang zu einer der News Reader-Anwendungen haben, können Sie unter der folgenden Webadresse nach entsprechenden Informationen hierzu suchen: http://groups.google.com/. Es gibt nämliche Dutzende Linux-relevante Newsgroups, unter anderem die folgenden:

- linux.help — Eine hervorragende Adresse, sich von Linux-Kollegen helfen zu lassen.
- linux.redhat — In dieser Newsgroup geht es hauptsächlich um Red Hat Linux-spezifische Themen.
- linux.redhat.install — Dieser Newsgroup können Sie Fragen zur Installation stellen oder nachschauen, wie andere Benutzer ähnliche Probleme lösen oder gelöst haben.
- linux.redhat.misc — Fragen bzw. Anfragen, die nicht unbedingt in die gängigen Kategorien gehören, sollten Sie hier stellen.
- linux.redhat.rpm — Eine gute Adresse, die Sie aufsuchen sollten, wenn Sie mit **RPM** bestimmte Schwierigkeiten haben.

2.1.3. Linux-Bücher für Anfänger

- *Red Hat Linux for Dummies, 2. Auflage* 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 8 Unleashed* von Bill Ball und Hoyle Duff; Pearson Education

Die hier vorgeschlagenen Bücher sind sicher eine wertvolle Informationsquelle für die allgemeinen Grundkenntnisse über das Red Hat Linux- System. Detailliertere Informationen über die in diesem Handbuch beprochenen Themen finden Sie in den entsprechend spezifischen Büchern, deren Titel in einigen Kapiteln dieses Handbuch für Sie aufgelistet wurden - meist im *Weitere Informationsquellen*-Bereich.

2.2. Für erfahrene Linux-Benutzer

Wenn Sie bereits andere Linux-Produkte verwendet haben, sind Ihnen vermutlich die am gängigsten Befehle längst 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 allerdings auch für Sie sehr verwirrend sein.

Das *Red Hat Linux Handbuch benutzerdefinierter Konfiguration* wird Ihnen die verschiedenen Konfigurationsoptionen Ihres Red Hat Linux-Systems erläutern, mit denen Sie bestimmte Ziele erreichen können. Nutzen Sie dieses Handbuch dazu, sich mit den verschiedenen Konfigurationsoptionen und ihrer Umsetzung vertraut zu machen.

Wenn Sie Software installieren, die nicht im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration* enthalten ist, hilft es oft, sich anzusehen, wie andere Benutzer unter ähnlichen Umständen vorgegangen sind. Die HOWTO-Dokumente vom Linux Documentation Project stehen Ihnen unter http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html zur Verfügung und dokumentieren ganz bestimmte Linux-Aspekte - vom Low-Level-Kernel über esoterische Veränderungen bis zum Einsatz von Linux für einen Amateur-Radiosender.

2.3. Dokumentation für Linux-Gurus

Wenn Sie bereits seit mehreren Jahren Red Hat Linux benutzen, wissen Sie wahrscheinlich längst, daß der beste Weg zum Verständnis eines spezifischen Programms, das Lesen seines Quellcodes und/oder der Konfigurationsverzeichnisse ist. Ein großer Vorteil Red Hat Linux ist daß der Quellcode von allen Benutzern gelesen werden kann.

Natürlich ist nicht jeder ein Programmierer, und Sie können mit dem Quellcode daher vielleicht wenig anfangen. Wenn Sie jedoch nur ein wenig Erfahrungen und Kenntnisse haben und wissen, wie man ihn lesen kann, finden Sie im Quellcode die Antwort auf alle Ihre Fragen.

3. Dokumentkonventionen

Beim Lesen dieses Handbuchs werden Sie feststellen, dass bestimmte Wörter in verschiedenen Fonts, Schriftbildern, Größen usw. dargestellt sind. Diese Unterscheidung folgt einer bestimmten Ordnung: bestimmte Wörter werden auf die gleiche Weise dargestellt, um darauf hinzuweisen, dass sie zu einer bestimmten Kategorie gehören. Dazu gehören:

`Befehl`

Linux-Befehle (sowie Befehle anderer Betriebssysteme, sofern verwendet) werden auf diese Weise dargestellt. Diese Darstellungsart weist darauf hin, dass Sie das Wort oder den Satz in die Befehlszeile eingeben und die [Enter-Taste] drücken können, um den entsprechenden Befehl auszuführen. Gelegentlich enthält ein Befehl Wörter, die eigentlich auf eine andere Weise dargestellt werden würden (beispielsweise Dateinamen). In einem solchen Fall werden sie als Teil des Befehls betrachtet, und der gesamte Satz wird als Befehl dargestellt. Beispiel:

Verwenden Sie den Befehl `cat testfile`, um den Inhalt einer Datei mit dem Namen `testfile` in einem aktuellen Verzeichnis anzeigen zu lassen.

`Dateiname`

Datei- und Verzeichnisnamen sowie die Namen von Pfaden und RPM-Paketen werden auf diese Weise dargestellt, was bedeutet, dass eine bestimmte Datei oder ein bestimmtes Verzeichnis mit diesem Namen in Ihrem Red Hat Linux-System vorhanden ist. Beispiele:

Die Datei `.bashrc` in Ihrem Home-Verzeichnis enthält Bash-Shell Definitionen und Aliase für Ihren Gebrauch.

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

Installieren Sie den `webalizer` RPM, wenn Sie ein Analyseprogramm für eine Webserver-Protokolldatei verwenden möchten.

Applikation

Diese Darstellungsart weist darauf hin, dass es sich bei diesem Programm um eine Endbenutzer-Anwendung handelt (im Gegensatz zur System-Software). Beispiel:

Verwenden Sie **Mozilla**, um im Web zu browsen.

[Taste]

Die Tasten der Tastatur werden auf diese Weise dargestellt. Beispiel:

Um die [Tab]-Vervollständigung zu verwenden, geben Sie einen Buchstaben ein und drücken Sie anschließend die Taste [Tab]. Auf diese Weise wird die Liste der Dateien im Verzeichnis angezeigt, die mit diesem Buchstaben beginnen.

[Tasten]-[Kombination]

Eine Tastenkombination wird auf diese Art und Weise dargestellt.

Mit der Tastenkombination [Strg]-[Alt]-[Rücktaste] beenden Sie Ihre grafische Sitzung und kehren zum grafischen Anmeldebildschirm oder zur Konsole zurück.

Text in der GUI-Schnittstelle

Überschriften, Worte oder Sätze, die Sie auf dem GUI-Schnittstellenbildschirm oder in Window finden, werden in diesem Stil wiedergegeben. Wenn Sie daher einen Text in diesem Stil finden, soll dieser einen bestimmten GUI-Bildschirm oder ein Element eines GUI-Bildschirms (z.B. ein Text, der sich auf ein Kontrollkästchen oder auf ein Feld bezieht) identifizieren. Beispiel:

Wählen Sie das Kontrollkästchen **Passwort erforderlich**, wenn Ihr Bildschirmschoner passwortgeschützt sein soll.

Erste Menüstufe auf einem GUI-Bildschirm oder in einem Fenster

Wenn ein Wort auf diese Art und Weise dargestellt ist, zeigt dies an, dass es sich hierbei um den Anfang eines Pulldown-Menüs handelt. Beim Klicken auf das Wort auf dem GUI-Bildschirm erscheint der Rest des Menüs. Zum Beispiel:

Unter **Datei** auf dem GNOME-Terminal sehen Sie die Option **Neuer Tab**, mit dem Sie mehrere Shell Prompts im gleichen Fenster öffnen können.

Wenn Sie eine Befehlsreihe aus einem GUI-Menü eingeben wollen, wird diese entsprechend dem folgenden Beispiel angezeigt:

Indem Sie **Hauptmenü** (im Panel) => **Programmieren** => **Emacs** wählen, starten Sie den Texteditor **Emacs**.

Schaltfläche auf einem GUI-Bildschirm oder in einem Fenster

Diese Darstellungsweise zeigt an, dass man den betreffenden Text auf der Schaltfläche eines GUI-Bildschirms finden kann. Zum Beispiel:

Indem Sie auf die Schaltfläche **Zurück** klicken, kehren Sie auf die Website zurück, die Sie zuletzt angesehen haben.

`Computerausgabe`

Ein Text, der auf diese Art und Weise dargestellt ist, weist darauf hin, dass der Computer diesen Text in der Befehlszeile anzeigt. Dort werden Antworten auf die von Ihnen eingegebenen Befehle, Fehlermeldungen und interaktive Prompts für Eingaben während Skripts angezeigt; auch Programme werden auf diese Art und Weise angezeigt. Zum Beispiel:

Durch Eingabe von `ls` erscheint der Inhalt eines Verzeichnisses:

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

Die Ausgabe, die als Antwort auf den Befehl erscheint (in diesem Fall der Inhalt des Verzeichnisses), wird auf diese Art und Weise dargestellt.

`Prompt`

Ein Prompt wird auf diese Art und Weise dargestellt, wenn der Computer Ihnen mitteilen will, dass Sie nun eine Eingabe tätigen können. Beispiele:

```
$
```

```
#
```

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

```
leopard login:
```

`Benutzereingabe`

Ein Text wird auf diese Art und Weise dargestellt, wenn er vom Benutzer entweder in die Befehlszeile oder in die Textbox auf einem GUI-Bildschirm eingegeben werden soll. Im folgenden Beispiel wird **`text`** in diesem Stil angezeigt:

Mit dem Befehl **`text`** am Prompt `boot:` booten Sie Ihr System in das textbasierte Installationsprogramm.

Weiterhin machen wir Sie mit Hilfe von bestimmten Strategien auf bestimmte Informationen aufmerksam. Entsprechend dem Wichtigkeitsgrad, das die jeweilige Information für Ihr System hat, sind diese Items entweder als Anmerkung, Hinweis oder Warnung gekennzeichnet. Zum Beispiel:

Anmerkung

Beachten Sie, dass Linux ein fallspezifisches System ist. In anderen Worten bedeutet dies, dass Rose nicht das gleiche ist wie ROSE und dies auch nicht das gleiche wie rOsE.

Tipp

Das Verzeichnis `/usr/share/doc` enthält zusätzliche Dokumentationen für im System installierte Pakete.

Wichtig

Wenn Sie die DHCP Konfigurationsdatei bearbeiten, werden die Änderungen erst wirksam, wenn Sie den DHCP-Daemon neu gestartet haben.

Achtung

Führen Sie keine alltäglichen Aufgaben als root aus — verwenden Sie hierzu außer für den Fall, dass Sie einen root-Account für Ihre Systemverwaltung benutzen, einen regulären Benutzeraccount.


Warnung

Falls Sie beschließen, nicht manuell zu partionieren, entfernt eine Serverinstallation alle bestehenden Partitionen von allen installierten Festplattenlaufwerken. Wählen Sie diese Installationsklasse nur dann, wenn Sie sich sicher sind, dass Sie keine zu speichernden Daten haben.

4. Verwenden der Maus

Für die Benutzung von Red Hat Linux ist eine Maus mit drei Tasten vorgesehen. Falls Sie im Besitz einer Maus mit nur zwei Tasten sind, sollten Sie während des Installationsprozesses die Drei-Tasten-Emulation wählen. Mit der Drei-Tasten-Emulation betätigen Sie die dritte, nicht real vorhandene (mittlere) Maus-Taste, indem Sie die beiden vorhandenen Tasten gleichzeitig drücken.

Immer wenn Sie in diesem Dokument dazu aufgefordert werden, etwas mit der Maus anzuklicken, bedeutet dies automatisch, dass Sie mit der linken Taste klicken sollen. Falls Sie hingegen die mittlere oder die rechte Maus-Taste betätigen sollen, werden Sie ausdrücklich dazu aufgefordert. (Rechts und links sind genau umgekehrt, wenn Sie Ihre Maus für die Benutzung durch einen Linkshänder konfiguriert haben.)

Wahrscheinlich kennen Sie den Ausdruck "ziehen und ablegen" (Drag & Drop) bereits. Wenn Sie dazu aufgefordert werden, eine Item auf Ihrem GUI-Desktop zu ziehen und abzulegen, bedeutet dies, dass Sie etwas anklicken sollen und dann die Maus-Taste gedrückt halten. Sie halten nun die Maus-Taste weiterhin gedrückt und ziehen das Element, indem Sie die Maus auf die gewünschte Position bewegen. Nachdem Sie auf dieser Position angekommen sind, lassen Sie die Maus-Taste los und legen damit das Element ab.

5. Kopieren und Einfügen von Text mit X

Das Kopieren und Einfügen von Text mit der Maus und dem X Window System ist sehr einfach. Um Text zu kopieren, klicken Sie auf Ihre linke Maustaste und ziehen Sie den Cursor über den Text, um ihn hervorzuheben. Um den Text an einer anderen Stelle einzufügen, klicken Sie einfach an der gewünschten Stelle auf die mittlere Maustaste.

6. Fortsetzung folgt!

Das *Red Hat Linux Referenzhandbuch* ist Teil des ständig wachsenden Engagements seitens Red Hat, den Red Hat Linux-Benutzer zum richtigen Zeitpunkt durch nützliche Informationen zu unterstützen. In den künftigen Ausgaben werden Sie erweiterte Informationen über Änderungen im Systemaufbau und in der Systemorganisation, neue und leistungsstarke Sicherheits-Tools und weitere Ressourcen finden, mit denen Sie Ihr Red Hat Linux-System noch besser nutzen — und selbstverständlich auch Ihr System-Knowhow!

Hier könnten wir Ihre Hilfe gebrauchen!

6.1. Wir brauchen Ihre Rückmeldung!

Wenn Sie Fehler im *Red Hat Linux Referenzhandbuch* entdecken oder Vorschläge oder Anregungen zur Verbesserung diesse Handbuchs machen möchten, würden wir uns sehr freuen, von Ihnen zu hören! Schreiben Sie bitte Bugzilla (http://bugzilla.redhat.com/bugzilla) mit dem Kenntwort *rhl-rg*.

Geben Sie bitte dabei auch die Kennziffer dieses Handbuchs ein:

```
rhl-rg(DE)-9-Print-RHI (2003-02-13T19:20)
```

Nur mit der Kennziffer des Handbuchs wissen wir, welche Version Ihnen vorliegt.

Wenn Sie Vorschläge zur Verbesserung der Dokumentation haben, beschreiben Sie uns Ihren Vorschlag bitte so präzise wie möglich. Und wenn Sie einen Fehler entdeckt haben, hilft es uns , wenn Sie uns den genauen Abschnitt und die Textstelle angeben - nur so können wir die Stelle finden und korrigieren.

7. Melden Sie sich für den Support an

Wenn Sie eine offizielle Version von Red Hat Linux 9 erworben haben, können Sie die Vorteile als Kunde von Red Hat nutzen.

Sie können einige oder andere der folgenden Vorteile nutzen, je nachdem welches der Red Hat Linux Produkte Sie erworben haben:

- Red Hat Support — Sie erhalten vom Red Hat, Inc. Support-Team Hilfe bei der Installation.
- Red Hat Network — Einfaches Update Ihrer Pakete. Sie erhalten auf Ihr System abgestimmte Sicherheits-Meldungen. Unter http://rhn.redhat.com finden Sie weitere Details.
- *Under the Brim: The Official Red Hat E-Newsletter* — Sie erhalten monatlich die neuesten Mitteilungen und Produktinformationen direkt von Red Hat.

Melden Sie sich unter http://www.redhat.com/apps/activate/. Ihre Produkt ID finden Sie auf der schwarz/rot/weißen Karte in Ihrer Red Hat Linux Box.

Weitere Informationen über den technischen Support für das Red Hat Linux finden Sie im *Technischen Support anfordern* des *Red Hat Linux Installationshandbuch*.

Viel Glück und vielen Dank, dass Sie sich für Red Hat Linux entschieden haben!

Das Red Hat Dokumentationsteam

I. System

Um das System effektiv zu verwalten, ist es entscheidend, seine Komponenten zu kennen und zu verstehen, wie diese zusammenhängen. Dieser Teil behandelt viele wichtige Aspekte des Systems. Er behandelt den Boot-Prozess, das grundlegende Layout des Dateisystems, den Ort von wichtigen Systemdateien und Dateisystemen, sowie die grundlegenden Konzepte hinter Benutzern und Gruppen. Zusätzlich wird das X Window System ausführlich beschrieben.

Inhaltsverzeichnis

redhat

Kapitel 1.

Boot, Init und Shutdown

Einer der größten Vorteile von Red Hat Linux ist die flexible und Benutzer-konfigurierbare Methode des Bootens und Herunterfahrens des Betriebssystems. Benutzer können viele Aspekte des Bootvorgangs frei einstellen, einschließlich welche Programme während des Bootens gestartet werden. Ebenso beendet das richtige Herunterfahren des Systems die Prozesse auf organisierte und konfigurierbare Art und Weise, auch wenn die individuelle Gestaltung dieses Prozesses kaum erforderlich ist.

Das Verstehen der Funktionsweise der Boot- und Shutdownprozesse erleichtert nicht nur das individuelle Gestalten von Red Hat Linux je nach Ihren Anforderungen, sondern macht auch das Beheben von Fehlern einfacher, die beim Starten oder Herunterfahren des Systems auftreten können.

1.1. Der Bootprozess

Nachfolgend werden die grundlegenden Phasen des Bootprozesses für ein x86-System beschrieben:

1. Das System-BIOS prüft das System und startet den ersten Bootloader auf dem MBR der primären Festplatte.
2. Der Bootloader der ersten Phase wird in den Arbeitsspeicher geladen und startet den Bootloader der zweiten Phase von der `/boot/`-Partition.
3. Der Bootloader der zweiten Phase lädt den Kernel in den Arbeitsspeicher, welcher wiederum seinerseits alle erforderlichen Module lädt und die root-Partition als schreibgeschützt mountet.
4. Der Kernel übergibt die Steuerung des Bootprozesses an das Programm `/sbin/init`.
5. Das Programm `/sbin/init` lädt alle Dienste und Tools des Arbeitsplatzes und mountet alle in `/etc/fstab` genannten Partitionen.
6. Dem Benutzer wird eine Anmeldeaufforderung für das gerade gestartete Linux-System angezeigt.

Da das Konfigurieren des Bootprozesses häufiger ist als die individuelle Gestaltung des Herunterfahrens, wird im restlichen Kapitel die Funktionsweise des Bootprozesses sowie die individuelle Anpassung an Ihre Bedürfnisse detailliert behandelt.

1.2. Der Bootprozess im Detail

Der wirkliche Beginn des Bootprozesses hängt von der verwendeten Hardware-Plattform ab. Sobald jedoch der Kernel vom System gefunden und geladen wurde, ist der standardmäßige Bootprozess auf allen Architekturen identisch. Dieses Kapitel bezieht sich auf eine x86-Architektur.

1.2.1. Das BIOS

Wenn ein x86-Computer gestartet wird, sucht der Prozessor am Ende des Systemspeichers nach dem *Basic Input/Output System* oder *BIOS*-Programm und führt es aus. Das BIOS steuert nicht nur den ersten Schritt des Bootprozesses, sondern stellt auch die Schnittstelle der untersten Ebene zu den Peripheriegeräten dar. Daher ist es im schreibgeschützten permanenten Speicher abgelegt und ständig einsatzbereit.

Andere Plattformen verwenden verschiedene Programme, um Aufgaben der niedrigen Ebene durchzuführen, die denen des BIOS auf einem x86-System stark ähneln. Itanium-basierte Computer zum Beispiel verwenden die *Extensible Firmware Interface* (*EFI*)*-Shell*, während Alpha-Systeme die *SRM-Konsole* verwenden.

Nach dem Start prüft das BIOS das System, sucht und prüft Peripheriegeräte und sucht dann nach einem gültigen Gerät zum Starten des Systems. Normalerweise prüft es zuerst die Disketten- und CD-ROM-Laufwerke auf startfähige Medien und sucht dann auf den Festplatten des Systems. Die Reihenfolge der zum Booten durchsuchten Laufwerke wird oft durch eine Einstellung auf dem BIOS gesteuert. Häufig ist die erste, zum Booten festgelegte Festplatte das Laufwerk C oder das Master-IDE-Gerät auf dem primären IDE-Bus. Das BIOS lädt das Programm, das im ersten Sektor dieses Geräts gespeichert ist und *Master Boot Record* oder *MBR* genannt wird, in den Speicher. Der MBR ist nur 512 Bytes groß und enthält vom Rechner lesbare Anweisungen zum Booten des Rechners zusammen mit der Partitionstabelle. Nach dem Laden prüft das BIOS das jeweilige Programm auf dem MBR.

1.2.2. Der Bootloader

In diesem Abschnitt wird der Bootprozess für die x86-Plattform betrachtet. Je nach Systemarchitektur kann der Bootprozess leicht variieren. Unter Abschnitt 1.2.2.1 finden Sie einen kurzen Überblick über die Prozesse für Systeme, die keine x86 sind.

Unter Red Hat Linux stehen zwei Bootloader zur Verfügung: *GRUB* oder *LILO*. GRUB ist der Default-Bootloader, LILO ist allerdings verfügbar für alle die diesen entweder benötigen oder vorziehen. Für weitere Informationen zum Konfigurieren von GRUB oder LILO, siehe Kapitel 2.

Die Linux-Bootloader für x86-Plattformen werden in mindestens zwei Phasen unterteilt. Die erste Phase ist ein kleiner binärer Rechnercode auf dem MBR. Seine einzige Aufgabe besteht im Suchen des Bootloaders der zweiten Phase und dem Laden des ersten Teils in den Arbeitsspeicher.

GRUB ist der neuere Bootloader und hat den Vorteil, dass er ext2 und ext3 [1] Partitionen lesen kann und seine Konfigurationsdatei — `/boot/grub/grub.conf` — zur Bootzeit laden kann. Sehen Sie Abschnitt 2.7 für Informationen zum Bearbeiten dieser Datei.

Unter LILO verwendet der Bootloader der 2. Phase die Informationen auf dem MBR, um zu ermitteln, welche Bootoptionen dem Benutzer zur Verfügung stehen. Dies bedeutet, dass Sie bei jeder Konfigurationsänderung oder manuellen Kernelaktualisierung den Befehl `/sbin/lilo -v -v` ausführen müssen, um die entsprechenden Informationen auf den MBR zu schreiben. Detaillierte Informationen hierzu finden Sie unter Abschnitt 2.8.

Tipp

Wenn Sie ein Upgrade des Kernel mit Hilfe des **Red Hat Update Agent** durchführen, wird die Konfigurationsdatei des Bootloader automatisch aktualisiert. Weitere Informationen zu RHN finden Sie unter folgendem URL: https://rhn.redhat.com

Wenn der Bootloader der 2. Phase in den Arbeitsspeicher geladen ist, wird dem Benutzer der grafische Anfangsbildschirm von Red Hat Linux mit den verschiedenen Betriebssystemen oder Kernel angezeigt, die gestartet werden sollen. Auf diesem Bildschirm kann ein Benutzer die Pfeiltasten benutzen, um ein Betriebssystem auszuwählen und dann die [Enter-Taste] drücken, um dieses zu booten. Sollte keine Taste gedrückt werden, wird der Bootloader nach einiger Zeit das standardmäßig ausgewählte Betriebsystem booten.

1. GRUB liest ext3 Dateisysteme als ext2, unabhängig von der Journal-Datei. Sehen Sie das Kapitel *Das ext3 Dateisystem* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration* für mehr Informationen zum ext3 Dateisystem.

Anmerkung

Wenn SMP-Kernel-Support (Symmetric Multi-Processor) installiert ist, stehen Ihnen beim Erststart des Systems mehrere Optionen zur Verfügung. Unter LILO wird `linux`, für den SMP Kernel, und `linux-up`, für den Einzelprozessor, angezeigt. Unter GRUB wird `Red Hat Linux (<Kernelversion>-smp)`, für den SMP Kernel, und `Red Hat Linux (<Kernelversion>)`, für den Einzelprozessor, angezeigt.

Treten beim SMP-Kernel Probleme auf, wählen Sie einen nicht-SMP-Kernel beim Neustart aus.

Nachdem der Bootloader der 2. Phase den zu bootenden Kernel ermittelt hat, sucht er die entsprechende Binärdatei des Kernel im `/boot`-Verzeichnis. Die eigentliche Binärdatei ist die Datei `/boot/vmlinuz-2.4.x-xx`, die den Einstellungen des Bootloaders entspricht.

Informationen zum Ändern von Befehlszeilenargumenten im Kernel finden Sie unter Kapitel 2. Informationen zum Ändern des Runlevels am GRUB- oder LILO-Prompt finden Sie unter Abschnitt 2.10.

Anschließend legt der Bootloader das entsprechende Image der *initialen RAM-Disk*, *initrd* im Speicher ab. `initrd` wird vom Kernel zum Laden der nicht kompilierten Treiber verwendet, die zum Starten des Systems erforderlich sind. Dies ist besonders wichtig, wenn Sie SCSI-Festplatten haben oder das ext3 Dateisystem [2] verwenden.

Warnung

Entfernen Sie auf gar keinen Fall das `/initrd/`-Verzeichnis aus dem Dateisystem. Wenn dieses Verzeichnis entfernt wird, kann das System nicht starten und der Kernel meldet einen gravierenden Fehler.

Sobald der Kernel und das *initrd*-Image in den Speicher geladen sind, übergibt der Bootloader die Steuerung des Bootprozesses an den Kernel.

Für einen detaillierteren Überblick des GRUB und des LILO Bootloaders, sehen Sie Kapitel 2.

1.2.2.1. Bootloader für andere Architekturen

Ist der Red Hat Linux Kernel erst einmal geladen und übergibt den Bootprozess zum `init` Befehl, erfolgt die selbe Abfolge von Events auf jeder Architektur. Der Hauptunterschied zwischen den Bootprozessen der verschiedenen Architekturen liegt deshalb in der Applikation, welche zum Finden und Laden des Kernel verwendet wird.

Die Alpha-Architektur, zum Beispiel, verwendet den `aboot` Bootloader, während die Itanium-Architektur den ELILO Bootloader verwendet.

Lesen Sie das für die jeweilige Plattform spezifische *Red Hat Linux Installationshandbuch* für Informationen zum Konfigurieren der Bootloader.

2. Detaillierte Informationen zum Erstellen von *initrd*, sehen Sie das Kapitel *Das ext3 Dateisystem* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

1.2.3. Der Kernel

Wenn der Kernel lädt, initialisiert und konfiguriert er sofort den Arbeitsspeicher des Computers. Anschließend wird die an das System angeschlossene Hardware konfiguriert, einschließlich aller Prozessoren und E/A-Subsysteme sowie alle Speichergeräte. Dann sucht er nach dem komprimierten `initrd`-Image an einem bestimmten Speicherort im Speicher, dekomprimiert es, mountet es und lädt alle notwendigen Treiber. Danach initialisiert er die mit dem Dateisystem verbundenen virtuellen Geräte wie LVM oder Software-RAID, bevor das `initrd`-Disk-Image dekomprimiert und der gesamte Speicher freigesetzt wird, der belegt war.

Nach dem Initialisieren aller Geräte des Systems erstellt der Kernel ein root-Gerät, mountet die root-Partition als schreibgeschützt und setzt nicht verwendeten Speicher frei.

Zu diesem Zeitpunkt ist der Kernel in den Speicher geladen und betriebsbereit. Allerdings ist das System ohne die Möglichkeit für den Benutzer, sinnvolle Eingaben vorzunehmen, nicht von großem Nutzen.

Der Kernel startet den Befehl `/sbin/init`, um die Benutzerumgebung einzurichten.

1.2.4. Das Programm `/sbin/init`

Das Programm `/sbin/init` (auch `init` genannt) koordiniert den verbleibenden Bootprozess und konfiguriert die Benutzerumgebung.

Wenn `init` gestartet wird, wird es automatisch der "Stammvater" aller zukünftigen Prozesse des Systems, die auf einem Red Hat Linux-System automatisch gestartet werden. Zuerst führt es das `/etc/rc.d/rc.sysinit`-Skript aus, mit dem der Umgebungspfad eingestellt wird, Swapping gestartet, die Dateisysteme überprüft werden, u.v.m. `rc.sysinit` kümmert sich im Grunde um alle Prozesse, die beim Starten des Systems durchgeführt werden müssen. Die meisten Systeme verwenden zum Beispiel eine Uhr. In diesem Fall liest `rc.sysinit` die Konfigurationsdatei `/etc/sysconfig/clock`, um die Hardware-Uhr zu initialisieren. Falls Sie über spezielle serielle Portprozesse verfügen, die ebenfalls initialisiert werden müssen, führt `rc.sysinit` die Datei `/etc/rc.serial` aus.

Anschließend führt `init` das `/etc/inittab`-Skript aus, das beschreibt, wie das System auf jedem *SysV init- Runlevel* eingerichtet werden sollte [3]. Die Datei `/etc/inittab` legt u.a. den Standard-Runlevel fest und bestimmt, dass `/sbin/update` bei jedem Start eines bestimmten Runlevels ausgeführt werden muss. [4].

Danach legt `init` die Quellfunktionsbibliothek `/etc/rc.d/init.d/functions` für das System fest. In der Datei wird festgelegt, wie Programme zu starten oder zu beenden sind und wie die PID eines Programms bestimmt werden kann.

Danach startet `init` alle Hintergrundprozesse, indem es im entsprechenden `rc`-Verzeichnis nach den Runleveln sucht, die in `/etc/inittab` als Standard festgelegt sind. Die `rc`-Verzeichnisse sind gemäß den Runleveln nummeriert, die sie darstellen. So ist zum Beispiel `/etc/rc.d/rc5.d/` das Verzeichnis für Runlevel 5.

Das Programm `init` sucht beim Starten auf Runlevel 5 im Verzeichnis `/etc/rc.d/rc5.d/`, um die Prozesse zu ermitteln, die gestartet und beendet werden müssen.

Folgend ist ein Beispiel-Listing für das Verzeichnis `/etc/rc.d/rc5.d/`:

```
K05innd -> ../init.d/innd
K05saslauthd -> ../init.d/saslauthd
K10psacct -> ../init.d/psacct
K12cWnn -> ../init.d/cWnn
K12FreeWnn -> ../init.d/FreeWnn
```

3. Weitere Informationen zu SysV init Runleves finden Sie unter Abschnitt 1.4.
4. Das `update`-Programm gibt fehlerhafte Buffer auf der Festplatte wieder frei.

```
K12kWnn -> ../init.d/kWnn
K12mysqld -> ../init.d/mysqld
K12tWnn -> ../init.d/tWnn
K15httpd -> ../init.d/httpd
K15postgresql -> ../init.d/postgresql
K16rarpd -> ../init.d/rarpd
K20bootparamd -> ../init.d/bootparamd
K20iscsi -> ../init.d/iscsi
K20netdump-server -> ../init.d/netdump-server
K20nfs -> ../init.d/nfs
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwalld -> ../init.d/rwalld
K20rwhod -> ../init.d/rwhod
K24irda -> ../init.d/irda
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
K34dhcrelay -> ../init.d/dhcrelay
K34yppasswdd -> ../init.d/yppasswdd
K35atalk -> ../init.d/atalk
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K35winbind -> ../init.d/winbind
K40mars-nwe -> ../init.d/mars-nwe
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K45smartd -> ../init.d/smartd
K46radvd -> ../init.d/radvd
K50netdump -> ../init.d/netdump
K50snmpd -> ../init.d/snmpd
K50snmptrapd -> ../init.d/snmptrapd
K50tux -> ../init.d/tux
K54pxe -> ../init.d/pxe
K55routed -> ../init.d/routed
K61ldap -> ../init.d/ldap
K65identd -> ../init.d/identd
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
K70aep1000 -> ../init.d/aep1000
K70bcm5820 -> ../init.d/bcm5820
K74ntpd -> ../init.d/ntpd
K74ups -> ../init.d/ups
K74ypserv -> ../init.d/ypserv
K74ypxfrd -> ../init.d/ypxfrd
K84bgpd -> ../init.d/bgpd
K84ospf6d -> ../init.d/ospf6d
K84ospfd -> ../init.d/ospfd
K84ripd -> ../init.d/ripd
K84ripngd -> ../init.d/ripngd
K85zebra -> ../init.d/zebra
K90isicom -> ../init.d/isicom
K92ipvsadm -> ../init.d/ipvsadm
K95firstboot -> ../init.d/firstboot
S00microcode_ctl -> ../init.d/microcode_ctl
S05kudzu -> ../init.d/kudzu
```

```
S08ip6tables -> ../init.d/ip6tables
S08ipchains -> ../init.d/ipchains
S08iptables -> ../init.d/iptables
S09isdn -> ../init.d/isdn
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13portmap -> ../init.d/portmap
S14nfslock -> ../init.d/nfslock
S17keytable -> ../init.d/keytable
S20random -> ../init.d/random
S24pcmcia -> ../init.d/pcmcia
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
S28autofs -> ../init.d/autofs
S44acpid -> ../init.d/acpid
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S80sendmail -> ../init.d/sendmail
S80spamassassin -> ../init.d/spamassassin
S84privoxy -> ../init.d/privoxy
S85gpm -> ../init.d/gpm
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
S90cups -> ../init.d/cups
S90xfs -> ../init.d/xfs
S95anacron -> ../init.d/anacron
S95atd -> ../init.d/atd
S97rhnsd -> ../init.d/rhnsd
S99local -> ../rc.local
S99mdmonitor -> ../init.d/mdmonitor
```

Wie Sie sehen, befindet sich keines der Skripte, die die Dienste starten und beenden, im Verzeichnis `/etc/rc.d/rc5.d/`. Vielmehr sind alle Dateien in `/etc/rc.d/rc5.d/` *symbolische Links*, die auf Skripte im `/etc/rc.d/init.d/`-Verzeichnis zeigen. Symbolische Links werden in allen `rc`-Verzeichnissen verwendet, so dass die Runlevel durch Erstellen, Ändern und Löschen der symbolischen Links neu konfiguriert werden können, ohne dass die aktuellen Skripte davon betroffen werden, auf die sie verweisen.

Der Name jedes symbolischen Links beginnt entweder mit einem `K` oder einem `S`. Die `K`-Links sind Prozesse, die auf diesem Runlevel entfernt werden, während die Links gestartet werden, die mit einem `S` beginnen.

Zuerst beendet der Befehl `init` alle symbolischen `K`-Links im Verzeichnis mit Hilfe des Befehls `/etc/rc.d/init.d/<`*`Befehl`*`> stop`, wobei `<`*`Befehl`*`>` der zu beendende Prozess ist. Anschließend werden alle symbolischen `S`-Links mit Hilfe von `/etc/rc.d/init.d/<`*`Befehl`*`> start` gestartet.

Tipp

Wenn das System den Bootvorgang beendet hat, können Sie sich als root anmelden und dieselben Skripte zum Starten und Beenden der Dienste ausführen. So beendet zum Beispiel der Befehl `/etc/rc.d/init.d/httpd stop` den Apache-Web-Server.

Alle symbolischen Links sind nummeriert, um die Startreihenfolge festzulegen. Sie können die Reihenfolge ändern, in der die Dienste gestartet oder beendet werden, indem Sie die Nummerierung

ändern. Je kleiner die Nummer, desto früher wird gestartet. Die symbolischen Links mit derselben Nummer werden in alphabetischer Reihenfolge gestartet.

Anmerkung

Als eine der letzten Aktionen führt das Programm `init` alle Skripte aus, die sich in `/etc/rc.d/rc.local` befinden. Diese Datei ist nützlich für das Anpassen des Systems. Für mehr zur Verwendung von `rc.local` lesen Sie Abschnitt 1.3.

Nachdem der Befehl `init` das entsprechende `rc`-Verzeichnis für das Runlevel verarbeitet hat, sucht das Skript `/etc/inittab` einen `/sbin/getty`-Prozess für jede virtuelle Konsole (Anmeldebildschirme), die dem Runlevel zugewiesen ist. Runlevel 2 bis 5 rufen alle sechs virtuellen Konsolen auf, während Runlevel 1 (Einzelbenutzermodus) nur eine aufruft und Runlevel 0 und 6 gar keine. Der `/sbin/mingetty`-Prozess öffnet Kommunikationswege zu *tty*-Geräten[5],legt die Modi fest, druckt den Anmeldebildschirm, ruft den Benutzernamen ab und initiiert den Anmeldeprozess für den Benutzer.

Auf Runlevel 5 führt `/etc/inittab` das Skript `/etc/X11/prefdm` aus. Das `prefdm`-Skript führt den gewünschten X-Desktop-Manager aus — `gdm`, `kdm` oder `xdm`, je nach Inhalt der Datei `/etc/sysconfig/desktop`.

Zu diesem Zeitpunkt ist das System im Runlevel 5 und zeigt den Anmeldebildschirm an.

1.3. Ausführen von zusätzlichen Programmen zum Zeitpunkt des Bootens

Das Skript `/etc/rc.d/rc.local` wird vom Befehl `init` zum Zeitpunkt des Bootens ausgeführt, nachdem die restliche Initialisierung abgeschlossen ist, sowie bei Änderungen der Runlevel. Das Hinzufügen von Befehlen zu diesem Skript ist ein einfacher Weg, notwendige Tasks auszuführen, wie das Starten von speziellen Services oder das Initialisieren von Geräten, ohne ein Schreiben komplizierter Installationsskripte im Verzeichnis `/etc/rc.d/init.d/` und das Erzeugen symbolischer Links zu erfordern.

Wenn Sie das Einstellen von seriellen Ports benötigen, können Sie außerdem `/etc/rc.serial` erstellen und ändern, so dass es zum Zeitpunkt des Bootens automatisch ausgeführt wird. Dieses Skript kann eine Vielzahl von `setserial`-Befehlen ausführen, um die seriellen Ports des Systems speziell zu konfigurieren. Auf der `setserial`-man-Seite finden Sie weitere Informationen hierzu.

1.4. SysV Init Runlevels

Das SysV init Runlevel System stellt einen Standardprozess zur Kontrolle, welche Programme von `init` während des Initialisierens des Runlevels gestartet oder angehalten werden, bereit. SysV wurde gewählt, da es einfacher zu benutzen und flexibler ist als der herkömmliche BSD-Style-Init-Prozess.

Die Konfigurationsdateien für SysV init befinden sich im Verzeichnis `/etc/rc.d/`. In diesem Verzeichnis befinden sich die Skripte `rc`, `rc.local`, `rc.sysinit` und, optional, `rc.serial` sowie die folgenden Verzeichnisse:

```
init.d/
rc0.d/
rc1.d/
```

5. Weitere Informationen zu `tty`-Geräten finden Sie unter Abschnitt 5.3.11.

```
rc2.d/
rc3.d/
rc4.d/
rc5.d/
rc6.d/
```

Das Verzeichnis `init.d` enthält die vom Befehl `/sbin/init` zum Steuern der Dienste verwendeten Skripte. Jedes der nummerierten Verzeichnisse stellt die sechs Runlevel dar, die standardmäßig unter Red Hat Linux konfiguriert sind.

1.4.1. Runlevels

Runlevels sind ein Zustand, oder *Modus*, durch die im SysV Verzeichnis `/etc/rc.d/rc<x>.d/` enthaltenen Services definiert werden, wobei <x> die Nummer des Runlevels ist.

Die Idee hinter SysV init Runlevels basiert auf der Gegebenheit, dass verschiedene Systeme auf verschiedene Weise verwendet werden können. Ein Server, zum Beispiel, ist effizienter, wenn kein X Window System läuft und Systemressourcen verschwendet. Zu anderen Zeiten muss z.B. ein Systemadministrator das System auf einem niedrigeren Runlevel betreiben, um diagnostische Aufgaben zu erledigen, wie das Beheben von korrumpierten Dateisystemen in Runlevel 1, wenn keine anderen Benutzer auf dem System sein können.

Die Eigenschaften eines gegebenen Runlevel bestimmen, welche Services von `init` angehalten und gestartet werden. Runlevel 1 (Einzelbenutzer-Modus), zum Beispiel, hält alle Netzwerk-Services, während Runlevel 3 diese startet. Durch die Angabe, bei welchem Runlevel spezifische Services angehalten oder gestartet werden, kann `init` schnell den Modus der Maschine ändern, ohne dass der Benuzter diese Services manuell starten oder anhalten müsste.

Die folgenden Runlevels sind in Red Hat Linux standardmäßig definiert:

- `0` — Anhalten
- `1` — Einzelbenutzer Textmodus
- `2` — Nicht belegt (benutzerspezifisch)
- `3` — Vollständiger Mehrbenutzer Textmodus
- `4` — Nicht belegt (benutzerspezifisch)
- `5` — Vollständiger Mehrbenutzer graphischer Modus (mit einem X-basierten Anmeldebildschirm)
- `6` — Neu booten

Im allgemeinen arbeitet Red Hat Linux auf Runlevel 3 oder Runlevel 5 — und zwar jeweils im vollständigen Mehrbenutzermodus. Die Runlevels 2 und 4 können vom Benutzer definiert werden, da diese ja nicht verwendet werden.

Der Standard-Runlevel wird in `/etc/inittab` bestimmt. Um für Ihr System den Standard-Runlevel herauszufinden, müssen Sie eine Zeile suchen, die der unten angegebenen `/etc/inittab` ähnelt:

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

Der standardmäßige Runlevel im obigen Beispiel ist fünf, wie die Nummer hinter dem Doppelpunkt angibt. Um diesen zu ändern, bearbeiten Sie `/etc/inittab` als root.

Warnung

Seien Sie beim Bearbeiten von `/etc/inittab` vorsichtig. Einfache Schreibfehler können dazu führen, dass das System nicht mehr booten kann. Sollte dies vorkommen, verwenden Sie entweder eine Bootdiskette, treten Sie in den Einzelbenutzermodus ein, oder geben Sie Rescue-Modus ein, um Ihren Computer zu booten und die Datei zu reparieren.

Für mehr Information zu Einzelbenutzer und Rescue-Modus, sehen Sie Kapitel *Rescue-Modus* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

Es ist möglich, den Default-Runlevel zur Bootzeit zu ändern, indem Sie die Argumente ändern, die der Bootloader dem Kernel übergibt. Weitere Informationen zum Ändern der Runlevel zur Bootzeit finden Sie unter Abschnitt 2.10.

1.4.2. Runlevel Utilities

Einer der besten Wege, die Runlevels zu konfigurieren, ist die Verwendung eines *Initscript Utility*. Diese Tools erleichtern den Task, die Dateien in der SysV init Verzeichnishierarchie zu warten und nimmt es den Systemadministratoren ab, die große Anzahl von symbolischen Links in den Unterverzeichnissen von `/etc/rc.d/` direkt ändern zu müssen.

Red Hat Linux stellt drei dieser Utilities zur Verfügung:

- `/sbin/chkconfig` — Das `/sbin/chkconfig` Utility stellt ein einfaches Befehlszeilentool für die Pflege der `/etc/rc.d/init.d/`-Verzeichnishierarchie zur Verfügung.
- **/sbin/ntsysv** — Das ncurses-basierte **/sbin/ntsysv** Utility stellt eine interaktive textbasierte Oberfläche zur Verfügung, was einige benutzerfreundlicher finden, als die Befehlszeilenoberfläche von `chkconfig`.
- **Services-Konfigurationstool** — Das graphische **Services-Konfigurationstool** (`redhat-config-services`) Programm ist ein flexibles GTK2-basiertes Utility zum Konfigurieren der Runlevels.

Im Kapitel *Kontrolle des Zugriffs auf die Dienste* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration* finden Sie weitere Informationen zu diesen Tools.

1.5. Herunterfahren

Um Red Hat Linux herunterzufahren, kann der root-Benutzer den Befehl `/sbin/shutdown` ausführen. Die man-Seiten zu `shutdown` enthalten eine vollständige Liste von Optionen. Hier sind die zwei am häufigsten verwendeten:

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

Nachdem das System vollständig heruntergefahren wurde, hält die Option `-h` die Maschine an, und die Option `-r` startet diese neu.

Normale Benutzer können die Befehle `reboot` und `halt` verwenden, um das System herunterzufahren, solange das System in den Runlevels 1 bis 5 ist. Jedoch nicht alle Linux Betriebssysteme unterstützten diese Funktion.

Sollte der Computer sich nicht selbst herunterfahren, seien Sie vorsichtig und schalten Sie den Computer nicht aus, bis eine Nachricht erscheint, dass das System angehalten wurde.

Wenn Sie dies nicht tun und den Computer ausschalten, bevor diese Meldung erscheint, kann auf einigen Partitionen noch ein Mount bestehen, was zur Korruption von Daten führen kann.

redhat

Kapitel 2.

Bootloader

Bevor Red Hat Linux auf einem System ausgeführt werden kann, muss es über ein spezielles Programm namens *Bootloader* geladen werden. Das Bootloaderprogramm ist in der Regel auf der ersten Festplatte des Systems oder einem anderen Gerät installiert und ist für das Laden der für den Linux-Kernel erforderlichen Dateien oder in manchen Fällen das Laden anderer Betriebssysteme in den Speicher verantwortlich.

2.1. Bootloader und Systemarchitektur

Jede Rechnerarchitektur, die unter Red Hat Linux ausgeführt werden kann, verwendet unterschiedliche Bootloader. Die Alpha-Architektur benutzt beispielsweise den `aboot`-Bootloader, während die Itanium-Architektur den `ELILO`-Bootloader verwendet.

In diesem Kapitel werden Befehle und Konfigurationsoptionen der beiden Bootloader besprochen, die mit Red Hat Linux für x86-Architekturen geliefert werden: GRUB und LILO.

2.2. GRUB

GNU GRand Unified Bootloader oder GRUB ist ein Programm, mit dem der Benutzer das Betriebssystem oder den Kernel auswählen kann, das bzw. der beim Systemstart geladen werden soll. Desweiteren kann der Benutzer Argumente an den Kernel übergeben.

2.2.1. GRUB und der x86-Bootprozess

In diesem Abschnitt wird die spezifische Rolle von GRUB beim Booten eines x86-Systems ausführlich beschrieben. Detaillierte Informationen zum gesamten Bootprozess finden Sie unter Abschnitt 1.2.

GRUB lädt sich selbst in folgenden Phasen in den Speicher:

1. *Der Stage 1 oder primäre Bootloader wird vom BIOS in den Speicher vom MBR gelesen*[1]. Der primäre Bootloader nimmt weniger als 512 Bytes Plattenplatz im MBR in Anspruch. Seine einzige Aufgabe ist das Laden des Stage 1.5 oder Stage 2 Bootloaders.
2. *Der Stage 1.5 Bootloader wird nur dann vom Stage 1-Bootloader in den Speicher eingelesen, wenn dies notwendig ist.* Für manche Hardware ist ein Zwischenschritt beim Aufrufen des Stage 2 Bootloaders erforderlich. Dies trifft manchmal zu, wenn die `/boot`-Partition 1024 Zylinder überschreitet oder im LBA-Modus verwendet wird. Der Stage 1.5 Bootloader befindet sich entweder auf der `/boot/`- Partition oder auf einem kleinen Teil des MBR und der `/boot` Partition.
3. *Der Stage 2 oder sekundäre Bootloader wird in den Speicher gelesen.* Der sekundäre Bootloader zeigt die Menü- und Befehlsumgebung von GRUB an. Mit dieser Oberfläche können Sie das zu startende Betriebssystem bzw. den Linux-Kernel auswählen, Argumente an den Kernel weiterleiten oder sich die Systemparameter wie zum Beispiel verfügbaren RAM anzeigen lassen.
4. *Der sekundäre Bootloader liest das Betriebssystem bzw. den Kernel und* `initrd` *in den Speicher.* Sobald GRUB festlegt, welches Betriebssystem gestartet werden soll, lädt er es in den Speicher und übergibt die Steuerung der Rechners an das Betriebssystem.

1. Weitere Informationen zum BIOS und MBR finden Sie unter Abschnitt 1.2.1.

Diese zum Starten von Red Hat Linux verwendete Bootmethode wird *direktes Laden* genannt, da der Bootloader das Betriebssystem direkt lädt. Zwischen dem Bootloader und dem Kernel ist keine Zwischenstufe vorhanden.

Der von den anderen Betriebssystemen verwendete Bootprozess kann von dem hier beschriebenen abweichen. Die Betriebssysteme DOS und Windows von Microsoft wie auch andere proprietäre Betriebssysteme werden mit Hilfe der Bootmethode *Verkettetes Laden* geladen. Bei dieser Methode verweist der MBR einfach auf den ersten Sektor der Partition, auf der das Betriebssystem installiert ist. Dort befinden sich die für das Starten des Betriebssystems erforderlichen Dateien.

GRUB unterstützt sowohl das direkte als auch das verkettete Laden, wodurch fast alle Betriebssysteme gestartet werden können.

Warnung

Während der Installation überschreiben DOS und Windows von Microsoft den MBR komplett und löschen somit alle vorhandenen Bootloader. Wird ein duales Bootsystem erstellt, wird empfohlen, das Betriebssystem von Microsoft zuerst zu installieren. Die entsprechenden Anweisungen hierzu finden Sie im Anhang *Installing Red Hat Linux in a Dual-Boot Environment* im *Red Hat Linux Installationshandbuch*.

2.2.2. Funktionen von GRUB

GRUB enthält zahlreiche Funktionen, die im Vergleich zu anderen für die x86-Architektur verfügbaren Bootloadern vorteilhaft sind. Nachfolgend ist eine Liste mit den wichtigsten Funktionen angeführt:

- *GRUB liefert auf x86-Rechnern eine echte befehlsbasierte Umgebung für die Phase vor dem Laden des Betriebssystems.* Dies verleiht dem Benutzer maximale Flexibilität beim Laden der Betriebssysteme mit bestimmten Optionen bzw. beim Sammeln von Informationen über das System. Viele nicht-x86-Architekturen verwenden seit Jahren prä-OS-Umgebungen, die die Steuerung des Bootprozesses des Systems von einer Befehlszeile aus ermöglichen. Einige Befehlsfunktionen stehen mit LILO oder anderen x86-Bootloadern zur Verfügung, GRUB bietet jedoch eine größere Anzahl solcher Funktionen.
- *GRUB unterstützt den Logical Block Addressing (LBA) Modus.* LBA übergibt die Adressierkonvertierung, die dazu dient, Dateien zu suchen, an die Firmware der Festplatte, und wird auf vielen IDE- und allen SCSI-Festplatten verwendet. Vor LBA stießen Bootloader auf die 1024-Zylindergrenze des BIOS, oberhalb derer das BIOS keine Dateien finden konnte. Die LBA-Unterstützung ermöglicht GRUB, Betriebssysteme von Partitionen oberhalb dieser Grenze zu booten, sofern das System-BIOS den LBA-Modus unterstützt. Die meisten modernen BIOS-Versionen unterstützen den LBA-Modus.
- *GRUB kann ext2-Partitionen lesen.* Hierdurch kann GRUB bei jedem Systemstart auf die Konfigurationsdatei `/boot/grub/grub.conf` zugreifen und die Notwendigkeit umgehen, eine neue Version des Stage 1 Bootloaders auf den MBR schreiben zu müssen, wenn die Konfiguration geändert wird. GRUB muss nur dann neu auf dem MBR installiert werden, wenn die physische Stelle der `/boot`- Partition auf der Platte verschoben wird. Detaillierte Informationen zum Installieren von GRUB auf den MBR finden Sie unter Abschnitt 2.3.

2.3. Installation von GRUB

Wenn Sie GRUB während des Installationsprozesses nicht installiert haben, können Sie ihn später installieren. Er wird automatisch zum standardmäßigen Bootloader.

Vor der Installation von GRUB sollten Sie sicherstellen, dass Sie das neueste GRUB-Paket haben. Sie können auch das GRUB-Paket von den Red Hat Linux- Installations-CD-ROMs verwenden. Weitere Informationen zum Installieren von Paketen finden Sie im Kapitel *Paket-Management mit RPM* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

Öffnen Sie nach der Installation des GRUB-Pakets einen root-Shell-Prompt, und führen Sie den Befehl `/sbin/grub-install <Speicherort>` aus, wobei *<Speicherort>* der Speicherort ist, in den der Stage 1 GRUB-Bootloader installiert werden soll.

Mit dem folgenden Befehl installieren Sie GRUB auf den MBR des Master-IDE-Geräts auf dem primären IDE-Bus: `/sbin/grub-install /dev/hda`

Beim nächsten Systemstart wird das grafische Bootloader-Menü von GRUB angezeigt, bevor der Kernel lädt.

2.4. GRUB-Terminologie

Zu den grundlegenden Kenntnissen vor der Verwendung von GRUB gehört, wie das Programm Geräte wie Festplatten und Partitionen anspricht. Diese Informationen sind insbesondere dann wichtig, wenn GRUB zum Starten mehrerer Betriebssysteme konfiguriert werden soll.

2.4.1. Gerätenamen

Nehmen Sie an, dass Ihr System mehrere Festplatten hat. Die erste Festplatte eines Systems wird von GRUB als `(hd0)`, die erste Partition auf dieser Festplatte als `(hd0,0)` und die fünfte Partition auf der zweiten Festplatte als `(hd1,4)` bezeichnet. Im Allgemeinen sieht die Konvention für die Namensgebung für Dateisysteme bei GRUB wie folgt aus:

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

Klammern und Kommata sind wichtige Elemente in den Konventionen der Gerätebezeichnungen. Der *<Gerätetyp>* gibt an, ob eine Festplatte (`hd`) oder Diskette (`fd`) angegeben wurde.

Die *<BIOS-Gerätenummer>* ist die Nummer des Geräts gemäß dem System-BIOS, die mit `0` beginnt. Die primäre IDE-Festplatte ist mit `0`, die sekundäre IDE-Festplatte mit `1` nummeriert. Diese Anordnung entspricht ungefähr der Art, in der der Linux-Kernel die Geräte nach Buchstaben anordnet, wobei sich `a` in `hda` auf `0`, `b` in `hdb` auf `1` usw. bezieht.

Anmerkung

Das Nummeriersystem von GRUB für Geräte beginnt bei `0` und nicht bei `1`. Fehler bei der Unterscheidung gehören zu den häufigsten Fehlern, die von neuen GRUB- Benutzern begangen werden.

Die *<Partitionsnummer>* bezieht sich auf die Nummer einer spezifischen Partition auf einem Plattengerät. Wie die *<BIOS-Gerätenummer>* beginnt die Nummerierung der Partitionen bei `0`. Während die meisten Partitionen mit Nummern bezeichnet werden, werden sie durch Buchstaben wie `a` oder `c` angegeben, wenn Ihr System BSD-Partitionen verwendet.

Bei GRUB gelten die folgenden Regeln für die Bezeichnung von Geräten und Partitionen:

- Unabhängig davon, ob es sich bei den Festplatten um IDE- oder SCSI-Festplatten handelt, beginnen alle Festplatten mit `hd`. Disketten dagegen beginnen mit `fd`.
- Um ein ganzes Gerät ohne Berücksichtigung seiner Partitionen anzugeben, lassen Sie einfach das Komma und die Partitionsnummer weg. Dies ist dann wichtig, wenn Sie GRUB anweisen, den

MBR für eine bestimmte Festplatte zu konfigurieren. Beispielsweise gibt `(hd0)` den MBR auf dem ersten Gerät an, und `(hd3)` gibt den MBR auf dem vierten Gerät an.

- Wenn ein System über mehrere Festplatten verfügt, muss deren Startreihenfolge gemäß BIOS bekannt sein. Dies ist sehr einfach, wenn das System nur IDE- oder SCSI-Festplatten besitzt. Besitzt es jedoch mehrere, sind die Dinge etwas komplizierter.

2.4.2. Dateinamen und Blocklisten

Wenn Sie Befehle in Bezug auf eine Datei in GRUB eingeben, wie z.B. eine Menüliste, die zu verwenden ist, wenn das Booten von mehreren Betriebssystemen ermöglicht werden soll, muss die Datei sofort nach der Angabe des Geräts und der Partition spezifiziert werden.

Ein Beispiel für die Angabe einer Datei in einem absoluten Dateinamen:

```
(<type-of-device><bios-device-number>,<partition-number>)/path/to/file
```

In den meisten Fällen geben Benutzer Dateien mit dem Verzeichnispfad auf der entsprechenden Partition und den Dateinamen an.

GRUB können weiterhin Dateien angegeben werden, die nicht im Dateisystem angezeigt werden. Ein Beispiel ist ein Kettenloader, der sich in den ersten wenigen Blöcken einer Partition befindet. Zur Angabe von solchen Dateien muss eine *Blockliste* zur Verfügung gestellt werden, die GRUB Block für Block angibt, an welcher Stelle der Partition sich die Datei befindet. Da eine Datei aus mehreren Blocksätzen bestehen kann, werden die Blocklisten auf eine ganz bestimmte Art und Weise geschrieben. Jeder Teilabschnitt einer Datei wird durch einen Offset an Blöcken gefolgt von einer Anzahl an Blöcken beschrieben, und die Abschnitte werden in Reihenfolge und durch Kommas getrennt aufgelistet.

Folgend ist ein Beispiel einer Blockliste:

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

Diese Blockliste weist GRUB an, eine Datei zu verwenden, die mit dem ersten Block auf der Partition beginnt und die Blöcke 0 bis 49, 99 bis 124 und 199 verwendet.

Blocklisten schreiben zu können ist dann sehr nützlich, wenn GRUB zum Laden von Betriebssystemen verwendet wird, die das verkettete Laden benutzen, wie z.B. Microsoft Windows. Sie können den Offset an Blöcken weglassen, wenn Sie bei Block 0 starten. Beispiel: die Kettenlade-Datei auf der ersten Partition der ersten Festplatte würde somit folgenden Namen besitzen:

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

Im Folgenden wird der Befehl `chainloader` mit einer ähnlichen Blocklisten-Bezeichnung in der GRUB-Befehlszeile gezeigt, nachdem Sie als root das korrekte Gerät und Partition eingestellt haben:

```
chainloader +1
```

2.4.3. root-Dateisystem von GRUB

Der Begriff "root-Dateisystem" bei GRUB mag verwirren. Dabei ist zu beachten, dass das root-Dateisystem von GRUB nichts mit dem root-Dateisystem von Linux gemeinsam hat.

Das root-Dateisystem von GRUB ist die root-Partition für ein bestimmtes Gerät. GRUB verwendet diese Angabe u.a., um das Gerät zu mounten und Dateien von diesem Gerät zu laden.

Nachdem GRUB die root-Partition geladen hat, die unter Red Hat Linux der `/boot`-Partition entspricht und den Linux-Kernel enthält, kann der Befehl `kernel` mit dem Speicherort der Kerneldatei

als Option ausgeführt werden. Sobald der Linux-Kernel bootet, stellt er ein eigenes root-Dateisystem ein. Das ursprüngliche root-Dateisystem von GRUB und die Mounts sind bereits vergessen: Sie dienten lediglich dem Booten der Kerneldatei.

Weitere Informationen zu den Befehlen `root` und `kernel` finden Sie unter Abschnitt 2.6.

2.5. GRUB-Oberflächen

GRUB bietet drei Oberflächen, welche unterschiedliche Stufen an Funktionalität bieten. Jede einzelne Oberfläche ermöglicht das Booten des Linux Kernels und anderen Betriebssystemen.

Dabei handelt es sich um folgende Schnittstellen:

Menüoberfläche

Wurde GRUB vom Red Hat Linux-Installationsprogramm automatisch konfiguriert, wird diese Oberfläche standardmäßig angezeigt. Sie besitzt ein Menü mit Betriebssystemen oder Kerneln, die mit ihren eigenen Bootbefehlen vorkonfiguriert als Liste nach Namen geordnet angezeigt werden. Anhand der Pfeiltasten können Sie eine andere Option als die Standardauswahl wählen. Drücken Sie die [Enter-Taste], um diese Option zu booten. Es kann auch eine Zeit eingestellt sein, nach der GRUB mit dem Laden der Standardoption beginnt.

Drücken Sie in der Menüoberfläche die Taste [e], um die Oberfläche des Eintrag-Editors aufzurufen, bzw. die Taste [c], um eine Befehlszeilenoberfläche zu laden.

Weitere Informationen zum Konfigurieren dieser Oberfläche finden Sie unter Abschnitt 2.7.

Oberfläche Menüeintrag-Editor

Um auf den Menüeintrag-Editor zuzugreifen, drücken Sie die Taste [e] im Bootloader-Menü. Die GRUB-Befehle für diesen Eintrag werden hier angezeigt, und die Benutzer haben die Möglichkeit, diese Befehlszeilen vor dem Starten des Betriebssystems durch Hinzufügen einer Befehlszeile ([o] fügt die neue Zeile nach der aktuellen Zeile ein, [O] davor), durch Bearbeiten ([e]) oder Löschen ([d]) zu ändern.

Nachdem die gewünschten Änderungen an den Zeilen vorgenommen wurden, können Sie die Taste [b] drücken, um die Befehle auszuführen und das Betriebssystem zu booten. Mittels der Taste [Esc] werden die Änderungen verworfen und die Standardmenüoberfläche geladen. Über die Taste [c] wird die Befehlszeilenoberfläche geladen.

Tipp

Weitere Informationen zum Ändern der Runlevel mit GRUB unter Verwendung des Menüeintrag-Editors finden Sie unter Abschnitt 2.10.

Befehlszeilenoberfläche

Die Befehlszeile ist die einfachste GRUB-Oberfläche, die gleichzeitig auch die größte Kontrolle bietet. Die Befehlszeile ermöglicht es, alle relevanten GRUB-Befehle einzugeben und diese anschließend durch Drücken der [Enter-Taste] auszuführen. Diese Oberfläche bietet einige erweiterte, shell-ähnliche Funktionen, einschließlich der kontextbasierten Verwendung der Taste [Tab] zur Zeilenvervollständigung sowie den Kombinationen mit der Taste [Strg] bei der Eingabe von Befehlen (beispielsweise [Strg]-[a], wenn Sie zum Anfang einer Zeile springen möchten, und [Strg]-[e], wenn Sie zum Ende einer Zeile springen möchten). Darüber hinaus funktionieren die Tasten [Pos1], [Ende] und [Entf] wie in der `bash`-Shell.

Eine Liste mit den gebräuchlichsten Befehlen finden Sie unter Abschnitt 2.6.

2.5.1. Reihenfolge der Oberflächen

Wenn die GRUB-Umgebung mit dem Laden des Bootloaders der zweiten Phase beginnt, sucht diese nach der Konfigurationsdatei. Wird die Konfigurationsdatei gefunden, wird diese verwendet, um die Menüliste zu erstellen und die Bootmenüoberfläche anzuzeigen.

Kann die Konfigurationsdatei nicht gefunden oder nicht gelesen werden, lädt GRUB die Befehlszeilenoberfläche, in welcher der Benutzer Befehle eingeben kann, um den Bootprozess abzuschliessen.

Wenn die Konfigurationsdatei ungültig ist, druckt GRUB den Fehler und fordert zur Eingabe auf. Dies kann sehr nützlich sein, da die Benutzer auf diese Weise genau sehen, wo das Problem aufgetreten ist, und die Datei entsprechend korrigieren können. Durch Drücken einer beliebigen Taste wird die Menüoberfläche erneut geladen, wo die entsprechende Menüoption bearbeitet und der Fehler gemäß der Angabe von GRUB korrigiert werden kann. Schlägt die Korrektur fehl, meldet GRUB den Fehler, und die Menüoberfläche wird neu geladen.

2.6. GRUB-Befehle

GRUB bietet eine Reihe nützlicher Befehle auf seiner Befehlszeilenoberfläche. Nach dem Namen einiger dieser Befehle können Optionen eingegeben werden. Diese Optionen sind vom Befehl und anderen Optionen auf derselben Zeile durch Leerzeichen zu trennen.

In der folgenden Liste sind die nützlichsten Befehle aufgeführt:

- `boot` — Bootet das Betriebssystem oder den Kettenloader, das/der zuvor angegeben und geladen wurde.
- `chainloader` <*Dateiname*> — Lädt die angegebene Datei als Kettenloader. Um die Datei im ersten Sektor der angegebenen Partition zu erfassen, verwenden Sie `+1` als Name der Datei.
- `displaymem` — Zeigt den derzeitigen Speicherbedarf entsprechend den Informationen des BIOS an. Dies ist besonders zum Ermitteln des RAM eines Systems vor dem Booten nützlich.
- `initrd` <*Dateiname*> — Ermöglicht die Angabe einer initialen RAM-Disk, die beim Booten verwendet wird. Eine `initrd` ist erforderlich, wenn der Kernel bestimmte Module zum ordnungsgemäßen Starten benötigt. Dies ist zum Beispiel dann der Fall, wenn die root-Partition mit dem Dateisystem ext3 formatiert wurde.
- `install` <*Stage-1*> <*Installationsdiskette*> <*Stage-2*> `p` <*Konfigurationsdatei*> — Installiert GRUB in den System-MBR.

  Beim Verwenden des Befehls `install` muss der Benutzer folgendes angeben:

  - <*stage-1*> — Spezifiziert Gerät, Partition, und Datei, wo das erste Boot-Loader Image gefunden werden kann, z.B. `(hd0,0)/grub/stage1`.
  - <*install-disk*> — Gibt die Platte an, auf welcher der Boot-Loader der ersten Phase installiert sein sollte, z.B. `(hd0)`.
  - <*stage-2*> — Übergibt dem Boot-Loader der ersten Phase den Ort, an welchem sich der Boot-Loader der zweiten Phase befindet, z.B. `(hd0,0)/grub/stage2`.
  - `p` <*config-file*> — Diese Option sagt dem `install` Befehl, dass dieser nach der Konfigurationsdatei des Menüs, durch <*config-file*> spezifiziert, suchen soll. Ein Beispiel eines gültigen Pfads zur Konfigurationsdatei ist `(hd0,0)/grub/grub.conf`.

Warnung

Der Befehl `install` überschreibt alle Informationen im MBR. Wird der Befehl ausgeführt, gehen alle Angaben verloren (außer GRUB-Daten), die zum Booten anderer Betriebssysteme verwendet werden.

- `kernel <Kernel-Dateiname> <Option-1> <Option-N>` — Gibt die Kernel-Datei an, die vom GRUB-root-Dateisystem geladen werden soll, wenn das Betriebssystem mit Hilfe des direkten Ladens gestartet werden soll. Nach dem Befehl `kernel` können Optionen angegeben und beim Laden dem Kernel übergeben werden.

  Bei Red Hat Linux wird der Befehl `kernel` beispielsweise wie folgt angezeigt:
  ```
  kernel /vmlinuz root=/dev/hda5
  ```
  Diese Zeile gibt an, dass die Datei `vmlinuz` vom GRUB-root-Dateisystem geladen wird (z.B. `(hd0,0)`). Weiterhin wird dem Kernel eine Option übergeben, die angibt, dass sich das root-Dateisystem für den Linux-Kernel beim Laden auf `hda5`, der fünften Partition auf der ersten IDE-Festplatte, befinden sollte. Bei Bedarf können nach dieser Option weitere Optionen angegeben werden.

- `root <Gerät-und-Partition>` — Konfiguriert die root-Partition von GRUB als diese Kombination von Gerät und Partition (z.B. `(hd0,0)`) und mountet die Partition, so dass Dateien gelesen werden können.

- `rootnoverify <Gerät-und-Partition>` — Entspricht dem Befehl `root`, mountet jedoch nicht die Partition.

Darüber hinaus stehen noch andere Befehle zur Verfügung. Geben Sie `info grub` ein, um eine vollständige Liste zu erhalten.

2.7. Menükonfigurationsdatei von GRUB

Die Konfigurationsdatei (`/boot/grub/grub.conf`), die verwendet wird, um die Liste der zu bootenden Betriebssysteme in der Menüoberfläche von GRUB zu erstellen, ermöglicht dem Benutzer im Wesentlichen, eine festgelegte Reihe von Befehlen auszuwählen. Dabei können die in Abschnitt 2.6 angeführten Befehle sowie einige spezielle Befehle verwendet werden, die ausschließlich in der Konfigurationsdatei zur Verfügung stehen.

2.7.1. Spezielle Konfigurationsdateibefehle

Die folgenden Befehle können ausschließlich in der Menükonfigurationsdatei von GRUB verwendet werden:

- `color <normale-Farbe> <ausgewählte-Farbe>` — Ermöglicht, spezifische, im Menü zu verwendende Farben einzustellen, wobei zwei Farben als Vorder- und Hintergrundfarben konfiguriert werden. Verwenden Sie einfache Farbbezeichnungen wie `red/black`. Zum Beispiel:
  ```
  color red/black green/blue
  ```
- `default <Titel>` — Der standardmäßige Eintrag, der geladen wird, wenn die Menüoberfläche durch Zeitüberschreitung abbricht.
- `fallback <Titel>` — Wenn verwendet: der Eintrag, der verwendet wird, wenn der erste Versuch fehlschlug.
- `hiddenmenu` — Wenn verwendet: verhindert, dass die GRUB-Menüoberfläche angezeigt wird und lädt den `default` Eintrag, wenn der `timeout`-Zeitraum abläuft. Der Benutzer kann das standardmäßige GRUB-Menü anzeigen, indem er die Taste [Esc] drückt.
- `password <Passwort>` — Wenn verwendet: verhindert, dass der Benutzer, der das Passwort nicht kennt, die Einträge für diese Menüoption bearbeitet.

Nach dem Befehl `password <Passwort>` können Sie auch eine alternative Menükonfigurationsdatei angeben, so dass - wenn das Passwort bekannt ist - GRUB den zweiten Schritt des Bootloaders erneut startet und diese alternative Konfigurationsdatei verwendet, um das Menü zu erstellen. Wenn diese alternative Datei nicht in den Befehl eingeschlossen wird, dann könnte ein Benutzer, der das Passwort kennt, die aktuelle Konfigurationsdatei bearbeiten.

- `timeout` — Wenn verwendet: stellt die Zeit in Sekunden ein, bevor GRUB den Eintrag lädt, der von `default` vorgegeben wird.
- `splashimage` — Gibt den Speicherort des Splashscreen-Images an, das verwendet wird, wenn GRUB bootet.
- `title` — Stellt einen Titel ein, der einer bestimmten Gruppe von Befehlen zugeordnet ist, die für das Laden eines Betriebssystems benutzt werden.

Das Zeichen `#` am Anfang einer Zeile kann verwendet werden, um Kommentare in die Menükonfigurationsdatei einzufügen.

2.7.2. Struktur der Konfigurationsdatei

Die Konfigurationsdatei der Menüoberfläche von GRUB ist `/boot/grub/grub.conf`. Die Befehle für das Festlegen der allgemeinen Einstellungen für die Menüoberfläche werden am Anfang der Datei platziert. Darauf folgen die verschiedenen Einträge für jedes der im Menü genannten Betriebssysteme oder Kernel.

Eine sehr einfache GRUB-Menükonfigurationsdatei, die entweder Red Hat Linux oder Microsoft Windows 2000 bootet, könnte wie folgt aussehen:

```
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz

# section to load linux
title Red Hat Linux (2.4.18-5.47)
        root (hd0,0)
        kernel /vmlinuz-2.4.18-5.47 ro root=/dev/sda2
        initrd /initrd-2.4.18-5.47.img

# section to load Windows 2000
title windows
        rootnoverify (hd0,0)
        chainloader +1
```

Diese Datei würde GRUB anweisen, ein Menü mit Red Hat Linux als standardmäßigem Betriebssystem zu erstellen, was nach 10 Sekunden automatisch gebootet wird. Gegeben sind zwei Abschnitte - einer für jeden Betriebssystemeintrag - mit spezifischen Befehlen für die Partitionstabelle dieses Systems.

Anmerkung

Der Standardwert ist als Nummer angegeben, die sich auf die erste `title`-Zeile bezieht, auf die GRUB stößt. Wenn Sie `windows` als Standard festlegen möchten, ändern Sie `default=0` in `default=1`.

Die Konfiguration einer GRUB-Menükonfigurationsdatei für das Starten mehrerer Betriebssysteme übersteigt den Umfang dieses Kapitels. Für eine Liste zusätzlicher Ressources, sehen Sie Abschnitt 2.11.

2.8. LILO

LILO ist das Akronym für *LI*nux *LO*ader und wurde während vieler Jahre verwendet, um Linux auf x86- Systemen zu starten. Obwohl GRUB jetzt der Standardbootloader ist, bevorzugen manche Personen LILO, da sie mit dem Programm vertraut sind. Andere wiederum verwenden ihn, weil GRUB möglicherweise beim Starten gewisser Hardware Probleme bereitet.

2.8.1. LILO und der x86-Bootprozess

In diesem Abschnitt wird die spezifische Rolle von LILO beim Booten eines x86-Systems ausführlich beschrieben. Detaillierte Informationen zum gesamten Bootprozess finden Sie unter Abschnitt 1.2.

LILO wird fast genauso wie GRUB in den Speicher geladen, mit dem Unterschied, dass er nur ein zweistufiger Loader ist.

1. *Der Stage 1 oder primäre Bootloader wird vom BIOS aus dem MBR in den Speicher gelesen*[2]. Der primäre Bootloader nimmt weniger als 512 Bytes Plattenplatz im MBR in Anspruch. Seine einzige Aufgabe ist das Laden des Stage 2 Bootloaders sowie das Übergeben der Geometriedaten der Platte an diesen.
2. *Der Stage 2- oder sekundäre Bootloader wird in den Speicher gelesen.* Der sekundäre Bootloader zeigt den Einstiegsbildschirm von Red Hat Linux an. Mit diesem Bildschirm können Sie das Betriebssystem bzw. den Linux-Kernel auswählen, das/der gestartet werden soll.
3. *Der Stage 2 Bootloader liest das Betriebssystem bzw. den Kernel und* `initrd` *in den Speicher.* Sobald LILO festlegt, welches Betriebssystem gestartet werden soll, lädt er es in den Speicher und übergibt die Steuerung der Rechners an das Betriebssystem.

Wenn der Stage 2 Bootloader in den Arbeitsspeicher geladen ist, zeigt LILO den Red Hat Linux-Einstiegsbildschirm mit den verschiedenen Betriebssystemen oder Kernel an, die zum Starten konfiguriert wurden. Wenn Sie nur Red Hat Linux installiert haben und keine Änderungen an der Konfigurationsdatei von LILO vorgenommen haben, wird nur **linux** als Option angezeigt. Sollte das System mehrere Prozessoren haben, wird eine **linux-up** Option für den Einzelprozessor Kernel und **linux** für den SMP Kernel vorhanden sein. Ist LILO dazu konfiguriert, andere Betriebssysteme zu booten, erscheinen diese Bootoptionen auch auf dem Bildschirm.

Die Pfeiltasten ermöglichen Ihnen das Betriebssystem zu markieren, und durch Drücken der [Enter-Taste] wird der Bootvorgang gestartet.

Um Zugriff zu einem `boot:` Prompt zu erhalten, drücken Sie [Strg]-[X].

2.8.2. LILO vs. GRUB

Im Großen und Ganzen gesehen funktioniert LILO wie GRUB, mit Ausnahme folgender drei Hauptunterschiede:

- Die Befehlsoberfläche ist nicht interaktiv.
- Er speichert Informationen über den Speicherort des Kernels oder anderer zu ladenden Betriebssysteme im MBR.

2. Weitere Informationen zum BIOS und MBR finden Sie unter Abschnitt 1.2.1.

- Er kann keine ext2-Partitionen lesen.

Der erste Punkt bedeutet, dass der Befehls-Prompt für LILO nicht interaktiv ist und nur Befehle mit Argumenten zulässt.

Die letzten beiden Punkte bedeuten, dass Sie nach Änderungen an der Konfigurationsdatei von LILO oder der Installation eines neuen Kernels den Stage 1 LILO Bootloader mit folgendem Befehl neu in den MBR schreiben müssen:

```
/sbin/lilo -v -v
```

Dies stell ein größeres Risiko als die GRUB-Methode dar, da ein nicht richtig konfigurierter MBR zur Folge hat, dass das System nicht mehr booten kann. Sollte bei GRUB die Konfigurationsdatei fehlerhaft konfiguriert sein, so startet er einfach nur die Befehlszeilenoberfläche, wo der Benutzer das System manuell booten kann.

Tipp

Wenn Sie den Kernel mit Hilfe des **Red Hat Update Agent** aktualisieren, wird der MBR automatisch aktualisiert. Weitere Informationen zu RHN finden Sie Online unter folgender URL https://rhn.redhat.com

2.9. Optionen in `/etc/lilo.conf`

Die LILO Konfigurationsdatei heisst `/etc/lilo.conf`. Der Befehl `/sbin/lilo` benutzt diese, um zu bestimmen, welche Information zum MBR geschrieben werden sollen.

Warnung

Wenn Sie vorhaben, `/etc/lilo.conf` zu bearbeiten, sollten Sie unbedingt eine Sicherungskopie der Datei anlegen, ehe Sie die Änderungen vornehmen. Stellen Sie außerdem sicher, dass Sie über eine funktionierende Bootdiskette verfügen, um bei Problemen das System starten und den MBR ändern zu können. Weitere Informationen zum Erstellen einer Bootdiskette finden Sie unter den man-Seiten zu `mkbootdisk`.

Die Datei `/etc/lilo.conf` wird vom Befehl `/sbin/lilo` verwendet, um festzulegen, welches Betriebssystem oder welcher Kernel gestartet wird, wie auch um den eigenen Installationsort zu ermitteln.

Die Datei `/etc/lilo.conf` könnte beispielsweise so aussehen:

```
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
```

Im obigen Beispiel ist ein System dargestellt, das zum Booten zweier Betriebssysteme konfiguriert ist: Red Hat Linux und DOS. Einige Zeilen dieser Datei werden im Folgenden etwas näher betrachtet:

- `boot=/dev/hda` — Weist LILO an, sich selbst auf der ersten Festplatte des ersten IDE-Controllers zu installieren.
- `map=/boot/map` — Sucht die Zuordnungsdatei. Normalerweise sollten hier keine Änderungen vorgenommen werden.
- `install=/boot/boot.b` — Weist LILO an, die angegebene Datei als neuen Bootsektor zu installieren. Normalerweise sollten hier keine Änderungen vorgenommen werden. Wenn die `install`-Zeile fehlt, geht LILO davon aus, dass `/boot/boot.b` standardmäßig zu verwenden ist.
- `prompt` — Weist LILO an, alle Verweise in der `message`-Zeile anzuzeigen. Es wird davon abgeraten, die `prompt`-Zeile zu entfernen. Wenn Sie dies dennoch tun, können Sie nach wie vor einen Prompt aufrufen, indem Sie die [Umschalt]-Taste gedrückt halten, während der Rechner hochfährt.
- `timeout=50` — Legt den Zeitraum fest, den LILO auf Benutzereingaben wartet, ehe er mit dem Starten des `default`-Zeileneintrags fortfährt. Dies wird in Zehntelsekunden gemessen. 50 ist der Standardwert.
- `message=/boot/message` — Verweist auf den Bildschirm von LILO, auf dem Sie das zu startende Betriebssystem bzw. den Kernel auswählen.
- `lba32` — Beschreibt LILO die Festplattengeometrie. Ein anderer üblicher Eintrag ist `linear`. Sie sollten diese Zeile nicht ändern, es sei denn, Sie verfügen über die notwendigen Kenntnisse. Ansonsten könnten Sie Ihr System in einen nicht mehr startfähigen Status versetzen.
- `default=linux` — Verweist auf das Betriebssystem, das LILO standardmäßig aus den unterhalb dieser Zeile genannten Optionen starten soll. Der Name `linux` bezieht sich auf die untere Zeile `label` in allen Bootoptionen.
- `image=/boot/vmlinuz-2.4.0-0.43.6` — Gibt den Linux-Kernel an, der mit genau diesen Bootoptionen gestartet werden soll.
- `label=linux` — Benennt die Betriebssystemoption im LILO-Bildschirm. In diesem Fall handelt es sich auch um den Namen, auf den die Zeile `default` verweist.
- `initrd=/boot/initrd-2.4.0-0.43.6.img` — Verweist auf das *initiale RAM-Disk*-Image, das zum Zeitpunkt des Bootens verwendet wird, um die Geräte wirklich zu initialisieren und zu starten, die das Booten des Kernels ermöglichen. Die initiale RAM-Disk ist eine Sammlung von rechnerspezifischen Treibern, die zum Betreiben von SCSI- Karten, Festplatten oder anderer Geräte benötigt wird, die zum Laden des Kernels erforderlich sind. Versuchen Sie niemals, initiale RAM-Disks auf mehreren Rechnern gemeinsam zu nutzen.
- `read-only` — Gibt an, dass die root-Partition (siehe die Zeile `root` unten) schreibgeschützt ist und während des Bootprozesses nicht geändert werden kann.
- `root=/dev/hda5` — Weist LILO an, welche Plattenpartition als root-Partition verwendet werden soll.

2.10. Ändern von Runleveln zum Zeitpunkt des Bootens

Unter Red Hat Linux können Sie den Standard-Runlevel zum Zeitpunkt des Bootens ändern.

Wenn Sie LILO verwenden, greifen Sie auf den Prompt `boot:` zu, indem Sie die Tasten [Strg]-[X] drücken. Geben Sie anschließend Folgendes ein:

`linux <`*`runlevel-number`*`>`

Ersetzen Sie in diesem Befehl <*Runlevel-Nummer*> entweder durch die Nummer des Runlevels, in dem Sie booten möchten (**`1`** bis **`5`**), oder durch das Wort **`single`** oder **`emergency`**.

Falls Sie GRUB verwenden, führen Sie diese Schritte aus:

- Wählen Sie auf dem grafischen GRUB-Bootloader-Bildschirm das **Red Hat Linux**-Bootlabel aus, und drücken Sie zur Bearbeitung [e].
- Gehen Sie mit der Pfeiltaste zur Kernelzeile hinunter und drücken zur Bearbeitung [e].
- Geben Sie am Prompt die Nummer des Runlevels, auf dem Sie booten möchten (**`1`** bis **`5`**), das Wort **`single`** oder **`emergency`** ein, und drücken Sie dann die [Enter-Taste].
- Sie kehren nun zum GRUB-Bildschirm mit den Kernel- Informationen zurück. Drücken Sie die [b]-Taste, um das System zu starten.

Weitere Informationen zu Runleveln finden Sie unter Abschnitt 1.4.1.

2.11. Zusätzliche Ressourcen

Dieses Kapitel stellt lediglich eine Einführung in GRUB und LILO dar. Weitere Informationen über die Funktionsweise von GRUB und LILO finden Sie in folgenden Ressourcen.

2.11.1. Installierte Dokumentation

- `/usr/share/doc/grub-`<*version-number*>`/` — Dieses Verzeichnis enthält wertvolle Informationen über die Verwendung und Konfiguration von GRUB. <*version-number*> im Pfad zu dieser Datei entspricht der Version des installierten GRUB Pakets.
- Die Info-Seite von GRUB, auf die mit Hilfe des Befehls `info grub` zugegriffen werden kann, enthält eine Einführung, ein Referenzhandbuch für Benutzer, ein Referenzhandbuch für Programmierer sowie ein FAQ-Dokument zu GRUB und seiner Verwendung.
- `/usr/share/doc/lilo-`<*version-number*>`/` — Dieses Verzeichnis enthält viele Informationen über die Verwendung und Konfiguration von LILO. Besondere Aufmerksamkeit verdient das Unterverzeichnis `doc/` mit der informativen Postscriptdatei `User_Guide.ps`. <*version-number*> im Pfad zu dieser Datei entspricht der Version des installierten LILO Pakets.

2.11.2. Hilfreiche Websites

- http://www.gnu.org/software/grub — Die Homepage des GNU-GRUB-Projekts. Hier sind Informationen über die Entwicklung von GRUB und ein FAQ-Dokument enthalten.
- http://www.uruk.org/orig-grub — Die ursprüngliche GRUB-Dokumentation, bevor das Projekt zur weiteren Entwicklung an die Free Software Foundation übergeben wurde.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Multiboot-with-GRUB.html — Behandelt verschiedene Verwendungen für GRUB, einschließlich das Booten von nicht-Linux-Betriebssystemen.

- http://www.linuxgazette.com/issue64/kohli.html — Eine Einführung über die Konfiguration von GRUB auf einem System und ein Überblick der Befehlszeilenoptionen von GRUB.
- http://www.tldp.org/HOWTO/mini/LILO.html — In diesem mini-HOWTO werden die verschiedenen Verwendungsweisen von LILO besprochen, u.a. das Booten von nicht-Linux-Betriebssystemen.

redhat

Kapitel 3.

Struktur des Dateisystems

3.1. 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 Sicherheitskonzept interagiert, hängt davon ab, wie es die Dateien in einem primären Speicherelement (meist ein Festplattenlaufwerk) speichert. Es ist aus mehreren Gründen sehr wichtig, dass Benutzern und Programmen ein gemeinsamer Leitfaden zur Verfügung steht, aus dem hervorgeht, wo Dateien gelesen und geschrieben werden können.

Ein Dateisystem kann aus der Sicht zweier verschiedener Dateikategorien betrachtet werden:

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

Gemeinsam genutzte Dateien sind Dateien, auf die verschiedene Hosts zugreifen können, während *nicht gemeinsam genutzte* Dateien anderen Hosts nicht zur Verfügung stehen. *Variable* Dateien können jederzeit ohne Einwirken geändert werden; *statische* Dateien, wie schreibgeschützte Dokumentationen oder Binärdateien bleiben ohne direkten oder indirekten Eingriff des Systemadministrators unverändert.

Diese Betrachtungsweise hilft beim Verständnis der Zugriffsoptionen zusammen, die für das entsprechende Verzeichnis gewählt wurde. Die Art, wie das Betriebssystem und seine Benutzer die Dateien verwenden, bestimmt somit auch das Verzeichnis, in dem sie abgelegt werden. Und ob dieses Verzeichnis schreibgeschützt gemountet wird, mit Schreib- und Lesezugriff, und welche Zugriffsrechte für seine Dateien erteilt werden. Ausschlaggebend ist die oberste Organisationsstufe, da der Zugriff auf die darunterliegenden Verzeichnisse eingeschränkt werden kann bzw. sich unter Umständen Sicherheitsprobleme ergeben, wenn diese Stufe nicht organisiert bzw. oder eine allgemein nutzbare Struktur hat.

Eine Struktur hat jedoch nur als Standardstruktur einen Sinn, denn konkurrierende Strukturen können mehr Probleme bereiten als lösen. Aus diesem Grund hat sich Red Hat für die am meisten verbreitete Dateisystemstruktur entschieden und diese auch nur insofern erweitert, als damit innerhalb von Red Hat Linux verwendete Dateien angepasst wurden.

3.2. Übersicht über den Dateisystem-Hierarchiestandard (FHS)

Red Hat ist an das *Filesystem Hierarchy Standard* (*FHS*) - dem Dateisystem-Hierarchiestandard gebunden. Dabei handelt es sich um ein gemeinsam mit anderen Institutionen erarbeitetes Dokument, in dem die Namen und Speicherstellen vieler Dateien und Verzeichnisse festgelegt sind.

Das aktuelle FHS-Dokument ist die maßgebende Referenz für alle FHS-konformen Dateisystem, wobei der Standard jedoch viele Bereiche undefiniert oder erweiterbar lässt. In diesem Abschnitt geben wir Ihnen einen Überblick über diesen Standard und eine Beschreibung jener Bereiche des Dateisystems, die vom Standard nicht erfasst werden.

Den vollständigen Standard finden Sie unter:

http://www.pathname.com/fhs

Die Erfüllung dieses Standards setzt einiges voraus, aber die beiden wichtigsten Aspekte sind sicherlich die Kompatibilität mit anderen Systemen und die Möglichkeit, eine `/usr/`-Partition schreibge-

schützt zu mounten, da sie gmeinsam genutzte ausführbare Dateien enthält und daher keine Änderungen durch den Benutzer vorgenommen werden sollten. Da /usr/ schreibgeschützt gemountet ist, besteht die Möglichkeit, sie über die CD-ROM oder rüber einen schreibgeschützten NFS-Mount von einem anderen Rechner aus zu mounten.

3.2.1. FHS-Organisation

Die hier beschriebenen Verzeichnisse und Dateien stellen nur eine kleine Teilmenge der im Dokument zum Dateisystemstandard angegebenen Verzeichnisse und Dateien dar. Vollständige Informationen finden Sie im neuesten Dokument zum Dateisystemstandard FHS.

3.2.1.1. Das /dev/-Verzeichnis

Das /dev/-Verzeichnis enthält Dateisystemeinträge, die die an das System angeschlossenen Geräte wiedergeben. Diese Dateien sind für das einwandfreie Funktionieren des Systems unerlässlich.

3.2.1.2. Das /etc/-Verzeichnis

Das /etc/-Verzeichnis ist für lokale Konfigurationsdateien Ihres Rechners reserviert. Unter /etc/ dürfen keine Binärdateien abgelegt werden. Sämtliche Binärdateien, die zu einem früheren Zeitpunkt in /etc/ abgelegt wurden, müssen nun nach /sbin/ oder evtl. /bin/ verschoben werden.

Die Verzeichnisse X11/ und skel/ sind Unterverzeichnisse von /etc/:

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

Im /etc/X11/-Verzeichnis werden X11- Konfigurationsdateien, wie z.B. XF86Config, abgelegt Im /etc/skel/-Verzeichnis werden Benutzerdateien- Gerippe abgelegt. Wenn ein neuer Benutzer hinzukommt, dienen sie dazu, ein Home-Verzeichnis anzulegen.

3.2.1.3. Das /lib/-Verzeichnis

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

3.2.1.4. Das /mnt/-Verzeichnis

Das /mnt/-Verzeichnis ist für vorübergehend gemountete Dateisysteme wie CD-ROMs und Disketten.

3.2.1.5. Das /opt/-Verzeichnis

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

Für Pakete, deren Dateien nicht über das ganze Dateiystem verteilt abgelegt werden sollen, stellt /opt/ ein logisches und überschaubares organisatorisches System unter dem Verzeichnis dieses Pakets zur Verfügung. Für den Systemadministrator bedeutet dies eine einfache Art und Weise, die Rolle jeder Datei innerhalb eines bestimmten Pakets zu bestimmen.

Wenn z.B. ein besimmtes Softwarepaket, das in `/opt/` abgelegt ist, `sample` heißt, dann können alle zugehörigen Dateien in Verzeichnisse innerhalb `/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/` oder `man/` u.ä. aufweisen.

3.2.1.6. Das `/proc/`-Verzeichnis

Das `/proc/`-Verzeichnis enthält spezielle Dateien, die entweder Informationen zum Kernel schicken oder sie vom Kernel erhalten.

Aufgrund der großen Anzahl verfügbarer Daten in `/proc/` und der vielen Verwendungsmöglichkeiten dieses Verzeichnisses im Zusammenhang mit dem Kernel, wurde diesem Thema ein ganzes Kapitel gewidmet. Weitere Informationen hierzu finden Sie unter Kapitel 5.

3.2.1.7. Das `/sbin/`-Verzeichnis

Das `/sbin/`-Verzeichnis enthält die ausführbaren Dateien , die nur vom root-Benutzer ausgeführt werden können. Die ausführbaren Dateien in `/sbin/` dienen ausschließlich dem Booten und Mounten von `/usr/` sowie den Wiederherstellungsvorgängen innerhalb des Systems. FHS bedeutet:

> "`/sbin/` enthält typischerweise Dateien, die zum Booten des Systems unerlässlich sind, sowie Binärdateien in `/bin/`. Jede nach dem Mounten von `/usr/` verwendete ausführbare Datei (sofern keine Probleme auftreten) sollte in `/usr/sbin/` abgelegt werden. Rein lokale Systemverwaltungs-Binärdateien sollten in `/usr/local/sbin/` abgelegt werden."

Zumindest die folgenden Programme sollten sich also in `/sbin/` befinden:

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

3.2.1.8. Das `/usr/`-Verzeichnis

Im `/usr/`-Verzeichnis werden Dateien abgelegt, die allen Benutzern auf eine Site zur Verfügung gestellt werden. Das `/usr/`-Verzeichnis verfügt normalerweise über eine eigene Partition, bei der es möglich sein sollte, sie schreibgeschützt zu mounten. Zumindest folgende Verzeichnisse sollten Unterverzeichnisse von `/usr/` sein:

```
/usr
  |- bin/
  |- dict/
  |- doc/
  |- etc/
  |- games/
```

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

Das `bin/`-Verzeichnis enthält ausführbare Dateien, `dict/` enthält nicht FHS-konforme Dokumentationsseiten, `etc/` enthält Konfigurationsdateien für das gesamte System, `games/` ist für Spiele reserviert, `include/` enthält C-Header-Dateien, `kerberos/` enthält Binärdateien und viele andere Kerberos-Elemente und `lib/` enthält Objektdateien und Bibliotheken,die nicht konzipiert wurden, um direkt von Benutzern oder Shell-Skripts verwendet zu werden. Das `libexec/`- Verzeichnis enthält kleinere Hilfsprogramme, die von anderen Programmen aufgerufen werden, `sbin/` enthält die Binärdateien für die Systemverwaltung (d.h. die 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).

3.2.1.9. Das `/usr/local/`-Verzeichnis

Laut FHS:

> "Die `/usr/local/`-Hierarchie 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 benutzt werden, auf die innerhalb einer Gruppe von Rechnern zugegriffen werden kan, und die nicht in `/usr/` abgelegt sind."

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

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

3.2.1.10. Das `/var/`-Verzeichnis

Der Dateisystemstandard FHS erfordert, dass das Mounten von `/usr/` im schreibgeschützten Modus möglich ist. Daher sollten Programme, die Protokolldateien schreiben oder `spool/` or `lock/`-Verzeichnisse benötigen, am besten in das the `/var/` schreiben. Laut FHS steht `/var/` für:

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

Nachfolgend einige der Verzeichnisse, die Unterverzeichnisse von `/var/` sein sollten:

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

Systemprotokolldateien wie z.B. `messages` und `lastlog` werden im `/var/log/`- Verzeichnis abgelegt. Das `/var/lib/rpm/`-Verzeichnis enthält auch die RPM- Systemdatenbanken. Sperrdateien werden in `/var/lock/`, abgelegt, wobei es sich hier normalerweise um spezifische Verzeichnisse für die Programme handelt, das diese Dateien benutzt. Das `/var/spool/`-Verzeichnis hat Unterverzeichnisse, in denen verschiedene Datendateien speichern können.

3.2.2. `/usr/local/` in Red Hat Linux

In Red Hat Linux unterscheidet sich der Verwendungszweck für `/usr/local/` ganz leicht von den durch FHS definierten Verwendungszwecken. Laut FHS soll in `/usr/local/` Software abgelegt werden, die bei Aktualisierungen der System-Software geschützt werden soll. Das Aktualisieren von Red Hat Linux mit dem `rpm`-Befehl und der grafischen **Paketverwaltungstool**- Applikation gewährleistet einige Sicherheit im Hinblick auf das Überschreiben. Deshalb ist es nicht nötig, die Dateien dadurch zu schützen, dass Sie sie im `/usr/local/`- Verzeichnis ablegen. Stattdessen empfehlen wir Ihnen, für lokal auf Ihrem Rechner verwendete Software auf `/usr/local/` zurückzugreifen.

Wenn, zum Beispiel, das Verzeichnis `/usr/` als eine Read-Only (Nur-Lesen) NFS Share von einem Remote Host gemountet wird, ist es immernoch möglich, ein Programm oder Paket unter `/usr/local/` zu installieren.

3.3. Spezielle Dateispeicherstellen

Red Hat Linux erweitert die FHS-Struktur ein wenig, um Platz für spezielle Dateien zu schaffen.

Die meisten Dateien, die zum *Red Hat Package Manager* (*RPM*) gehören, werden im Verzeichnis `/var/lib/rpm/` hinterlegt. Weitere Informationen über RPM finden Sie im Kapitel *Paketverwaltung mit RPM* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

Das `/var/spool/up2date/`-Verzeichnis enthält Dateien, die vom **Red Hat Update Agent** verwendet werden, einschließlich RPM-Header-Informationen für das System. Hier können Sie auch RPMs, die Sie während des Updates Ihres Systems heruntergeladen haben, zwischenspeichern. Weitere Informationen zum Red Hat Network finden Sie auf der Red Hat Network Website unter Eingabe folgenden URLs: https://rhn.redhat.com/.

Eine weitere Red Hat Linux-spezifische Speicherstelle ist das `/etc/sysconfig/`-Verzeichnis. In diesem Verzeichnis wird eine ganze Reihe unterschiedlicher Konfigurationsinformationen gespeichert. Viele Skripts, die beim Booten ausgeführt werden, greifen auf die Dateien in diesem Verzeichnis zurück. Siehe hierzu Kapitel 4 für weitere Informationen über den Inhalt dieses Verzeichnisses und die Bedeutung, die diese Dateien für den Bootprozess haben.

Schließlich soll auch das `/initrd/`-Verzeichnis nicht unerwähnt bleiben. Es ist zwar leer, wird aber während des Boot-Prozesses als kritischer Mount-Punkt verwendet.

Warnung

Entfernen Sie unter gar keinen Umständen das `/initrd/`- Verzeichnis. Wenn Sie dieses Verzeichnis löschen, kann Ihr System nicht starten und der Kernel gibt eine gravierende Fehlermeldung.

Kapitel 4.

Das Verzeichnis `sysconfig`

Das Verzeichnis `/etc/sysconfig/` ist der Ort, an dem sich eine Anzahl von Konfigurationsdateien für Red Hat Linux befindet.

Dieses Kapitel spricht einige der Dateien im Verzeichnis `/etc/sysconfig/`, deren Funktionen und deren Inhalt, an. Die Information in diesem Kapitel erhebt keinen Anspruch auf Vollständigkeit, da viele der Dateien eine Reihe von Optionen haben, die nur in sehr spezifischen Fällen verwendet werden.

4.1. Dateien im Verzeichnis `/etc/sysconfig/`

Folgende Dateien befinden sich normalerweise in `/etc/sysconfig/`:

- `amd`
- `apmd`
- `arpwatch`
- `authconfig`
- `cipe`
- `clock`
- `desktop`
- `dhcpd`
- `firstboot`
- `gpm`
- `harddisks`
- `hwconf`
- `i18n`
- `identd`
- `init`
- `ipchains`
- `iptables`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`
- `named`
- `netdump`
- `network`
- `ntpd`
- `pcmcia`

- radvd
- rawdevices
- redhat-config-securitylevel
- redhat-config-users
- redhat-logviewer
- samba
- sendmail
- soundcard
- spamassassin
- squid
- tux
- ups
- vncservers
- xinetd

Anmerkung

Sollten einige dieser Dateien nicht im Verzeichnis /etc/sysconfig/ enthalten sein, sind die entsprechenden Programme eventuell nicht installiert.

4.1.1. /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.

4.1.2. /etc/sysconfig/amd

Die Datei /etc/sysconfig/apmd wird von apmd verwendet, um zu erfahren, welche Prozesse nach den Befehlen suspend/resume gestartet/gestoppt/geändert werden sollen. In ihr ist festgelegt, ob apmd beim Starten aktiviert oder deaktiviert wird, je nachdem ob Ihre Hardware *Advanced Power Management* (*APM*) unterstützt bzw. ob Sie diese Funktionalität benutzen möchten oder nicht. apm ist ein Daemon mit Kontrollfunktion, der im Linux-Kernel mit einem Power-Management-Code arbeitet. Er kann darauf hinweisen, dass die Batterie fast leer ist, falls Ihr Red Hat Linux auf einem Laptop läuft u.v.m.

4.1.3. /etc/sysconfig/arpwatch

Die Datei /etc/sysconfig/arpwatch wird verwendet, um beim Booten Argumente an den arpwatch-Daemon zu übertragen. Der arpwatch-Daemon pflegt eine Tabelle mit Ethernet-MAC-Adressen und deren IP-Adressen-Paarungen. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von arpwatch. Standardmäßig legt diese Datei als Besitzer des arpwatch-Prozesses den Benutzer pcap fest.

4.1.4. /etc/sysconfig/authconfig

Die Datei /etc/sysconfig/authconfig legt die Art der Authorisierung fest, die auf dem Rechner verwendet werden soll. Sie enthält mindestens eine 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.

4.1.5. /etc/sysconfig/clock

Die Datei /etc/sysconfig/clock steuert die Interpretation der Werte der Hardware-System-Uhr.

Derzeit gelten die folgenden Werte:

- UTC=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - true oder yes — Die Hardware-Uhr ist auf UTC (Universal Time Coordinate) eingestellt.
  - false oder no — Die Hardware-Uhr ist auf lokale Zeit eingestellt.

- ARC=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - true oder yes — Zeigt an, dass der 42-Jahre-Offset der Konsole aktiviert ist. Diese Einstellung ist lediglich für ARC- oder AlphaBIOS-basierte Alpha-Systeme. Alle anderen Werte geben an, dass die normale UNIX-Epoche eingestellt ist.

- SRM=<*Wert*>, wobei <*Wert*> folgender ist:
  - true oder yes — Die 1900-Epoche der Konsole ist aktiviert. Diese Einstellung ist lediglich für SRM-basierte Alpha-Systeme. Jeder andere Wert gibt an, dass die normale UNIX-Epoche eingestellt ist.

- ZONE=<*Dateiname*> — Die Zeitzonen-Datei unter /usr/share/zoneinfo, von der /etc/localtime eine Kopie ist. Diese Datei enthält Informationen wie folgende: ZONE="America/New York"

Frühere Versionen von Red Hat Linux benutzten folgende Versionen (welche nicht länger verwendet werden):

- CLOCKMODE=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - GMT — Zeigt an, dass die Uhr auf Weltzeit (GMT) eingestellt ist.

- ARC — Zeigt an, dass der 42-Jahre-Offset der Konsole aktiviert ist (nur bei Alpha-gestützten Systemen).

4.1.6. /etc/sysconfig/desktop

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

```
DESKTOP="GNOME"
```

4.1.7. /etc/sysconfig/dhcpd

Die Datei /etc/sysconfig/dhcp wird verwendet, um beim Booten Argumente an den dhcp-Daemon zu übertragen. Der dhcpd-Daemon implementiert das Dynamic Host Configuration Protocol (DHCP) und das Internet Bootstrap Protocol (BOOTP). DHCP und BOOTP weisen Rechnern auf dem Netzwerk Hostnamen zu. Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von dhcpd.

4.1.8. /etc/sysconfig/firstboot

Ab Red Hat Linux 8.0 ruft das Programm /sbin/init beim Erststart des Systems das Skript etc/rc.d/init.d/firstboot auf. Dieses Skript ruft seinerseits **Setup-Agent** auf. Diese Applikation ermöglicht dem Benutzer das Installieren weiterer Anwendungen und Dokumentation vor dem Abschluss des Initialstarts.

Die Datei /etc/sysconfig/firstboot weist den **Setup-Agent** einfach an, nicht ausgeführt zu werden. Wenn diese Applikation beim nächsten Systemstart ausführen möchten, müssen Sie einfach nur /etc/sysconfig/firstboot entfernen und chkconfig --level 5 firstboot on ausführen.

4.1.9. /etc/sysconfig/gpm

Die Datei /etc/sysconfig/gpm wird verwendet, um beim Booten Argumente an den gpm-Daemon zu übertragen. Der gpm-Daemon ist der Maus-Server, mit dem die Geschwindigkeit der Maus erhöht und die Möglichkeit des Kopierens mit der mittleren Maus-Taste geschaffen werden kann. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von gpm. Standardmäßig sind die Einstellungen für die Maus /dev/mouse.

4.1.10. /etc/sysconfig/harddisks

Die Datei /etc/sysconfig/harddisks ermöglicht es Ihnen, Ihre Festplatte(n) abzustimmen. Der Administrator kann auch /etc/sysconfig/hardiskhd[a-h] verwenden, um die Parameter für bestimmte Laufwerke zu konfigurieren.

Warnung

Nehmen Sie keine leichtsinnigen Änderungen in dieser Datei vor. Wenn Sie die hier gespeicherten Standardwerte ändern, besteht das Risiko, dass Sie alle Daten der Festplatte(n) verlieren!

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

- `USE_DMA=1`, wobei der Wert 1 DMA aktiviert. 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. *Äußerste Vorsicht!*
- `EIDE_32BIT=3` aktiviert (E)IDE 32-Bit E/A-Support für eine Schnittstellen-Karte.
- `LOOKAHEAD=1` aktiviert Lookahead-Lesezugriffe auf das Laufwerk.
- `EXTRA_PARAMS=` legt fest, wo zusätzliche Parameter hinzugefügt werden können.

4.1.11. `/etc/sysconfig/hwconf`

In der Datei `/etc/sysconfig/hwconfig` sind alle Hardware-Komponenten aufgeführt, die `kudzu` in Ihrem System entdeckt hat, außerdem Informationen zu den verwendeten Treibern, der Anbieter-ID und der Geräte-ID. `kudzu` findet und konfiguriert neue bzw. geänderte Hardware-Komponenten. Die Datei `/etc/sysconfig/hwconfig` ist nicht dazu gedacht, manuell bearbeitet zu werden. Wenn Sie sie dennoch bearbeiten, könnte es passieren, dass manche Geräte plötzlich als hinzugefügt oder entfernt angezeigt werden.

4.1.12. `/etc/sysconfig/i18n`

Mit der Datei `/etc/sysconfig/i18n` wird die Standardsprache, jede unterstützte Sprache und der Default-System-Font eingestellt. Zum Beispiel:

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

4.1.13. `/etc/sysconfig/identd`

Mit der Datei `/etc/sysconfig/identd` werden zum Zeitpunkt des Bootens Argumente an den `identd`-Daemon übertragen. Der `identd`-Daemon leitet den Benutzernamen von Prozessen mit offenen TCP/IP-Verbindungen zurück. Einige Netzwerk-Services, wie z.B. FTP- und IRC-Server werden Fehlermeldungen geben und langsamer arbeiten, wenn `identd` nicht läuft. Im Allgemeinen ist `identd` jedoch kein unbedingt erforderlicher Service. Wenn die Sicherheit auf dem Spiel steht, sollten Sie diesen Befehl nicht ausführen. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von `identd`. Standardmäßig enthält diese Datei keine Parameter.

4.1.14. `/etc/sysconfig/init`

In der Datei `/etc/sysconfig/init` wird die Art der Bildschirmdarstellung und deren Funktionalität während des Bootprozesses gesteuert.

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 Misserfolg von Geräten und Diensten beim Booten in verschiedenen Farben angezeigt wird.
  - BOOTUP=verbose erzeugt ein Display im herkömmlichen Stil. Dieses Display liefert mehr Informationen als bloße Mitteilungen über Erfolg oder Misserfolg.
  - Alle anderen Werte erzeugen ein neues Display, aber ohne ANSI-Formatierung.

- RES_COL=<*Wert*>, wobei <*Wert*> die Spaltennummer des Bildschirms ist, in der Status-Kennungen beginnen. Standardeinstellung ist 60.
- MOVE_TO_COL=<*Wert*>, wobei <*Wert*> den Cursor zu dem Wert in der Zeile RES_COL führt, was über den Befehl echo -en geschieht.
- SETCOLOR_SUCCESS=<*Wert*>, wobei <*Wert*> die Farbe für die Anzeige von erfolgreichen Vorgängen ist. Dies geschieht über den Befehl echo -en, wobei die Farbe auf grün gesetzt wird.
- SETCOLOR_FAILURE=<*Wert*>, wobei <*Wert*> die Farbe für die Anzeige von nicht erfolgreichen Vorgängen bestimmt. Dies geschieht über den Befehl echo -en, wobei die Farbe rot eingestellt wird.
- SETCOLOR_WARNING=<*Wert*>, wobei <*Wert*> die Farbe für die Anzeige von Warnungen bestimmt. Dies geschieht über den Befehl echo -en, wobei die Farbe gelb eingestellt wird.
- SETCOLOR_NORMAL=<*Wert*>, wobei <*Wert*> 'normal' eingestellt wird. Dies geschieht über den Befehl echo -en.
- LOGLEVEL=<*Wert*>, wobei <*Wert*> den anfänglichen Anmelde-Level für den Kernel bestimmt. Die Standardeinstellung ist 3. Der Wert 8 aktiviert alles (einschließlich Debugging), der Wert 1 deaktivert alles außer der Kernel-Panik. syslogd hebt diese Einstellungen auf, nachdem es gestartet ist.
- PROMPT=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - yes — Aktiviert die Key-Überprüfung für den interaktiven Modus.
  - no — Deaktiviert die Key-Überprüfung für den interakiven Modus.

4.1.15. /etc/sysconfig/ipchains

Die Datei /etc/sysconfig/ipchains enthält Informationen, welche vom ipchains-Initialisationsskript zum Einrichten des ipchains-Services verwendet werden.

Diese Datei ist durch das Ausführen des service ipchains save>-Befehls modifiziert, falls es gültige ipchains- Vorschriften gibt. Sie sollten diese Datei nicht manuell bearbeiten. Verwenden Sie statt dessen den Befehl ipchains, um die notwendigen Paket-Filter-Vorschriften zu konfigurieren, und speichern Sie die Vorschriften anschließend in dieser Datei.

4.1.16. /etc/sysconfig/iptables

Genau wie /etc/sysconfig/ipchains speichert /etc/sysconfig/iptables vom Kernel verwendete Informationen, um spezialisierte Paket-Filter-Dienste zu liefern.

Wenn Sie mit der Erstellung der iptables-Regeln noch nicht vertraut sind, sollten Sie diese Datei nicht manuell ändern. Es ist am einfachsten, solche Regeln mit **Sicherheitslevel-Konfigurationstool** (redhat-config-securitylevel), dem Befehl /usr/sbin/lokkit oder der **GNOME Lokkit**-Applikation hinzuzufügen.

Sobald diese Datei vorhanden ist, bleiben alle hier gespeicherten Firewall-Regeln durch einen Systemneustart bestehen.

4.1.17. /etc/sysconfig/irda

Die Datei /etc/sysconfig/irda steuert die Konfiguration der Infrarot-Geräte auf Ihrem System beim Starten.

Folgende Werte können verwendet werden:

- IRDA=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - yes — irattach wird ausgeführt, wodurch regelmäßig überprüft wird, ob irgendeine Komponente versucht, eine Verbindung zum Infrarot-Port herzustellen, z.B. ein Notebook, das versucht, eine Netzwerkverbindung herzustellen. Damit Infrarot- Geräte auf Ihrem System laufen können, muss diese Zeile auf yes eingestellt sein.
  - no — irattach wird nicht ausgeführt, wodurch keine Verbindung zu Infrarot-Geräten besteht.

- DEVICE=<*Wert*>, wobei <*Wert*> das Gerät ist (normalerweise ein serieller Port), über das die Infrarot-Verbindungen abgewickelt werden.
- DONGLE=<*Wert*>, wobei <*Wert*> die Art Dongle angibt, die für die Infrarot-Kommunikation verwendet wird. Diese Einstellung ist für die Benutzer wichtig, die serielle Dongles statt eigentlicher Infrarot-Ports verwenden. Ein Dongle ist ein Gerät, das mit einem herkömmlichen seriellen Port verbunden ist, um per Infrarot zu kommunizieren. Diese wird standardmäßig auskommentiert, da Notebooks mit echten Infrarot-Ports viel häufiger vorkommen als Computer mit angefügten Dongles.
- DISCOVERY=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - yes — Startet irattach im Discovery-Modus, d.h. dieser Befehl sucht aktiv nach anderen Infrarot-Geräten. Dieser Befehl muss aktiviert werden, damit der Rechner aktiv nach einer Infrarot-Verbindung suchen kann (d.h. nach dem Peer, der die Verbindung nicht einleitet).
  - no — Startet irattach nicht im Discovery-Modus.

4.1.18. /etc/sysconfig/keyboard

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

- KEYBOARDTYPE=sun|pc. Wird nur bei Spark-Prozessoren verwendet. sun gibt an, dass eine Sun-Tastatur an /dev/kbd angeschlossen ist, und pc steht für die Verbindung einer PS/2-Tastatur mit einem PS/2-Port.
- KEYTABLE=<*Datei*>, wobei <*Datei*> der Name der keytable-Datei ist.

  Beispiel: KEYTABLE="us". Die Dateien, die als keytables verwendet werden können, beginnen unter /lib/kbd/keymaps/i386 und verzweigen von dort aus in verschiedene Tastatur-Layouts, die alle mit <*Datei*>.kmap.gz gekennzeichnet sind. Die erste Datei, die unter /lib/kbd/keymaps/i386 mit der KEYTABLE-Einstellung übereinstimmt, wird verwendet.

4.1.19. /etc/sysconfig/kudzu

Mit /etc/sysconfig/kuzdu können Sie beim Booten mit Hilfe von kudzu eine sichere Überprüfung Ihrer System-Hardware vornehmen. Bei einer sicheren Überprüfung wird die Überprüfung der seriellen Ports deaktiviert.

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

4.1.20. /etc/sysconfig/mouse

Die Datei /etc/sysconfig/mouse stellt Informationen über die verfügbare Maus zur Verfügung. Die folgenden Werte können verwendet werden:

- FULLNAME=<*Wert*>, wobei sich <*Wert*> auf den vollen Namen der verwendeten Mausart bezieht.
- MOUSETYPE=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - imps2 — Generische USB Rad-Maus.
  - 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 — ältere MouseMan™- Maus.
  - mmhittab — mmhittab-Maus.

- XEMU3=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - yes — Die Maus hat nur zwei Buttons, drei Buttons sollten jedoch emuliert werden.
  - no — Die Maus hat bereits drei Buttons.
- XMOUSETYPE=<*Wert*>, wobei sich <*Wert*> auf die Mausart bezieht, die bei der Ausführung von X verwendet wird. Die hier aufgeführten Optionen entsprechen den MOUSETYPE-Einstellungen dieser Datei.
- DEVICE=<*Wert*>, wobei <*Wert*> die Maus ist.

Außerdem gibt es /dev/mouse, einen symbolischen Link, der auf das eigentliche Mausgerät zeigt.

4.1.21. /etc/sysconfig/named

Die Datei /etc/sysconfig/named wird verwendet, um beim Booten Argumente an den named-Daemon zu übertragen. Der named-Daemon ist ein *Domain Name System* (*DNS*)-Server, der die Version 9 von *Berkeley Internet Name Domain* (*BIND*) implementiert. Auf diesem Server gibt es eine Tabelle, mit deren Hilfe bestimmte Hostnamen IP-Adressen im Netzwerk zugeordnet werden.

Verwenden Sie bitte bis auf weiteres nur die folgenden Werte:

- ROOTDIR="*</irgend/wo>*", wobei sich *</irgend/wo>* auf den vollständigen Verzeichnispfad einer konfigurierten Chroot-Umgebung bezieht, unter der named ausgeführt wird. Besagte Umgebung muss zunächst konfiguriert werden. Nach Eingabe von info chroot erhalten Sie mehr Informationen dazu, wie Sie bei der Konfiguration vorgehen müssen.
- OPTIONS="*<Wert>*", wobei *<Wert>* jede der auf der man-Seite für named aufgeführten Optionen sein kann, mit Ausnahme von **-t**. An Stelle von **-t** verwenden Sie oben bitte die ROOTDIR-Zeile.

Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf der man-Seite von named. Detaillierte Informationen zum Konfigurieren eines BIND-DNS-Servers finden Sie unter Kapitel 12. Standardmäßig enthält diese Datei keine Parameter.

4.1.22. /etc/sysconfig/netdump

/etc/sysconfig/netdump ist die Konfigurationsdatei für den /etc/init.d/netdump- Dienst. Mit dem netdump-Dienst werden sowohl Oops- also auch Speicherdaten auf dem Netzwerk übertragen. netdump ist grundsätzlich nicht erforderlich. Sie sollten diese Datei also nur ausführen, wenn es unbedingt notwendig ist. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von netdump.

4.1.23. /etc/sysconfig/network

Die Datei /etc/sysconfig/arpwatch wird verwendet, um Informationen über die gewünschte Netzwerkkonfiguration anzugeben. Die folgenden Werte können verwendet werden:

- NETWORKING=*<Wert>*, wobei *<Wert>* einer der folgenden booleschen Werte ist:
  - yes — Das Netzwerk sollte konfiguriert sein.
  - no — Das Netzwerk sollte nicht konfiguriert sein.

- HOSTNAME=*<Wert>*, wobei *<Wert>* der *Fully Qualified Domain Name* (*FQDN*) sein sollte, z.B. hostname.domain.com, kann aber auch jeder andere, von Ihnen gewünschte Hostname sein.

Anmerkung

Um die Kompatibilität mit älterer Software (z.B.trn) zu gewährleisten, sollte die /etc/HOSTNAME-Datei den gleichen Wert wie hier enthalten.

- GATEWAY=*<Wert>*, wobei *<Wert>* die IP-Adresse des Netzwerk-Gateways ist.
- GATEWAYDEV=*<Wert>*, wobei *<Wert>* das Gateway-Gerät ist, z.B. eth0.
- NISDOMAIN=*<Wert>*, wobei *<Wert>* der NIS-Domainname ist.

4.1.24. /etc/sysconfig/ntpd

Die Datei /etc/sysconfig/ntpd wird verwendet, um beim Booten Argumente an den ntpd-Daemon zu übertragen. Mit dem ntpd-Daemon wird die Systemuhr eingestellt und in Übereinstimmung mit einem Standard-Zeit-Server im Internet gebracht. Hierbei wird Version 4 des Network Time Protocol (NTP) implementiert. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie, wenn Sie den Browser zu folgender Datei führen: /usr/share/doc/ntp-<version>/ntpd.htm (wobei <Version> die jeweilige Version von ntpd bezeichnet). Standardmäßig legt diese Datei den Besitzer des ntpd-Prozesses auf den Benutzer ntp.

4.1.25. /etc/sysconfig/pcmcia

Mit der Datei /etc/sysconfig/pcmcia werden die Informationen zur Konfiguration von PCMCIA bestimmt. Die folgenden Werte können verwendet werden:

- PCMCIA=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - yes — Der PCMCIA-Support sollte aktiviert werden.
  - no — Der PCMCIA-Support sollte 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 mit den Optionen für den PCMCIA-cardmgr ist (z.B. -q für den Ruhemodus -m, um nach ladbaren Kernelmodulen im angegebenen Verzeichnis zu suchen usw.). Weitere Informationen finden Sie auf der cardmgr-man-Seite.

4.1.26. /etc/sysconfig/radvd

Die Datei /etc/sysconfig/radvd wird verwendet, um beim Booten Argumente an den radvd-Daemon zu übertragen. Der radvd-Daemon spricht auf Router-Anfragen an und versendet Router-Anzeigen für das IP Version 6-Protokoll. Mit diesem Dienst können die Rechner eines Netzwerks dynamisch ihre Standard-Router auf der Grundlage vorgenannter Router-Anzeigen ändern. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von radvd. Standardmäßig stellt diese Datei als Besitzer des radvd-Prozesses den Benutzer radvd ein.

4.1.27. /etc/sysconfig/rawdevices

Mit der Datei /etc/sysconfig/rawdevices werden Rawdevice-Verbindungen konfiguriert, z.B.:

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

4.1.28. /etc/sysconfig/redhat-config-securitylevel

Die Datei /etc/sysconfig/redhat-config-securitylevel enthält alle Optionen, welche beim letzten Ausführen von **Sicherheitslevel-Konfigurationstool** (redhat-config-securitylevel) gewählt wurden. Benutzer sollten diese Datei nicht manuell bearbeiten. Für mehr Informationen zu **Sicherheitslevel-Konfigurationstool** lesen Sie das Kapitel *Basiskonfiguration der Firewall* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

4.1.29. /etc/sysconfig/redhat-config-users

Die Datei /etc/sysconfig/clock ist die Konfigurationsdatei für die grafische Applikation **redhat-config-users**. Unter Red Hat Linux wird diese Datei dazu verwendet, um Systembenutzer, wie root, Daemon oder lp herauszufiltern. Diese Datei kann über das Pull-Down-Menü **Einstellungen => Systembenutzer und Gruppen filtern** in der Anwendung **redhat-config-users** berabeitet werden. Die Bearbeitung sollte nicht manuell erfolgen. Weitere Informationen zur Verwendung dieser Anwendung finden Sie im Kapitel *Benutzer- und Gruppen-Konfiguration* des *Red Hat Linux Handbuchs benutzerdefinierter Konfiguration*.

4.1.30. /etc/sysconfig/redhat-logviewer

Die Datei /etc/sysconfig/netdump ist die Konfigurationsdatei für die grafische interaktive Anwendung zum Anzeigen von Protokollen, **redhat-logviewer**. Diese Datei wird über das Pull-Down-Menü **Bearbeiten => Einstellungen** in **redhat-logviewer** bearbeitet. Die Bearbeitung sollte nicht manuell erfolgen. Weitere Informationen zum Verwenden der Anwendung finden Sie im Kapitel *Protokolldateien* des *Red Hat Linux Handbuchs benutzerdefinierter Konfiguration*.

4.1.31. /etc/sysconfig/samba

Die Datei /etc/sysconfig/samba wird verwendet, um beim Booten Argumente an die Daemonen smbd und nmbd zu übertragen. Mit Hilfe des smbd-Daemonen können Windows-Clients im Netzwerk Verbindungen mit gemeinsamen Dateien herstellen. Mit dem nmbd-Daemonen steht Ihnen NetBIOS mit IP-Naming-Diensten zur Verfügung. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von smbd. Standardmäßig sind smbd und nmbd so eingestellt, dass sie im Daemon-Modus ausgeführt werden.

4.1.32. /etc/sysconfig/sendmail

Die Datei /etc/sysconfig/sendmail ermöglicht das Versenden von Nachrichten an einen oder mehrere Empfänger, wobei die Nachrichten je nach Bedarf über beliebige Netzwerke geroutet werden können. In dieser Datei sind die Standardwerte für die Ausführung der Sendmail-Applikation festgelegt. Standardmäßig läuft es als Hintergrund-Daemon und wird einmal stündlich überprüft, für den Fall, dass Nachrichten zurückgesandt wurden.

Folgende Werte können verwendet werden:

- DAEMON=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - yes — Sendmail sollte so konfiguriert werden, dass er auf Port 25 eingehende Mails abfragt. Bei yes werden die -bd-Optionen von Sendmail verwendet.
  - no — Sendmail sollte nicht so konfiguriert werden, dass es auf Port 25 eingehende Mails abfragt.

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

4.1.33. /etc/sysconfig/soundcard

Die Datei /etc/sysconfig/soundcard wird von sndconfig erstellt und sollte nicht verändert werden. Diese Datei dient einzig und allein der Bestimmung des Karteneintrags, der im Menü standardmäßig geöffnet werden soll, wenn sndconfig beim nächsten Mal ausgeführt wird. Informationen zur Konfiguration der Soundkarte finden Sie in der Datei /etc/modules.conf.

Folgende Werte können enthalten sein:

- CARDTYPE=<*Wert*>, wobei <*Wert*> z.B. auf SB16 für eine Soundblaster 16- Soundkarte eingestellt ist.

4.1.34. /etc/sysconfig/spamassassin

Die Datei /etc/sysconfig/spamassassin wird verwendet, um Argumente zum spamd-Daemon (eine daemonisierte Version von Spamassassin) zur Bootzeit zu übergeben. Spamassassin ist ein Email-Spam-Filter. Für eine Liste der verfügbaren Optionen, sehen Sie die man-Seiten von spamd. Standardmäßig wird spamd für den Daemon-Mode konfiguriert, zum Erzeugen von Benuzter-Präferenzen und zum automatischen Erzeugen von Referenzlisten.

Weitere Informationen zu Spamassassin, finden Sie unter Abschnitt 11.4.2.6.

4.1.35. /etc/sysconfig/squid

Die Datei /etc/sysconfig/squid wird verwendet, um beim Booten Argumente an den squid-Daemon zu übertragen. Der squid-Daemon ist ein Proxy-Caching-Server für Web- Client-Applikationen. Weitere Informationen zum Konfigurieren eines squid-Proxy-Servers erhalten Sie, indem Sie mit einem Webbrowser das Verzeichnis /usr/share/doc/squid-<*Version*>/ öffnen (ersetzen Sie <*Version*> durch die auf Ihrem System installierte squid- Versionsnummer). Standardmäßig ist in dieser Datei der squid-Topstart im Daemon-Modus und die Zeitspanne, innerhalb der es sich schließt, festgelegt.

4.1.36. /etc/sysconfig/tux

/etc/sysconfig/tux ist die Konfigurationsdatei für den Red Hat Content Accelerator (früher TUX), den Kernel-basierten Web-Server. Weitere Informationen zum Konfigurieren von Red Hat Content Accelerator erhalten Sie, wenn Sie mit einem Web-Browser /usr/share/doc/tux-<*Version*>/tux/index.html öffnen (ersetzen Sie ><*Version*> mit der bereits auf Ihrem System installierten TUX-Versionsnummer). Die für diese Datei verfügbaren Parameter sind unter /usr/share/doc/tux-<*Version*>/tux/parameters.html aufgeführt.

4.1.37. /etc/sysconfig/ups

Die Datei /etc/sysconfig/ups wird verwendet, um Informationen über jegliche *Geräte mit kontinuierlicher Stromversorgung* (*UPS*) zu bestimmen, die mit Ihrem Systm verbunden sind. Ein UPS kann in einem Red Hat Linux-System sehr nützlich sein, da das System mit seiner Hilfe auch im Falle einer Stromunterbrechung korrekt heruntergefahren werden kann. Folgende Werte können verwendet werden:

- `SERVER=<`*`Wert`*`>`, wobei <*`Wert`*> einer der folgenden Werte ist:
  - `yes` — Ein UPS-Gerät wird an Ihr System angeschlossen.
  - `no` — Ein UPS-Gerät wird nicht an Ihr System angeschlossen.

- `MODEL=<`*`Wert`*`>`, wobei <*`Wert`*> einer der folgenden Werte oder auf `NONE` gesetzt sein muss, wenn an Ihrem System kein UPS-Gerät angeschlossen ist:
  - `apcsmart` — Ein APC Smart UPS™- oder ein ähnliches Gerät.
  - `fentonups` — Ein Fenton UPS™-Gerät.
  - `optiups` — Ein OPTI-UPS™-Gerät.
  - `bestups` — Ein Best Power™-UPS-Gerät.
  - `genericups` — Ein generisches Marken-UPS-Gerät.
  - `ups-trust425+625` — Ein Trust™-UPS-Gerät.

- `DEVICE=<`*`Wert`*`>`, wobei <*`Wert`*> festlegt, an welcher Stelle das UPS-Gerät angeschlossen wird, z.B. `/dev/ttyS0`.
- `OPTIONS=<`*`Wert`*`>`, wobei <*`Wert`*> ein Sonderbefehl ist, der an das UPS-Gerät übertragen werden muss.

4.1.38. `/etc/sysconfig/vncservers`

Die Datei `/etc/sysconfig/keyboard` konfiguriert, wie der *Virtual Network Computing* (*VNC*)-Server gestartet wird. 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) und dabei eine Vielfalt von Rechnerarchitekturen verwenden können.

Folgende Werte können enthalten sein:

- `VNCSERVERS=<`*`Wert`*`>`, wobei <*`Wert`*> z.B. wie folgt eingestellt wird: `"1:fred"`. Dies zeigt an, dass ein VNC-Server für den Benutzer Fred auf Anzeige :1 gestartet werden sollte. Benutzer Fred muss allerdings vorher mit `vncpasswd` ein VNC-Passwort eingestellt haben, um eine Verbindung mit dem Remote-VNC-Server herstellen zu können.

Beachten Sie bitte, dass Ihre Kommunikation nicht verschlüsselt ist, wenn Sie mit einem VNC-Server arbeiten. Sie sollten VNC also nicht auf einem unsicheren Netzwerk verwenden. Genaue Anweisungen hinsichtlich der Benutzung von SSH zum Schutz der Kommunikaton mit VNC finden Sie unter http://www.uk.research.att.com/vnc/sshvnc.html. Näheres über SSH finden Sie in Kapitel 18 oder im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

4.1.39. `/etc/sysconfig/xinetd`

Mit der Datei `/etc/sysconfig/xinetd` werden zum Zeitpunkt des Bootens Argumente an den `xinetd`-Daemon übertragen. Der `xinetd`-Daemon startet Programme, die Ihnen Internet-Dienste zur Verfügung stellen, wenn auf dem für diesen Dienst zuständigen Port eine entsprechende Anfrage eingeht. Weitere Informationen zu den möglichen Parametern in dieser Datei erhalten Sie auf den man-Seiten von `xinetd`. Weitere Informationen zum `xinetd`-Dienst finden Sie unter Abschnitt 15.3.

4.2. Verzeichnisse im Verzeichnis /etc/sysconfig/

Folgende Verzeichnisse befinden sich normalerweise in /etc/sysconfig/:

- apm-scripts/ — Dieses Verzeichnis enthält das Red Hat APM Suspend/Resume-Skript. Sie sollten diese Datei nicht direkt bearbeiten. Wenn Sie eine Anpassung wünschen, erstellen Sie einfach eine Datei mit dem Namen /etc/sysconfig/apm-scripts/apmcontinue, die am Ende des Skripts aufgerufen wird. Sie können das Skript auch mittels der Bearbeitung von /etc/sysconfig/apmd steuern.
- cbq/ — Dieses Verzeichnis enthält die Konfigurationsdateien für das Class Based Queuing im Rahmen der Verwaltung der Datenübertragungsrate von Netzwerk-Schnittstellen.
- networking/ — Dieses Verzeichnis wird für das **Red Hat Network Administration Tool** verwendet und sollte nicht manuell bearbeitet werden. Weitere Informationen zur Konfiguration von Schnittstellen mit dem **Red Hat Network Administration Tool** finden Sie im Kapitel *Netzwerkkonfiguration* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.
- network-scripts/ — Dieses Verzeichnis enthält die folgenden netzwerkrelevanten Konfigurationsdateien:
  - Netzwerk-Konfigurationsdateien für jede einzelne konfigurierte Schnittstelle, wie z.B. ifcfg-eth0 für die eth0-Ethernet-Schnittstelle.
  - Skripts zur Aktivierung und Deaktivierung von Netzwerk-Schnittstellen, wie z.B. ifup und ifdown.
  - Skripts zur Aktivierung und Deaktivierung von ISDN-Schnittstellen, wie z.B. ifup-isdn und ifdown-isdn
  - Verschiedene Skripte zu gemeinsam genutzten Netzwerk-Funktionen, die nicht unmittelbar berarbeitet werden sollten.

  Weitere Informationen zum Verzeichnis network-scripts finden Sie unter Kapitel 8.
- rhn/ — Dieses Verzeichnis enthält die Konfigurationsdateien für **Red Hat Network Registration Client**, **Red Hat Update Agent Configuration Tool**, **Red Hat Update Agent** und **Red Hat Network Alert Notification Tool** sowie systemid und GPG-Schlüssel. Keine der Dateien in diesem Verzeichnis sollte manuell bearbeitet werden. Weitere Informationen zu Red Hat Network finden Sie auf der Red Hat Network-Website unter folgender URL: https://rhn.redhat.com.

4.3. Zusätzliche Ressourcen

Da dieses Kapitel nur eine Einleitung zu den Dateien im Verzeichnis /etc/sysconfig/ darstellt, sind folgend Quellen angegeben, welche ausführlichere Informationen enthalten.

4.3.1. Installierte Dokumentation

- /usr/share/doc/initscripts-<*version-number*>/sysconfig.txt — Diese Datei enthält eine umfangreichere Liste der im Verzeichnis /etc/sysconfig/ enthaltenen Dateien und die Konfigurationsoptionen, welche diesen zur Verfügung stehen. <*version-number*> im Pfad zur Datei entspricht der Version des installierten initscripts-Pakets.

redhat

Kapitel 5.

Das /proc Dateisystem

Der Linux-Kernel hat zwei Hauptfunktionen: die Zugriffskontrolle auf physische Geräte eines Computers und die Planung wann und wie Prozesse diese Geräte beeinflussen. Das Verzeichnis `/proc` enthält eine Hierarchie spezieller Dateien, die den aktuellen Stand des Kernel darstellen und Anwendungen und Benutzern einen Einblick in die Sicht des Kernels auf das System gestatten.

Im Verzeichnis `/proc/` finden Sie eine Vielzahl an Informationen zur Systemhardware und allen derzeit laufenden Prozessen. Außerdem können einige Dateien des Baumverzeichnisses `/proc/` von Benutzern und Anwendungen so geändert werden, dass sich die Kernelkonfiguration ändert.

5.1. Ein virtuelles Dateisystem

Unter Linux werden alle Daten in Dateien gespeichert. Die meisten Benutzer kennen die beiden Grundarten von Dateien - Text und Binär. Das `/proc` Verzeichnis enthält allerdings eine andere Dateiart, die *Virtuelle Datei* genannt wird. Aus diesem Grund spricht man bei `/proc/` oft von einem *Virtuellen Dateisystem*.

Diese virtuellen Dateien haben einige interessante Besonderheiten. Die meisten werden mit einer Dateigröße von 0 Bytes aufgelistet, wenn man die Datei allerdings öffnet, zeigt sie oft einiges an Informationen. Außerdem spiegeln die meisten Zeit-und Datumseinstellungen der virtuellen Dateien die aktuelle Zeit und das aktuelle Datum wieder, was bedeutet, dass sie sich ständig ändern.

Virtuelle Dateien wie `/proc/interrupts`, `/proc/meminfo`, `/proc/mounts` und `/proc/partitions` bieten einen aktuellen Einblick in die Systemumgebung. Andere, wie `/proc/file systems` und das Verzeichnis `/proc/sys/` bieten Informationen zur System-Konfiguration und zu Schnittstellen.

Um eine bessere Strukturierung zu erreichen, sind Dateien mit ähnlichen Informationen in virtuelle Verzeichnisse und Unter-Verzeichnisse einsortiert. Zum Beispiel `/proc/ide` enthält Informationen zu allen physischen IDE Geräten. Prozessverzeichnisse enthalten Informationen zu jedem im System laufenden Prozess.

5.1.1. Anzeigen virtueller Dateien

Mit `cat`, `more` oder `less` können Sie die Dateien in `/proc/` mit ihrem enormen Informationsgehalt über das System direkt auslesen. Wenn Sie z.B. wissen möchten, welche Art von CPU ein Computer hat, geben Sie den Befehl `cat /proc/cpuinfo` ein, und es erscheint in etwa Folgendes:

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

```
wp  : yes
flags  : fpu vme de pse tsc msr mce cx8 pge mmx syscall 3dnow k6_mtrr
bogomips : 799.53
```

Bei der Anzeige unterschiedlicher virtueller Dateien im Dateisystem `/proc/` werden Sie feststellen, dass einige Informationen leicht verständlich sind, andere wiederum nicht lesbar sind. Aus diesem Grund gibt es Dienstprogramme, mit deren Hilfe Daten aus virtuellen Dateien lesbar angezeigt werden. Beispiele für diese Applikationen sind `lspci`, `apm`, `free` und `top`.

Anmerkung

Einige virtuelle Dateien im `/proc` können nur vom root gelesen werden.

5.1.2. Ändern virtueller Dateien

Im Allgemeinen sind die meisten virtuellen Dateien im Verzeichnis `/proc` schreibgschützt. Einige können jedoch dazu verwendet werden, Änderungen der Kernel-Einstellungen vorzunehmen. Das gilt im Besonderen für Dateien im Unterverzeichnis `/proc/sys/`.

Sie können den Wert einer virtuellen Datei mit dem Befehl `echo` ändern und mit dem Symbol > den neuen Wert an die Datei weiterleiten. Um zum Beispiel den Hostnamen zu ändern, geben Sie Folgendes ein:

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

Andere Dateien funktionieren als binäre oder Boolesche Switches. Wenn Sie z.B. `cat /proc/sys/net/ipv4/ip_forward` eingeben, erscheint entweder `0` oder `1`. `0` gibt an, dass der Kernel keine Netzwerk-Pakete weiterleitet. Mit dem Befehl `echo` zum Ändern des Wertes der Datei `ip_forward` in `1` können Sie das Weiterleiten von Paketen sofort einschalten.

Tipp

Eine weiterer Befehl zur Änderung von Einstellungen im Unterverzeichnis `/proc/sys/` ist `/sbin/sysctl`. Weitere Informationen zu diesem Befehl erhalten Sie unter Abschnitt 5.4

Eine Liste einiger Kernel-Konfigurationsdateien, die in `/proc/sys/` enthalten sind, finden Sie unter Abschnitt 5.3.9.

5.2. Top-Level Dateien in /procDateisystem

Im Folgenden finden Sie eine Liste von einigen nützlichen virtuellen Dateien im Top-Level des Verzeichnisses `/proc`.

Anmerkung

In den meisten Fällen entspricht der Inhalt der in diesem Abschnitt aufgeführten Dateien nicht denen in Ihrem Rechner. Dies liegt daran, dass sich die meisten Informationen auf die Hardware beziehen, auf der Red Hat Linux läuft.

5.2.1. /proc/apm

Diese Datei bietet Informationen über den Status des *Advanced Power Management (APM)* Systems und wird vom Befehl `apm` benutzt. Die Ausgabe dieser Datei auf einem System ohne Akku, das an das Stromnetz angeschlossen ist, sieht ähnlich dieser Ausgabe aus:

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

Wenn Sie den Befehl `apm -v` auf diesen Systemen ausführen, wird Folgendes angezeigt:

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

Auf nicht batteriebetriebenen Systemen kann `apm` nicht viel mehr bewirken, als den Rechner in den Standby-Modus zu versetzen. Der `apm` Befehl ist auf Laptops viel sinnvoller einzusetzen. Das zeigt auch die folgende Ausgabe von `cat /proc/apm`. Dies ist eine beispielhafte Ausgabe eines Laptops, der mit dem Stromnetz verbunden ist.

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

Wird das gleiche Laptop für einige Minuten vom Stromnetz entfernt, ändert sich der Inhalt der Datei `apm` wie folgt:

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

Das Programm `apm` macht nun eine lesbare Ausgabe aus diesen Daten:

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

5.2.2. /proc/cmdline

Diese Datei zeigt die Parameter an, die dem Linux-Kernel zum Startzeitpunkt übergeben wurden. Eine `/proc/cmdline` Beispieldatei sieht wie folgt aus:

```
ro root=/dev/hda2
```

`(ro)`; zeigt an, dass der Kernel read-only von der zweiten Partition auf dem ersten IDE Device `/dev/hda2` geladen wurde.

5.2.3. /proc/cpuinfo

Diese virtuelle Datei identifiziert den von Ihrem System verwendeten Prozessor. Eine typische Ausgabe sieht zum Beispiel wie folgt aus:

```
processor       : 0
vendor_id       : AuthenticAMD
```

```
cpu family      : 5
model           : 9
model name      : AMD-K6(tm) 3D+ Processor
stepping        : 1
cpu MHz         : 400.919
cache size      : 256 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 1
wp              : yes
flags           : fpu vme de pse tsc msr mce cx8 pge mmx syscall 3dnow k6_mtrr
bogomips        : 799.53
```

- `processor` — Gibt jedem Prozessor eine ID-Nummer. Wenn Ihr System nur über einen Prozessor verfügt, wird nur `0` angezeigt.
- `cpu family` — Zeigt Ihnen den Prozessortyp an, den Ihr System benutzt. Basiert Ihr Rechner auf Intel, stellen Sie die Zahl einfach vor "86", um den Wert zu berechnen. Das ist besonders dann nützlich, wenn Sie die Architektur eines älteren Systems (586, 486, oder 386) herausfinden möchten. Da einige RPM Pakete für jede dieser speziellen Architekturen kompiliert werden, hilft Ihnen dieser Wert bei der Entscheidung, welches Packet zu installieren ist.
- `model name` — Zeigt den Namen und den Projektnamen des Prozessors an.
- `cpu MHz` — Zeigt die genaue Geschwindigkeit des Prozessors in Megahertz an.
- `cache size` — Zeigt die Menge von verfügbarem Level 2 Cache des Prozessors an.
- `flags` — Gibt eine Anzahl von Eigenschaften des Prozessors aus, wie zum Beispiel eine Floating Point Unit (FPU), oder die Verarbeitung von MMX-Befehlen.

5.2.4. /proc/devices

Diese Datei zeigt die Zeichen- und Block-Geräte an, die zur Zeit im Kernel konfiguriert sind. Geräte, deren Module nicht im Kernel geladen sind, werden nicht berücksichtigt. Eine Beispiel-Ausgabe dieser virtuellen Datei finden Sie hier:

```
Character devices:
  1 mem
  2 pty
  3 ttyp
  4 ttyS
  5 cua
  7 vcs
 10 misc
 14 sound
 29 fb
 36 netlink
128 ptm
129 ptm
136 pts
137 pts
162 raw
```

```
254 iscsictl

Block devices:
  1 ramdisk
  2 fd
  3 ide0
  9 md
 22 ide1
```

Die Ausgabe von `/proc/devices` enthält die Major Number und den Namen eines Gerätes und ist in zwei größere Sektionen aufgeteilt: `Character devices` und `Block devices`.

Zeichen-Geräte (Character Devices) sind bis auf zwei wichtige Unterschiede sehr ähnlich zu *Block-Geräten*.

1. Block-Geräte haben einen Puffer, der das Ordnen von Zugriffen vor der Ausführung zulässt. Das ermöglicht zum Beispiel bei Festplatten oder anderen Speichergeräten eine effizientere Speicherung. Zeichen-Geräte benötigen diese Pufferung nicht.
2. Block-Geräte können Informationen in Datenblöcken einer bestimmten Größe senden und empfangen. Diese Größe kann je nach Gerät konfiguriert werden. Zeichen-Geräte senden Daten, ohne eine vorkonfigurierte Größe zu beachten.

Zusätzliche Informationen über Geräte finden Sie in: `/usr/src/linux-2.4/Documentation/devices.txt`.

5.2.5. `/proc/dma`

Diese Datei enthält eine Liste von registrierten ISA Direct Memory Access (DMA) Kanälen, die verwendet werden. Eine Beispieldatei von `/proc/dma` sieht wie folgt aus:

```
 4: cascade
```

5.2.6. `/proc/execdomains`

Diese Datei zeigt die *Execution Domains*, die gegenwärtig vom Linux-Kernel unterstützt werden, und die jeweilige Anzahl unterstützter "Personalities" (Persönlichkeiten) an.

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

Betrachten Sie Execution Domains als "Persönlichkeit" eines bestimmten Betriebssystems. Da andere Binär-Formate wie Solaris, UnixWare oder FreeBSD mit Linux verwendet werden können, kann ein Programmierer die Art verändern, wie das Betriebssystem bestimmte Systemaufrufe dieser Binärformate behandelt, in dem er die "Personality" eines Tasks ändert. Bis auf die Execution Domain `PER_LINUX` können unterschiedliche "Personalities" als dynamisch ladbare Module implementiert werden.

5.2.7. `/proc/fb`

Diese Datei enthält eine Liste von Framebuffer-Geräten, inklusive der Framebuffer-Gerätenummer und dem zuständigen Treiber. Eine typische Ausgabe von `/proc/fb` für ein System mit einem Framebuffer-Gerät sieht wie folgt oder ähnlich aus:

```
0 VESA VGA
```

5.2.8. /proc/filesystems

Diese Datei zeigt eine Liste von Dateisystemen an, die zur Zeit vom Kernel unterstützt werden. Eine Beispielausgabe mit einem generischen `/proc/filesystems` sieht ähnlich wie folgendes aus:

```
nodev rootfs
nodev bdev
nodev proc
nodev sockfs
nodev tmpfs
nodev shm
nodev pipefs
 ext2
nodev ramfs
 iso9660
nodev devpts
 ext3
nodev autofs
nodev binfmt_misc
```

Die erste Spalte zeigt an, ob die Dateisysteme auf einem Block-Gerät liegen; wenn in der ersten Spalte `nodev` steht, bedeutet das, dass Sie nicht auf ein Block-Gerät gemountet sind. Die zweite Spalte zeigt die Namen des unterstützten Dateisystems an.

Der `mount` Befehl durchsucht die hier aufgelisteten Dateisysteme, wenn eines nicht als Argument angegeben wurde.

5.2.9. /proc/interrupts

Diese Datei zeigt die Anzahl von Interrupts pro IRQ auf der x86 Architektur an. Eine typische `/proc/interrupts` Datei ähnelt dem Folgenden:

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

Bei einer Multi-Prozessor-Maschine sieht dies etwas anders aus:

```
           CPU0       CPU1
  0: 1366814704          0          XT-PIC  timer
  1:        128        340    IO-APIC-edge  keyboard
  2:          0          0          XT-PIC  cascade
  8:          0          1    IO-APIC-edge  rtc
 12:       5323       5793    IO-APIC-edge  PS/2 Mouse
 13:          1          0          XT-PIC  fpu
 16:   11184294   15940594   IO-APIC-level  Intel EtherExpress Pro 10/100 Ethernet
 20:    8450043   11120093   IO-APIC-level  megaraid
 30:      10432      10722   IO-APIC-level  aic7xxx
 31:         23         22   IO-APIC-level  aic7xxx
NMI:          0
```

```
ERR:          0
```

Die erste Spalte bezeichnet die IRQ Nummer. Jeder CPU im Rechner hat seine eigene Spalte und seine eigenen Interrupts pro IRQ. Die nächste Spalte bezeichnet den Typ des Interrupts und die letzte Spalte enthält den Namen des Geräts, das auf diesem IRQ angesprochen werden kann.

Jeder der (plattform-abhängigen) Interrupt-Typen in dieser Datei hat eine unterschiedliche Bedeutung. Bei x86 Rechnern kommen folgende Werte häufig vor:

- `XT-PIC` — Die alten AT-Rechner Interrupts.
- `IO-APIC-edge` — Das Spannungssignal dieses Interrupts variiert zwischen tief und hoch, und hat eine *Flanke*, an der der Interrupt ausgelöst und nur einmal signalisiert wird. Dieser Interrupt-Typ wird wie der `IO-APIC-level` Interrupt nur auf Systemen mit Prozessoren der 586 Familie und höher benutzt.
- `IO-APIC-level` — Erzeugt Interrupts, wenn das Spannungssignal hoch geht, solange, bis das Signal wieder das Tief erreicht.

5.2.10. `/proc/iomem`

Diese Datei zeigt Ihnen das aktuelle Mapping des Systemspeichers für jedes physische Gerät an:

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

Die erste Spalte zeigt die Speicherregister an, die von jedem der verschiedenen Speichertypen verwendet werden. Die zweite Spalte zeigt die Art des Speichers in diesem Register an. Diese Spalte zeigt Ihnen vor allem auch an, welche Speicherregister vom Kernel im Systemspeicher benutzt werden, oder, wenn z.B. Ihre Netzwerkschnittstelle mehrere Ethernetports hat, welcher Port welche Speicherregister verwendet.

5.2.11. `/proc/ioports`

Die Ausgabe von `/proc/ioports` liefert eine Liste von zur Zeit registrierten Port-Regionen zur I/O Kommunikation mit einem Gerät. Diese Datei kann sehr lang sein; der Anfang kann ähnlich wie hier aussehen:

```
0000-001f : dma1
0020-003f : pic1
0040-005f : timer
```

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

Die erste Spalte zeigt den Adressbereich des I/O-Ports an, der für ein Gerät in der zweiten Spalte reserviert ist.

5.2.12. /proc/isapnp

Diese Datei listet *Plug and Play (PnP)* Karten in ISA Steckplätzen im System auf. Dies ist oft bei Soundkarten der Fall, aber kann auch viele andere Geräte umfassen. Eine `/proc/isapnp` Datei mit einem Soundblaster-Eintrag sieht ähnlich wie hier aus:

```
Card 1 'CTL0070:Creative ViBRA16C PnP' PnP version 1.0 Product version 1.0
  Logical device 0 'CTL0001:Audio'
    Device is not active
    Active port 0x220,0x330,0x388
    Active IRQ 5 [0x2]
    Active DMA 1,5
    Resources 0
      Priority preferred
      Port 0x220-0x220, align 0x0, size 0x10, 16-bit address decoding
      Port 0x330-0x330, align 0x0, size 0x2, 16-bit address decoding
      Port 0x388-0x3f8, align 0x0, size 0x4, 16-bit address decoding
      IRQ 5 High-Edge
      DMA 1 8-bit byte-count compatible
      DMA 5 16-bit word-count compatible
      Alternate resources 0:1
        Priority acceptable
        Port 0x220-0x280, align 0x1f, size 0x10, 16-bit address decoding
        Port 0x300-0x330, align 0x2f, size 0x2, 16-bit address decoding
        Port 0x388-0x3f8, align 0x0, size 0x4, 16-bit address decoding
        IRQ 5,7,2/9,10 High-Edge
        DMA 1,3 8-bit byte-count compatible
        DMA 5,7 16-bit word-count compatible
```

Diese Datei kann sehr lang werden, je nach Anzahl der angezeigten Geräte und deren Ressourcenanforderungen.

Jede Karte wird mit ihrem Namen, der PnP-Versionsnummer und der Produkt-Versionsnummer angezeigt. Wenn das Gerät aktiv und konfiguriert ist, zeigt die Datei auch den Port und die IRQs der Karte an. Zusätzlich zeigt die Karte auch die bevorzugten und möglichen (`preferred` und `acceptable`) Werte für verschiedene Parameter an. Das Ziel hierbei ist, PnP Karten perfekt einzustellen und Konflikte für IRQ und Ports zu vermeiden.

5.2.13. /proc/kcore

Diese Datei repräsentiert den physischen Speicher des Systems und wir im core-Dateiformat abgespeichert. Im Gegensatz zu den meisten `/proc` Dateien, zeigt `kcore` seine Größe an. Dieser Wert wird in Bytes angezeigt und entspricht der Größe des physischen Speichers (RAM) plus 4KB.

Der Inhalt dieser Datei ist so konzipiert, dass er nur von einem Debugger wie `gdb` untersucht werden kann, und ansonsten nicht lesbar ist.

Warnung

Öffnen Sie die virtuelle Datei `/proc/kcore` nicht. Die Inhalte der Datei werden als Textausgabe unlesbar auf dem Bildschirm angezeigt. Wenn Sie diese Datei unbeabsichtigt öffnen, drücken Sie [Strg]-[C], um den Prozess zu stoppen und kehren Sie mit `reset` zum Befehlszeilenprompt zurück.

5.2.14. /proc/kmsg

In dieser Datei befinden sich Mitteilungen, die vom Kernel erstellt wurden. Diese Mitteilungen werden dann von anderen Programmen, wie z.B. `/sbin/klogd`, hier abgerufen.

5.2.15. /proc/ksyms

Diese Datei enthält die vom Kernel exportierten Symbol-Definitionen, die von den Modul-Programmen benutzt werden, um ladbare Module dynamisch zu verlinken und einzubinden.

```
e003def4 speedo_debug [eepro100]
e003b04c eepro100_init [eepro100]
e00390c0 st_template [st]
e002104c RDINDOOR [megaraid]
e00210a4 callDone [megaraid]
e00226cc megaraid_detect [megaraid]
```

Der erste Spalte listet die Speicheradresse für die Kernelfunktion auf, die zweite Spalte bezieht sich auf den Namen der Funktion, und die letzte Spalte zeigt den Namen des geladenen Moduls an.

5.2.16. /proc/loadavg

Diese Datei bietet eine Übersicht über die durchschnittliche Auslastung der Prozessoren über Zeit, und liefert außerdem zusätzliche Informationen, die vom `uptime` und anderen Befehlen benutzt werden. Eine beispielhafte `/proc/loadavg` Datei finden Sie hier:

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

Die ersten drei Spalten messen die CPU-Ausnutzung der letzten 1, 5 und 10 Minuten. Die vierte Spalte zeigt die Anzahl der zur Zeit laufenden Prozesse und die Gesamtanzahl der Prozesse an. Die letzte Spalte zeigt die letzte Prozess-ID, die verwendet wurde.

5.2.17. /proc/locks

Diese Datei zeigt die Dateien, die zur Zeit vom Kernel gelockt (gesperrt) sind an. Der Inhalt dieser Datei enthält interne Debugging-Daten des Kernels und kann stark variieren, je nach Benutzungsgrad des Systems. Eine Beispiel `/proc/locks` Datei eines Systems mit leichter Belastung finden Sie hier:

```
1: FLOCK  ADVISORY  WRITE 807 03:05:308731 0 EOF c2a260c0 c025aa48 c2a26120
2: POSIX  ADVISORY  WRITE 708 03:05:308720 0 EOF c2a2611c c2a260c4 c025aa48
```

Jeder Sperre wird eine einmalige Zahl am Anfang jeder Zeile zugeordnet. Die zweite Spalte zeigt den verwendeten Sperr-Typ an, wobei `FLOCK` für die älteren UNIX Dateisperren des `flock` Systemaufrufs steht. `POSIX` wiederum steht für die neueren POSIX-Sperren mit dem `lockf` Systemaufruf.

Die dritte Spalte kann zwei Werte haben: `ADVISORY` oder `MANDATORY`. `ADVISORY` bedeutet, dass die Sperre andere Benutzer nicht vom Datenzugriff abhält; nur andere Sperr-Versuche werden verhindert. `MANDATORY` bedeutet, dass kein anderer Datenzugriff zugelassen wird, solange die Sperre bestehen bleibt. Die vierte Spalte zeigt an, ob die Sperre dem Eigentümer Lese- oder Schreibzugriff (`READ` oder `WRITE`) erlaubt und die fünfte Spalte zeigt die ID des gesperrten Prozesses an.

Die sechste Spalte zeigt die ID der gesperrten Datei, in folgendem Format an: *MAJOR-DEVICE*`:`*MINOR-DEVICE*`:`*INODE-NUMBER*. Die siebte Spalte zeigt Anfang und Ende der in der Datei gesperrten Region. Die übrigen Spalten zeigen auf Kernel-interne Datenstrukturen für spezielle Debugging-Funktionen und können ignoriert werden.

5.2.18. /proc/mdstat

Diese Datei enthält die aktuellen Informationen zu Konfigurationen mit mehreren Platten und RAID. Wenn Ihr System keine solche Konfiguration enthält, sieht Ihre `/proc/mdstat` Datei vermutlich so ähnlich aus:

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

Diese Datei bleibt solange in dem o.g. Zustand bis Sie ein Software-RAID erstellt haben oder `md` existiert. Dann können Sie `/proc/mdstat` anzeigen, um sich ein Bild davon zu machen, was gerade mit Ihren `md`*X* RAID-Geräten passiert.

Die folgende `/proc/mdstat` Datei zeigt ein System mit dem Gerät `md0`, das als RAID 1 Gerät konfiguriert ist und zur Zeit die Platten neu synchronisiert:

```
Personalities : [linear] [raid1]
read_ahead 1024 sectors
md0: active raid1 sda2[1] sdb2[0] 9940 blocks [2/2] [UU] resync=1% finish=12.3min
algorithm 2 [3/3] [UUU]
unused devices: <none>
```

5.2.19. /proc/meminfo

Dies ist eine der eher häufig benutzten Dateien im Verzeichnis /proc, da sie viele wertvolle Informationen über die RAM-Auslastung des Systems ausgibt.

Die folgende virtuelle Datei /proc/meminfo stammt von einem System mit 256MB Ram und 384MB Swap-Space:

```
        total:    used:    free:  shared: buffers:  cached:
Mem:  261709824 253407232  8302592        0 120745984 48689152
Swap: 402997248     8192 402989056
MemTotal:       255576 kB
MemFree:          8108 kB
MemShared:           0 kB
Buffers:        117916 kB
Cached:          47548 kB
Active:         135300 kB
Inact_dirty:     29276 kB
Inact_clean:       888 kB
Inact_target:        0 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       255576 kB
LowFree:          8108 kB
SwapTotal:      393552 kB
SwapFree:       393544 kB
```

Viele der hier ausgegebenen Informationen werden von den Befehlen free, top und ps verwendet. Die Ausgabe von free ist sogar im Aufbau und Inhalt ähnlich wie /proc/meminfo. Wenn Sie die Datei /proc/meminfo direkt ansehen, können Sie noch mehr Details ansehen:

- Mem — Zeigt den aktuellen Status des physischen Arbeitsspeichers im System mit einer kompletten Auflistung vom gesamten, benutzem, gemeinsam genutzem, gepuffertem und Cache-Speicher in Bytes (total, used, free, shared, buffered und cached).
- Swap — Zeigt die gesamte, benutzte und freie Menge von Swap in Bytes an (total, used und free).
- MemTotal — Gesamte RAM-Größe in Kilobytes.
- MemFree — Die Menge von physischem RAM, die vom System nicht benutzt wird, in Kilobytes.
- MemShared — Wird ab Kernel 2.4 nicht mehr benutzt, aber aus Kompatibilitätsgründen immer noch angezeigt.
- Buffers — Die Größe der physischen RAM in Kilobytes, der für Dateipufferung verwendet wird.
- Cached — Die Menge der physischen RAM, die als Cache verwendet wird, in Kilobyte.
- Active — Die Gesamtmenge des Puffer oder Page-Cache-Speicher in Kilobyte, der aktiv verwendet wird.
- Inact_dirty — Die Gesamtmenge von Puffer oder Cache-Seiten, die freigegeben werden können, in Kilobyte.
- Inact_clean — Die Gesamtmenge von Puffer oder Cache Seiten, die definitiv frei und verfügbar sind, in Kilobyte.
- Inact_target — Netto Menge von Zuordnungen pro Sekunden in Kilobyte, Durchschnitt pro Minute.
- HighTotal und HighFree — Die Gesamtmenge und der freie Speicher in Kilobytes, die nicht direkt in den Kernelbereich gemappt werden. Die Werte von HighTotal können von Kernel zu Kernel anders sein.

- `LowTotal` und `LowFree` — Die Gesamtmenge und der freie Speicher, die direkt in den Kernelbereich gemappt werden. Die Werte von `LowTotal` können von Kernel zu Kernel anders sein.
- `SwapTotal` — Die gesamte verfügbare Swapgröße, in Kilobyte.
- `SwapFree` — Die Gesamtmenge von freiem Swapspeicher, in Kilobyte.

5.2.20. /proc/misc

Diese Datei listet verschiedene Treiber auf, die im Major-Gerät mit der Nummer 10 aufgeführt sind:

```
135 rtc
  1 psaux
134 apm_bios
```

Die erste Spalte zeigt die Minor-Nummer des Geräts an und die zweite Spalte zeigt den benutzten Treiber an.

5.2.21. /proc/modules

Diese Datei zeigt eine Liste aller Module an, die im Kernel geladen wurden. Ihr Inhalt hängt von der Konfiguration und vom System ab; die Organisation sollte aber ähnlich sein wie in dieser Ausgabe von `/proc/modules`:

```
ide-cd                  27008   0 (autoclean)
cdrom                   28960   0 (autoclean) [ide-cd]
soundcore                4100   0 (autoclean)
agpgart                 31072   0 (unused)
binfmt_misc              5956   1
iscsi                   32672   0 (unused)
scsi_mod                94424   1 [iscsi]
autofs                  10628   0 (autoclean) (unused)
tulip                   48608   1
ext3                    60352   2
jbd                     39192   2 [ext3]
```

Die erste Spalte enthält den Namen des Moduls. Die zweite Spalte zeigt die Speichergröße des Moduls in Byte an. Die dritte Spalte zeigt an, ob das Modul zur Zeit geladen (`1`) oder nicht geladen (`0`) ist. Die letzte Spalte zeigt an, ob sich das Modul automatisch nach einer Zeit deaktivieren kann (`autoclean`) oder ob es zur Zeit nicht benutzt wird (`unused`). Jedes Modul mit einer Zeile, in der ein Name in Klammern (`[` und `]`) steht, zeigt an, dass dieses Modul ein anderes zum ordnungsgemäßen Funktionieren benötigt.

5.2.22. /proc/mounts

Diese Datei gibt Ihnen einen kurzen Überblick über alle Mounts im System:

```
rootfs / rootfs rw 0 0
/dev/hda2 / ext3 rw 0 0
/proc /proc proc rw 0 0
/dev/hda1 /boot ext3 rw 0 0
none /dev/pts devpts rw 0 0
none /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
```

Die Ausgabe aus dieser Datei ist sehr ähnlich zur Ausgabe von /etc/mtab, mit dem Unterschied, dass /proc/mount aktueller sein kann.

Die erste Spalte bezeichnet das Gerät das gemountet ist, wobei die zweite Spalte den zugehörigen Mount-Punkt anzeigt. Die dritte Spalte enthält den Dateisystemtyp und die vierte Spalte zeigt an, ob ein Dateisystem nur zum Lesen (ro) oder auch zum Schreiben (rw) gemountet ist. Die fünfte und sechste Spalte sind Dummy-Werte um das Format von /etc/mtab zu emulieren.

5.2.23. /proc/mtrr

Diese Datei bezieht sich auf die aktuellen Memory Type Range Registers (MTRRs), die im System verwendet werden. Wenn Ihre System Architektur MTRRs unterstüzt, könnte Ihre Datei /proc/mtrr so ähnlich wie diese aussehen:

```
reg00: base=0x00000000 (   0MB), size=  64MB: write-back, count=1
```

MTRRs werden seit der Intel P6 Familie benutzt (Pentium II und höher), um den Zugriff des Prozessors auf Speicherbereiche zu steuern. Wenn Sie eine Grafikkarte im PCI oder AGP Bus einsetzen, kann eine richtig konfigurierte /proc/mtrr Datei die Leistung um 150% erhöhen.

In den meisten Fällen werden diese Werte korrekt für Sie eingestellt. Weitere Informationen zu MTRRs und der Konfiguration per Hand finden Sie unter der URL: http://web1.linuxhq.com/kernel/v2.3/doc/mtrr.txt.html.

5.2.24. /proc/partitions

Die meisten Infomationen hier sind nicht sehr wichtig für die meisten Benutzer. Die folgenden Zeilen allerdings ausgenommen:

- major — Die Major-Nummer des Gerätes, auf dem diese Partition liegt. Die Major-Nummer in unserem Beispiel (3) entspricht dem Block-Gerät ide0 in /proc/devices.
- minor — Die Minor-Nummer des Geräts, auf dem diese Partition liegt. Diese dient dazu, die Partionen auf verschiedene physische Geräte aufzuteilen und hängt mit der Zahl am Ende des Partitionsnamens zusammen.
- #blocks — Listet die Anzahl von Plattenblöcken auf, die in einer bestimmten Partition enthalten sind.
- name — Der Name der Partition.

5.2.25. /proc/pci

Diese Datei enthält eine volle Auflistung jedes PCI-Geräts in Ihrem System. Wenn Sie viele PCI-Geräte im System haben, kann /proc/pci sehr lang werden. Ein Beispiel aus dieser Datei auf einem Standardrechner:

```
Bus  0, device   0, function  0:
  Host bridge: Intel Corporation 440BX/ZX - 82443BX/ZX Host bridge (rev 3).
    Master Capable.  Latency=64.
    Prefetchable 32 bit memory at 0xe4000000 [0xe7ffffff].
Bus  0, device   1, function  0:
  PCI bridge: Intel Corporation 440BX/ZX - 82443BX/ZX AGP bridge (rev 3).
    Master Capable.  Latency=64.  Min Gnt=128.
Bus  0, device   4, function  0:
  ISA bridge: Intel Corporation 82371AB PIIX4 ISA (rev 2).
```

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

Diese Ausgabe zeigt eine Liste aller PCI-Geräte an, sortiert nach Bus, Gerät und Funktion. Außer Namen und Version eines Gerätes, gibt Ihnen diese Liste auch detaillierte IRQ-Informationen, so dass ein Administrator Konflikten schnell beikommen kann.

Tipp

Für eine besser lesbare Version dieser Informationen geben Sie Folgendes ein:

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

5.2.26. /proc/slabinfo

Diese Datei gibt Ihnen Informationen über die Speicherbenutzung im *slab* Level. Linux Kernel über 2.2 benutzen *slab pools*, um Speicher über der Page-Ebene zu verwalten. Oft benutzte Objekte haben dabei eigene Slab Pools. Es folgt ein Ausschnitt einer typischen virtuellen Datei `/proc/slabinfo`:

```
slabinfo - version: 1.1
kmem_cache             64      68    112    2    2    1
nfs_write_data          0       0    384    0    0    1
nfs_read_data           0     160    384    0   16    1
nfs_page                0     200     96    0    5    1
ip_fib_hash            10     113     32    1    1    1
journal_head           51    7020     48    2   90    1
revoke_table            2     253     12    1    1    1
revoke_record           0       0     32    0    0    1
clip_arp_cache          0       0    128    0    0    1
ip_mrt_cache            0       0     96    0    0    1
```

Die Werte in dieser Datei stehen in folgender Reihenfolge: Cache-Name, Anzahl der aktiven Objekte, Anzahl der Gesamtobjekte, Größe des Objekts, Anzahl der Aktiven slabs (Blöcke) des Objekts, Gesamtanzahl der slabs des Objekkts und Anzahl der Seiten per slab.

Beachten Sie bitte, dass *active* in diesem Fall bedeutet, dass ein Objekt "in Verwendung" ist.

5.2.27. /proc/stat

Diese Datei enthält diverse Statistiken über das System seit dem letzten Neustart. Der Inhalt von `/proc/stat`, welcher auch sehr lang sein kann, fängt ähnlich wie unser Beispiel an:

```
cpu  1139111 3689 234449 84378914
cpu0 1139111 3689 234449 84378914
page 2675248 8567956
swap 10022 19226
intr 93326523 85756163 174412 0 3 3 0 6 0 1 0 428620 0 60330 0 1368304 5538681
disk_io: (3,0):(1408049,445601,5349480,962448,17135856)
ctxt 27269477
btime 886490134
processes 206458
```

Einige der bekannteren Statistiken sind:

- `cpu` — Misst die Anzahl von *Jiffies* (1/100 Sekunden), in denen das System im Benutzer-Modus, Benutzer-Modus mit niedriger Priorität (nice), System Modus und im Idle-Task war. Die Gesamtzahl für alle CPUs wird ganz oben ausgegeben und jede einzele CPU wird unten mit eigenen Statistiken aufgelistet.
- `page` — Anzahl der Speicherseiten, die das System von Platte und auf Platte geschrieben hat.
- `swap` — Anzahl der Swap-Seiten, die das System von Platte und auf Platte geschrieben hat.
- `intr` — Anzahl der Interrupts, die im System aufgetreten sind.
- `btime` — Die Boot-Zeit, gemessen in Sekunden seit dem 1 Januar 1970, auch bekannt als *epoch*.

5.2.28. /proc/swaps

Diese Datei misst den Swapspeicher und seine Auslastung. Für ein System mit nur einer Swap-Partition könnte die Ausgabe von `/proc/swap` so ähnlich aussehen:

```
Filename     Type       Size    Used   Priority
/dev/hda6    partition  136512  20024  -1
```

Obwohl Sie einige dieser Informationen auch in anderen Dateien im Verzeichnis `/proc` finden, liefert Ihnen die Datei `/proc/swap` einen Überblick über alle Swap-Dateinamen, Typen des Swap-Space und die Gesamtgröße sowie die verwendete Größe in Kilobyte. Die Prioritätsspalte ist sinnvoll wenn mehrere Swap-Dateien benutzt werden. Je niedriger die Priorität, desto wahrscheinlicher wird eine Swap-Datei benutzt.

5.2.29. /proc/uptime

Diese Datei enthält Informationen darüber, wie lange das System seit dem letzten Neustart läuft. Die Ausgabe von `/proc/uptime` ist relativ gering:

```
350735.47 234388.90
```

Die erste Zahl zeigt die Sekundenzahl an, die das System bereits läuft. Die zweite Zahl zeigt die Sekunden an, wielange die Maschine idle (im Leerlauf) war.

5.2.30. /proc/version

Diese Datei zeigt die Version des Linux-Kernels und des gcc an und außerdem die Version von Red Hat Linux, die auf dem System installiert ist:

```
Linux version 2.4.20-0.40 (user@foo.redhat.com)(gcc version 3.2.1 20021125
(Red Hat Linux 8.0 3.2.1-1)) #1 Tue Dec 3 20:50:18 EST 2002
```

Diese Information wird für eine Vielzahl von Zwecken benutzt, unter anderem um Versionsdaten am Login-Prompt auszugeben.

5.3. Verzeichnisse in /proc

Allgemeine Informationsgruppen bezüglich des Kernels werden in Verzeichnisse und Unterverzeichnisse in /proc sortiert.

5.3.1. Prozess-Verzeichnisse

Jedes /proc Verzeichnis enthält einige Verzeichnisse mit numerischen Namen. Eine Liste mit solchen fängt ähnlich dieser Liste an:

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

Diese Verzeichnisse heißen *Prozess-Verzeichnisse*, weil sie sich auf eine Prozess-ID beziehen und Informationen zu diesem Prozess enthalten. Der Eigentümer und die Gruppe jedes Prozess-Verzeichnisses wird auf die ID des Benutzers, der den Prozess ausführt, gesetzt. Wenn der Prozess beendet wird, verschwindet das zugehörige /proc Prozess-Verzeichnis.

Jedes Prozess-Verzeichnis enthält die folgenden Dateien:

- cmdline — Diese Datei enthält den Befehl, der bei Prozessstart ausgegeben wird.
- cpu — Bietet spezifische Informationen zur Prozessorlast aller CPUs an. Ein Prozess, der auf einem Dual-CPU-System läuft, könnte eine Ausgabe wie folgt haben:
  ```
  cpu  11 3
  cpu0 0 0
  cpu1 11 3
  ```
- cwd — Ein symbolischer Link zum aktuellen Arbeitsverzeichnis des Prozesses.
- environ — Gibt eine Liste von Umgebungsvariablen des Prozesses aus. Die Variablennamen werde in Großbuchstaben, die Werte in Kleinbuchstaben ausgegeben.
- exe — Ein symbolischer Link zur ausgeführten Datei des Prozesses.

- `fd` — Ein Verzeichnis mit allen Datei-Descriptors eines bestimmten Prozesses. Diese werden als nummerierte Links ausgegeben:

```
total 0
lrwx------    1 root     root           64 May  8 11:31 0 -> /dev/null
lrwx------    1 root     root           64 May  8 11:31 1 -> /dev/null
lrwx------    1 root     root           64 May  8 11:31 2 -> /dev/null
lrwx------    1 root     root           64 May  8 11:31 3 -> /dev/ptmx
lrwx------    1 root     root           64 May  8 11:31 4 -> socket:[7774817]
lrwx------    1 root     root           64 May  8 11:31 5 -> /dev/ptmx
lrwx------    1 root     root           64 May  8 11:31 6 -> socket:[7774829]
lrwx------    1 root     root           64 May  8 11:31 7 -> /dev/ptmx
```

- `maps` — Enthält Speicher-Maps zu den verschiedenen ausführbaren Dateien und Library-Dateien, die mit diesem Prozess zusammenhängen. Diese Datei kann sehr lang werden, wenn ein sehr komplexer Prozess ausgeführt wird, eine Beispielausgabe eines `sshd` Prozesses fängt so an:

```
08048000-08086000 r-xp 00000000 03:03 391479     /usr/sbin/sshd
08086000-08088000 rw-p 0003e000 03:03 391479     /usr/sbin/sshd
08088000-08095000 rwxp 00000000 00:00 0
40000000-40013000 r-xp 00000000 03:03 293205     /lib/ld-2.2.5.so
40013000-40014000 rw-p 00013000 03:03 293205     /lib/ld-2.2.5.so
40031000-40038000 r-xp 00000000 03:03 293282     /lib/libpam.so.0.75
40038000-40039000 rw-p 00006000 03:03 293282     /lib/libpam.so.0.75
40039000-4003a000 rw-p 00000000 00:00 0
4003a000-4003c000 r-xp 00000000 03:03 293218     /lib/libdl-2.2.5.so
4003c000-4003d000 rw-p 00001000 03:03 293218     /lib/libdl-2.2.5.so
```

- `mem` — Der Speicher, der von diesem Prozess benutzt wird. Diese Datei kann vom Benutzer nicht gelesen werden.
- `root` — Ein Link zum root Verzeichnis des Prozesses.
- `stat` — Der Status des Prozesses.
- `statm` — Der Status des Speichers, der von diesem Prozess benutzt wird. Eine beispielhafte `statm` Datei sieht aus wie folgt:

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

  Die sieben Spalten hängen mit verschiedenen Speicherstatistiken für den Prozess zusammen. Sie zeigen von links nach rechts verschiedene Aspekte des benutzten Speichers:

  1. Gesamte Programmgröße, in Kilobyte
  2. Größe der Speicherteile, in Kilobyte
  3. Anzahl der gemeinsam verwendeten Seiten
  4. Anzahl der Seiten mit Programmcode
  5. Anzahl der Seiten mit Stack/Daten
  6. Anzahl der Library-Seiten
  7. Anzahl der unsauberen Seiten

- `status` — Bietet den Status des Prozesses in einer lesbareren Form als `stat` oder `statm` an. Eine Beispielausgabe bei `sshd` sieht ähnlich wie folgt aus:

```
Name: sshd
State: S (sleeping)
Tgid: 797
Pid: 797
PPid: 1
TracerPid: 0
Uid: 0 0 0 0
```

```
Gid: 0 0 0 0
FDSize: 32
Groups:
VmSize:     3072 kB
VmLck:         0 kB
VmRSS:       840 kB
VmData:      104 kB
VmStk:        12 kB
VmExe:       300 kB
VmLib:      2528 kB
SigPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 8000000000001000
SigCgt: 0000000000014005
CapInh: 0000000000000000
CapPrm: 00000000ffffffff
CapEff: 00000000ffffffff
```

Die Informationen in dieser Ausgabe enthalten den Prozessnamen, die ID, den Status (wie z.B. `S (sleeping)` oder `R (running)`, Benutzer/Gruppe die den Prozess ausführen, und detailierte Daten bezüglich der Speicherauslastung.

5.3.1.1. /proc/self/

Das Verzeichnis `/proc/self` ist ein Link zum zur Zeit laufenden Prozess. Das erlaubt einem Prozess, sich selbst zu beobachten, ohne die eigene Prozess-ID zu kennen.

In einer Shell-Umgebung hat eine Auflistung des Verzeichnises `/proc/self` den gleichen Inhalt wie die Auflistung des Prozess-Verzeichnisses dieses Prozesses.

5.3.2. /proc/bus/

Dieses Verzeichnis enthält spezifische Informationen zu den verschiedenen Bussystemen, die auf einem System verfügbar sind. Zum Beispiel finden Sie auf einem Standard-PC mit ISA, PCI und USB Bus, aktuelle Daten zu jedem dieser Bussysteme im Verzeichnis `/proc/bus`.

Der Inhalt der Unterverzeichnisse und Dateien hängt sehr von der genauen Konfiguration Ihres Systems ab. Allerdings enthält jedes Verzeichnis für jedes der Bustypen mindestens ein Verzeichnis für jeden Bus eines Typen. Diese individuellen Bus-Verzeichnisse, normalerweise mit Zahlen wie `00` anzusprechen, enthalten binäre Dateien, die sich auf die verschiedenen Geräte auf dem Bus beziehen.

So hat ein System mit einem USB-Bus, aber ohne angeschlossene USB-Geräte ein `/proc/bus/usb` Verzeichnis mit verschiedenen Dateien:

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

Das Verzeichnis `/proc/bus/usb` enthält Dateien, die zu Geräten an den USB-Bussen gehören, genauso wie die Treiber, die gebraucht werden, um die Geräte zu benutzen. Das Verzeichnis `/proc/bus/usb/001` enthält alle Geräte am ersten USB-Bus. Wenn Sie sich den Inhalt der Datei `devices` ansehen, können Sie sehen, dass es sich um das USB root Hub auf dem Mainboard handelt:

```
T:  Bus=01 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#=  1 Spd=12  MxCh= 2
B:  Alloc=  0/900 us ( 0%), #Int=  0, #Iso=  0
D:  Ver= 1.00 Cls=09(hub  ) Sub=00 Prot=00 MxPS= 8 #Cfgs=  1
P:  Vendor=0000 ProdID=0000 Rev= 0.00
```

```
S:  Product=USB UHCI Root Hub
S:  SerialNumber=d400
C:* #Ifs= 1 Cfg#= 1 Atr=40 MxPwr=  0mA
I:  If#= 0 Alt= 0 #EPs= 1 Cls=09(hub  ) Sub=00 Prot=00 Driver=hub
E:  Ad=81(I) Atr=03(Int.) MxPS=   8 Ivl=255ms
```

5.3.3. /proc/driver/

Dieses Verzeichnis enthält Informationen zu bestimmten Treibern, die vom Kernel verwendet werden.

Eine allgemein hier zu findende Datei ist `rtc`, welche die Ausgabe des Treibers für die *Echtzeituhr (RTC)*, ein Gerät zum Erhalten der Zeit während der Rechner ausgeschaltet ist, darstellt. Eine Beispielausgabe von `/proc/driver/rtc`:

```
rtc_time : 01:38:43
rtc_date : 1998-02-13
rtc_epoch : 1900
alarm  : 00:00:00
DST_enable : no
BCD  : yes
24hr  : yes
square_wave : no
alarm_IRQ : no
update_IRQ : no
periodic_IRQ : no
periodic_freq : 1024
batt_status : okay
```

Informationen über den RTC finden Sie unter `/usr/src/linux-2.4/Documentation/rtc.txt`.

5.3.4. /proc/fs

Dieses Verzeichnis zeigt an, welche Dateisysteme exportiert werden. Arbeiten Sie mit einem NFS Server, geben Sie `cat /proc/fs/nfs/exports` ein, um die gemeinsam verwendeten Dateisysteme und die dafür gewährten Berechtigungen anzuzeigen. Weitere Informationen zur gemeinsamen Verwendung von Dateisystemen mit NFS finden Sie unter Kapitel 9.

5.3.5. /proc/ide/

Dieses Verzeichnis beinhaltet Informationen über IDE-Geräte auf diesem System. Jeder IDE-Kanal wird von einem seperaten Verzeichnis wie z.B. `/proc/ide/ide0` und `/proc/ide/ide1` repräsentiert. Zusätzlich gibt es eine `drivers` Datei, die die Versionsnummer der verschiedenen in diesem IDE-Kanal verwendeten Treiber darstellt:

```
ide-cdrom version 4.59
ide-floppy version 0.97
ide-disk version 1.10
```

Viele Chipsätze bieten eine Informationsdatei in diesem Verzeichnis an, welche zusätzliche Daten betreffend der Festplatten, die über die Kanäle angebunden sind, ausgibt. Zum Beispiel gibt ein generischer Intel PIIX4 Ultra 33 Chipsatz eine Datei `/proc/ide/piix` aus, die Ihnen zeigt, ob DMA oder UDMA für Geräte an den IDE-Kanälen aktiviert sind:

```
                              Intel PIIX4 Ultra 33 Chipset.
------------- Primary Channel ---------------- Secondary Channel -------------

                enabled                           enabled
------------- drive0 --------- drive1 -------- drive0 ---------- drive1 ------

DMA enabled:    yes              no              yes               no
UDMA enabled:   yes              no              no                no
UDMA enabled:   2                X               X                 X
UDMA
DMA
PIO
```

Im Verzeichnis eines IDE-Kanals, wie z.B. `ide0` für den ersten Kanal, finden Sie noch mehr Informationen. Die Datei `channel` zeigt die Kanalnummer an, wohingegen die Datei `model` den Bustyp am Kanal anzeigt, z.B. `pci`.

5.3.5.1. Das Geräte-Verzeichnis

In jedem IDE-Kanal-Verzeichnis befindet sich ein Geräte-Verzeichnis. Der Name des Geräte-Verzeichnisses entspricht dem Laufwerksbuchstaben im `/dev`-Verzeichnis. So ist z.B. das erste IDE-Laufwerk in `ide0` `hda`.

Anmerkung

Für jedes dieser Geräte-Verzeichnisse gibt es einen symbolischen Link zum `/proc/ide/` Verzeichnis.

Jedes Geräte-Verzeichnis enthält eine Sammlung von Informationen und Statistiken. Der Inhalt dieser Verzeichnisse verändert sich je nach angesprochenem Gerät. Einige der wichtigen Dateien, die bei verschiedenen Geräten vorhanden sind, umfassen unter anderem:

- `cache` — Der Geräte-Cache.
- `capacity` — Die Kapazität des Gerätes in 512 Byte Blöcken.
- `driver` — Treiber und Treiberversion, die benutzt wird, um das Gerät anzusprechen.
- `geometry` — Physische und logische Geometrie des Gerätes.
- `media` — Der Geräte-Typ, wie zum Beispiel `disk`
- `model` — Modellname oder Nummer des Gerätes
- `settings` — Eine Liste von aktuellen Parametern des Gerätes. Diese Datei enthält normalerweise einige wissenswerte, technische Informationen. Eine beispielhafte `settings` Datei für eine Standard IDE-Festplatte sieht so aus:

```
name                value           min           max           mode
----                -----           ---           ---           ----
bios_cyl            784             0             65535         rw
bios_head           255             0             255           rw
bios_sect           63              0             63            rw
breada_readahead    4               0             127           rw
bswap               0               0             1             r
current_speed       66              0             69            rw
file_readahead      0               0             2097151       rw
ide_scsi            0               0             1             rw
```

```
init_speed          66              0           69          rw
io_32bit            0               0           3           rw
keepsettings        0               0           1           rw
lun                 0               0           7           rw
max_kb_per_request  64              1           127         rw
multcount           8               0           8           rw
nice1               1               0           1           rw
nowerr              0               0           1           rw
number              0               0           3           rw
pio_mode            write-only      0           255         w
slow                0               0           1           rw
unmaskirq           0               0           1           rw
using_dma           1               0           1           rw
```

5.3.6. `/proc/irq/`

Dieses Verzeichnis wird benutzt, um IRQ zu CPU Verbindungen einzustellen. Dies erlaubt Ihnen, einen IRQ nur einer CPU zuzuweisen. Sie können eine CPU aber z.B. auch vom IRQ-Handling entbinden.

Jeder IRQ hat ein eigenes Verzeichnis, was die individuelle Konfiguration jedes IRQ ermöglicht. Die Datei `/proc/irq/prof_cpu_mask` ist eine Bitmaske, die die Standardwerte für die Datei `smp_affinity` im IRQ-Verzeichnis enthält. Die Werte in `smp_affinity` legen fest, welche CPUs diesen IRQ bearbeiten.

Weitere Informationen zum Verzeichnis `/proc/irq/` finden Sie unter

```
/usr/src/linux-2.4/Documentation/filesystems/proc.txt
```

5.3.7. `/proc/net/`

Dieses Verzeichnis bietet einen weitgehenden Einblick in verschiedene Netzwerk-Parameter und -Statistiken. Jede Datei deckt einen bestimmten Informationsbereich zum Systemnetzwerkbereich ab. Es folgt eine Teilliste dieser virtuellen Dateien:

- `arp` — Enthält die ARP-Tabelle des Kernels. Diese Datei ist besonders sinnvoll, um eine Hardware-Adresse einer IP-Adresse zuzuordnen.
- `atm` — Ein Verzeichnis, das Dateien mit verschiedenen Einstellungen und Statistiken zum *Asynchronous Transfer Mode (ATM)* enthält. Dieses Verzeichnis wird vor allem mit ATM-Netzkarten und ADSL-Karten benutzt.
- `dev` — Listet die verschiedenen Netzwerk-Geräte, die im System konfiguriert sind, mit Statistiken zum Senden und Empfangen, auf. Diese Datei zeigt Ihnen, welche Schnittstelle wieviel Bytes empfangen und gesendet hat, die Paketanzahl, Fehleranzahl und verlorene Pakete an.
- `dev_mcast` — Zeigt die verschiedenen Layer2 Multicast Gruppen an, auf denen ein Gerät zuhört.
- `igmp` — Listet die von diesem System zusammengefassten IP-Adressen auf.
- `ip_fwchains` — Wenn `ipchains` verwendet werden, zeigt diese virtuelle Datei alle aktuellen Regeln an.
- `ip_fwnames` — Wenn `ipchains` verwendet wird, listet diese virtuelle Datei alle Namen der Firewall-Ketten auf.
- `ip_masquerade` — Zeigt eine Tabelle mit Maskierungs-Informationen unter `ipchains` an.

- ip_mr_cache — Liste des Multicasting Routing Cache.
- ip_mr_vif — Liste der virtuellen Schnittstellen zum Multicasting.
- netstat — Enthält eine umfangreiche und detaillierte Sammlung von Netzwerk-Statistiken, mit TCP Timeouts, gesendeten und empfangenen SYN-Cookies und vielem mehr.
- psched — Liste der globalen Paket Scheduler Parametern.
- raw — Liste der Raw-Gerät Statistiken.
- route — Zeigt die Kernel-Routing-Tabelle an.
- rt_cache — Zeigt den aktuellen Routing Cache.
- snmp — Eine Liste von Simple Network Management Protocol (SNMP) Daten verschiedener Netzwerk-Protokolle.
- sockstat — Liefert Statistiken zum Socket.
- tcp — Enthält detaillierte Informationen zum TCP-Socket.
- tr_rif — Die Token Ring RIF Routing Tabelle.
- udp — Enthält detaillierte Informationen zum UDP-Socket.
- unix — Listet die UNIX-Domain-Sockets auf, die zur Zeit benutzt werden.
- wireless — Zeigt Informationen zu Wireless Interfaces.

5.3.8. /proc/scsi/

Dieses Verzeichnis ist analog zum Verzeichnis /proc/ide, kann aber nur für verbundene SCSI-Geräte verwendet werden.

Die wichtigste Datei hier ist /proc/scsi/scsi, welche eine Liste mit allen erkannten SCSI-Geräten enthält. Aus dieser Auflistung können Sie den Typ des Gerätes, den Modell-Namen, den Hersteller und die SCSI Kanal/ID-Daten abrufen.

Wenn ein System zum Beispiel ein SCSI CD-ROM, ein Bandlaufwerk, Festplatten und einen RAID-Controller beinhaltet, könnte die Datei ähnlich wie in diesem Beispiel aussehen:

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

Jeder SCSI-Treiber, der vom System benutzt wird, hat ein eigenes Verzeichnis in /proc/scsi, welches spezifische Dateien für jeden Controller enthält. Für unser Beispiel oben gibt es also die Verzeichnisse aic7xxx und megaraid, da diese beiden Treiber benutzt werden. Die Dateien in diesen beiden Unterverzeichnissen beinhalten typischerweise I/O Adressbereiche, IRQ-Informationen und Statistiken für den SCSI-Controller, der den Treiber benutzt. Jeder Controller liefert Informationen in verschiedener Größe und Art. Der Adaptec AIC-7880 Ultra SCSI Hostadapter in unserem Beispiel gibt folgende Ausgabe:

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

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

Statistics:


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


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

Dieser Bildschirm zeigt die Transfergeschwindigkeiten zu den verschiedenen SCSI-Geräten, die an den Controller angeschlossen sind, basierend auf der Channel-ID, sowie detaillierte Statistiken zu der Anzahl und Größe der Dateien, die von diesem Gerät gelesen oder geschrieben wurden. Der oben angegebenen Ausgabe entnehmen Sie, dass der Controller mit dem CD-ROM-Laufwerk mit 20 Megabyte pro Sekunde kommuniziert, während das Bandlaufwerk nur mit 10 Megabytes kommuniziert.

5.3.9. /proc/sys/

Das Verzeichnis /proc/sys/ unterscheidet sich von /proc, weil es nicht nur eine Menge Informationen über das System zeigt, sondern auch Administratoren erlaubt, Kerneleigenschaften sofort zu aktivieren oder zu deaktivieren.

Warnung

Versuchen Sie niemals, Ihre Kernel-Einstellungen auf einem Produktionssystem mit den Dateien in /proc/sys zu optimieren. Es kann in manchen Fällen passieren, dass eine Einstellung den Kernel instabil macht und damit ein Neustart erforderlich wird.

Überprüfen Sie daher unbedingt die Korrektheit der Syntax, bevor Sie eine Änderung in /proc/sys vornehmen.

Ob eine Datei konfiguriert werden kann oder nur Informationen liefern soll, findet man am besten heraus, indem man sie über -l an einem Shell-Prompt anzeigt. Wenn die Datei schreibbar ist, können Sie diese zum Konfigurieren des Kernels verwenden. Zum Beispiel sieht eine Auflistung von /proc/sys/fs so aus:

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

Hier sind die Dateien dir-notify-enable und file-max schreibbar und können deshalb benutzt werden, um den Kernel zu konfigurieren. Die anderen Dateien geben nur Informationen zu den aktuellen Einstellungen des Kernels aus.

Ein Wert in einer Datei in /proc/sys wird geändert, indem der neue Wert in diese Datei geschrieben wird. Zum Beispiel benutzt man, um den System Request Key in einem laufenden Kernel zu aktivieren, folgenden Befehl:

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

Dies ändert den Wert der Datei sysrq von 0 (off) auf 1 (on).

Der Sinn des System Request Key ist es, Ihnen zu erlauben, dem Kernel direkte Anweisungen mit einer simplen Tastenkombination zu geben, um den Rechner z.B. direkt herunter zu fahren, das System neu zu starten, alle Dateisystempuffer zu schreiben oder wichtige Informationen auf Ihre Konsole zu schreiben. Dieses Feature ist sehr sinnvoll, wenn Sie einen Development Kernel benutzen, oder Systemeinfrieren beobachten. Da sie jedoch für unbewachte Konsolen ein Sicherheitsrisiko darstellt, wird dies standardmäßig unter Red Hat Linux ausgeschaltet.

Weitere Informationen zum System Request Key finden Sie unter /usr/src/linux-2.4/Documentation/sysrq.txt.

Einige Konfigurations-Dateien in /proc/sys enthalten mehr als einen Wert. Um neue Werte in solchen Dateien zu speichern, müssen Sie ein Leerzeichen zwischen jeden Wert setzen, den Sie übergeben. Sehen Sie die Anwendung mit dem Befehl echo hier:

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

Anmerkung

Konfigurationsänderungen, die Sie mit `echo` vornehmen gehen automatisch verloren, wenn das System neu gestartet wird. Um Ihre Konfigurations-Änderungen nach dem Booten wirksam werden zu lassen, lesen Sie bitte Abschnitt 5.4.

Das Verzeichnis `/proc/sys` enthält verschiedene Unterverzeichnisse, die verschiedene Bereiche des laufenden Kernel kontrollieren.

5.3.9.1. /proc/sys/dev/

Dieses Verzeichnis bietet Optionen für bestimmte Geräte im System an. Viele Systeme haben mindestens zwei Verzeichnisse: `cdrom` und `raid`, aber benutzerdefinierte Kernel können andere Verzeichnisse haben, wie z.B. `parport`, das es ermöglicht, den parallelen Port zwischen mehreren Treibern zu teilen.

Das `cdrom` Verzeichnis enthält eine Datei namens `info`, die einige wichtige CD-ROM-Parameter ausgibt:

```
CD-ROM information, Id: cdrom.c 3.12 2000/10/18

drive name:  hdc
drive speed:  32
drive # of slots: 1
Can close tray:  1
Can open tray:  1
Can lock tray:  1
Can change speed: 1
Can select disk: 0
Can read multisession: 1
Can read MCN:  1
Reports media changed: 1
Can play audio:  1
Can write CD-R:  0
Can write CD-RW: 0
Can read DVD:  0
Can write DVD-R: 0
Can write DVD-RAM: 0
```

Diese Datei kann benutzt werden, um die Fähigkeiten einer unbekannten CD-ROM herauszufinden. Wenn mehrere Laufwerke vorhanden sind, hat jedes Gerät seine eigene Informationsspalte.

Verschiedene Dateien in `/proc/sys/dev/cdrom`, wie z.B. `autoclose` und `checkmedia`, können benutzt werden, um das CD-ROM Laufwerk einzustellen. Mit dem Befehl `echo` können Sie ein Feature aktivieren oder deaktivieren.

Wenn RAID-Unterstützung in den Kernel integriert wurde, ist ein Verzeichnis `/proc/sys/dev/raid` mit mindestens zwei Dateien vorhanden: `speed_limit_min` und `speed_limit_max`. Diese Einstellungen legen die Beschleunigung eines RAID Gerät für besonders I/O intensive Aufgaben, wie z.B. beim Synchronisieren von Festplatten, fest.

5.3.9.2. /proc/sys/fs/

Dieses Verzeichnis enthält eine Liste von Optionen und Informationen zu verschiedenen Einstellungen des Dateisystem, inklusive Quoten, Datei-Handles, Inoden und dentry-Informationen.

Das Verzeichnis `binfmt_misc` wirt benutzt, um Kernel Support für verschiedene Binär-Formate anzubieten.

Die wichtigen Dateien im Verzeichnis `/proc/sys/fs` sind:

- `dentry-state` — Zeigt den Status des Verzeichnis-Caches an. Diese Datei sieht so ähnlich wie diese aus:
  ```
  57411 52939 45 0 0 0
  ```
  Die erste Zahl zeigt die Gesamtzahl der Verzeichnis-Cache Einträge an, die zweite Zahl zeigt die Anzahl der nicht benutzten Einträgen an. Die dritte Zahl zeigt die Sekunden zwischem dem Löschen und dem erneuten Aufnehmen eines Verzeichnisses an. Die vierte misst die Seiten, die gerade vom System angefordert werden. Die letzten zwei Zahlen werden nicht benutzt und zeigen nur Nullen an.
- `dquot-nr` — Zeigt die maximale Anzahl von zwischengespeicherten Quoten-Einträgen an.
- `file-max` — Erlaubt es, die maximale Anzahl von Datei-Handles, die der Kernel zuweist, zu ändern. Diesen Wert zu ändern kann Fehler lösen, die beim Zuweisen von Datei-Handles entstehen können.
- `file-nr` — Zeigt die Anzahl zugewiesener, benutzter, und die maximale Anzahl der Datei-Handles an.
- `overflowgid` und `overflowuid` — Definiert die feste Benutzer- und Gruppen-ID, falls das System nur 16-bit Gruppen- und Benutzer-IDs unterstützt.
- `super-max` — Kontrolliert die maximal verfügbare Anzahl von Superblöcken.
- `super-nr` — Zeigt die aktuelle Anzahl der benutzten Superblöcke an.

5.3.9.3. /proc/sys/kernel/

Dieses Verzeichnis enthält eine Vielzahl von verschiedenen Konfigurationsdateien, die direkt die Kernelfunktion beeinflussen. Einige der wichtigsten Dateien sind unter anderem:

- `acct` — Kontrolliert die Aufhebung von Prozess Accounting, basierend auf der Prozentzahl des verfügbaren freien Speichers, der auf dem Dateisystem, das den Log enthält, verfügbar ist. Dieser Log sieht gewöhnlich so aus:
  ```
  4 2 30
  ```
  Der zweite Wert setzt den Schwellenwert des freien Speichers, wenn das Logging unterbrochen werden soll; der erste Wert hingegen zeigt den Wert an, wann das Logging wieder aufgenommen werden soll. Der dritte Wert zeigt das Intervall in Sekunden, in dem der Kernel das Dateisystem abfragt, um zu entscheiden, ob das Logging wieder aufgenommen oder unterbrochen werden soll.
- `cap-bound` — Kontrolliert die *Capability Bounding* Einstellungen. Diese bieten eine Liste von Möglichkeiten, die jeder Prozess auf dem System benutzten kann. Wenn eine Möglichkeit hier nicht aufgelistet ist, dann kann kein Prozess, egal mit welchen Privilegien, diese benutzen. Dies macht das System dadurch, dass bestimmte Dinge nicht ausgeführt werden können, sicherer (wenigstens nach einem bestimmten Punkt im Boot-Prozess nicht).

  Eine Liste gültiger Werte für diese virtuelle Datei finden Sie unter `/usr/src/linux-2.4/include/linux/capability.h`. Weitere Informationen zum Capability Bonding finden Sie unter: http://lwn.net/1999/1202/kernel.php3.

- `ctrl-alt-del` — Stellt ein, ob die Tastenkombination [Strg]-[Alt]-[Entf] den Rechner mittels des `init` Befehls (Wert `0`) neu startet oder einen sofortigen Neustart ohne Puffer-Synchronisation vornimmt; (Wert `1`).
- `domainname` — Erlaubt es, den Domainnamen des Systems zu konfigurieren, wie z.B. `example.com`.
- `hostname` — Erlaubt es, den Hostnamen des Systems zu konfigurieren, wie z.B. `www.example.com`.
- `hotplug` — Konfiguriert das Programm, welches benutzt wird, wenn eine Konfigurationsänderung vom System erkannt wird. Dies wird vor allem mit dem USB und dem Cardbus PCI benutzt. Der Standardwert `/sbin/hotplug` sollte nicht geändert werden, außer wenn Sie ein neues Programm testen, dass diese Rolle ausfüllt.
- `modprobe` — Stellt den Ort des Programms ein, das Kernel-Module bei Bedarf lädt. Der Standardwert von `/sbin/modprobe` zeigt an, dass `kmod` dieses Programm aufruft, wenn ein Kernel Thread `kmod` aufruft, um ein Modul zu laden.
- `msgmax` — Setzt die maximale Größe von gesendeten Mitteilungen von einem Prozess zum anderen (Standardwert: `8192` Bytes). Mit dem Erhöhen dieses Wertes sollten Sie vorsichtig sein, weil zwischengespeicherte Werte in nicht auslagerbarem Kernel-Speicher abgelegt werden, und jede Erhöhung in `msgmax` die RAM-Erfordernisse im System erhöhen.
- `msgmnb` — Setzt die maximale Anzahl von Bytes in einer einzelnen Mitteilungs-Queue. Standard ist hier `16384`.
- `msgmni` — Setzt die maximale Anzahl von Mitteilungs-Queue-IDs. Standard ist `16`.
- `osrelease` — Listet die Linux-Kernel Releasenummer auf. Diese Datei kann nur durch Neuübersetzung und Neukompilierung des Kernels verändert werden.
- `ostype` — Zeigt den Typ des Betriebssystems an. Diese Datei zeigt normalerweise `Linux` an; dieser Wert kann nur durch Ändern der Kernel-Quellen und Neukompilieren geändert werden.
- `overflowgid` und `overflowuid` — Definiert die feste Gruppen- und Benutzer-ID, die für Systemaufrufe bei Architekturen, die nur 16-bit Gruppen- und Benutzer-IDs unterstützen, benutzt werden.
- `panic` — Definiert die Anzahl von Sekunden, um die der Kernel den Neustart verschiebt, wenn ein "Kernel-Panik" auftritt. Dieser Wert steht normal auf `0`, was einen automatischen Neustart nach einer "Kernel-Panik" deaktiviert.
- `printk` — Diese Datei kontrolliert eine Vielzahl von Einstellungen zum Anzeigen und Loggen von Fehlermitteilungen. Jede Fehlermeldung vom Kernel hat einen *loglevel*, der die Wichtigkeit der Mitteilung wiedergibt. Die Loglevel-Werte teilen sich wie folgt auf:
  - `0` — Ein Kernel Notfall. Das System ist nicht benutzbar.
  - `1` — Kernel-Alarm, es müssen sofort Gegenmaßnahmen eingeleitet werden.
  - `2` — Der Kernel ist in kritischem Zustand.
  - `3` — Allgemeiner Kernel-Fehler.
  - `4` — Allgemeine Kernel-Warnung.
  - `5` — Kernel-Mitteilung zu einem normalen, jedoch ernstzunehmendem Zustand.
  - `6` — Kernel Informations-Mitteilung.
  - `7` — Kernel Debugging-Mitteilung.

  Vier Werte finden sich in der Datei `printk`:
  ```
  6 4 1 7
  ```
  Jede dieser Werte definiert eine andere Regel zum Verarbeiten von Fehlermeldungen. Der erste Wert, *Konsolen Loglevel* genannt, definiert die niedrigste Priorität von Mitteilungen, die auf die

Konsole ausgegeben werden (je niedriger die Priorität, desto höher die Loglevel-Nummer). Der zweite Wert setzt den Standart-Loglevel für Mitteilungen, welche keinen Loglevel gesetzt haben. Der dritte Wert setzt den niedrigsten Loglevel Konfigurationswert für den Konsolen Loglevel. Der letzte Wert setzt den Standardwert für den Konsolen-Loglevel.

- `rtsig-max` — Konfiguriert die maximale Anzahl an POSIX-Echtzeitsignalen, die das System gespeichert haben kann. Der Standardwert ist: `1024`.
- `rtsig-nr` — Die aktuelle Anzahl von POSIX-Echzeitsignalen, die zur Zeit vom Kernel zwischengespeichert werden.
- `sem` — Diese Datei konfiguriert die Semaphore-Einstellungen im Kernel. Eine *semaphore* ist ein System V IPC-Objekt, das benutzt wird, um den Einsatz eines bestimmten Prozesses zu überwachen.
- `shmall` — Zeigt den Gesamtwert des gemeinsam verwendeten Speichers in Bytes an, der gleichzeitig im System benutzt werden kann. Dieser Wert ist normalerweise: `2097152`.
- `shmmax` — Stellt die größte Speichersegmentgröße in Bytes ein, die vom Kernel erlaubt wird. Dieser Wert ist normalerweise `33554432`. Der Kernel unterstützt allerdings viel größere Werte.
- `shmmni` — Stellt die maximale Anzahl von gemeisam genutzten Speichersegmenten für das ganze System ein. Dieser Wert hat den Standardwert `4096`.
- `sysrq` — Aktiviert den System Request Key, wenn dieser Wert nicht auf das standardmäßige `0` gesetzt ist. Einzelheiten zum System Request Key finden Sie unter Abschnitt 5.3.9.
- `threads-max` — Stellt die maximale Anzahl von Threads, die vom Kernel genutzt werden können, ein. Standardwert: `4095`.
- `version` — Zeigt Datum und Zeit der letzten Kernel-Kompilierung an. Das erste Feld in dieser Datei, wie z.B. `#3` zeigt an, wie oft ein Kernel aus den Quellen neukompiliert wurde.

Das Verzeichnis `random` speichert eine Anzahl von Werten, die zum Erzeugen von Zufallszahlen im Kernel verwendet werden.

5.3.9.4. /proc/sys/net/

Dieses Verzeichnis enthält Unterverzeichnisse über verschiedene Netzwerk-Themen. Verschiedene Konfigurationen zur Kernel-Kompilierung erzeugen hier verschiedene Verzeichnisse, wie z.B. `appletalk`, `ethernet`, `ipv4`, `ipx` und `ipv6`. In diesen Verzeichnissen können Sie verschiedene Netzwerk-Einstellungen für diese Konfiguration am laufenden System ändern.

Aufgrund den vielfältigen Netzwerk-Optionen, die in Linux verwendet werden können, werden wir nur die wichtigsten Verzeichnisse in `/proc/sys/net` vorstellen.

Das Verzeichnis `/proc/sys/net/core/` enthält eine Vielzahl von Einstellungen, die die Interaktion zwischen Kernel und Netzwerkschichten beeinflussen. Die wichtigsten Dateien sind hier:

- `message_burst` — Die Anzahl Zehntelsekunden, die benötigt werden, um eine neue Warnungsmitteilung zu schreiben. Das wird benutzt, um *Denial of Service* (*DoS*) Angriffe zu vermeiden; die Standardeinstellung ist: `50`.
- `message_cost` — Wird auch verwendet, um DoS Angriffe zu vermeiden, indem ein Cost-Faktor auf jede Warnung gesetzt wird. Je höher der Wert dieser Datei (Standard ist `5`), desto eher wird die Warnung ignoriert.

  Eine DoS-Attacke bedeutet, dass ein Angreifer Ihr System mit Anfragen überhäuft, die Fehler erzeugen und ihre Diskpartitionen mit Logdateien füllen oder Ihre Systemressourcen zum Fehlerloggen verbrauchen. Die Einstellungen in `message_burst` und `message_cost` sind dazu da, ein Gleichgewicht zwischen gutem Logging und einem geringen Risiko einzustellen.

- `netdev_max_backlog` — Setzt die maximale Nummer von Paketen, die in die Warteschlange gestellt werden, wenn eine Schnittstelle Pakete schneller empfängt, als der Kernel diese verarbeiten kann. Der Standardwert hier ist: `300`.
- `optmem_max` — Konfiguriert die maximale zusätzliche Puffergröße pro Socket.
- `rmem_default` — Setzt die Standardgröße für den Empfangspuffer in Byte.
- `rmem_max` — Setzt die Maximalgröße des Empfangspuffers in Byte.
- `wmem_default` — Setzt die Standardgröße für den Sendepuffer in Byte.
- `wmem_max` — Setzt die Maximalgröße für den Sendepuffer in Byte.

Das Verzeichnis `/proc/sys/net/ipv4/` enthält weitere Netzwerkeinstellungen. Viele dieser Einstellungen, die zusammen verwendet werden, sind sehr hilfreich bei der Verhinderung von Angriffen auf das System oder bei der Verwendung des Systems als Router.

Achtung

Eine irrtümliche Änderung dieser Dateien kann die Netzwerkverbindungen beeinträchtigen.

Einige der wichtigsten Dateien im Verzeichnis `/proc/sys/net/ipv4`:

- `icmp_destunreach_rate`, `icmp_echoreply_rate`, `icmp_paramprob_rate` und `icmp_timeexeed_rate` — Stellt die maximale ICMP Send-Paket Rate in 1/100 Sekunden (bei Intel Systemen) an Hosts unter verschiedenen Bedingungen ein. Eine Einstellung von `0` entfernt alle Verzögerungen und sollte nicht eingestellt werden.
- `icmp_echo_ignore_all` und `icmp_echo_ignore_broadcasts` — Erlaubt dem Kernel, ICMP ECHO Pakete von allen Hosts oder nur solche von Broadcast- oder Multicast-Adressen zu ignorieren. Eine `0` erlaubt dem Kernel zu antworten, eine `1` ignoriert diese Pakete.
- `ip_default_ttl` — Stellt die Standard *Time To Live (TTL)* ein, die die Anzahl von Sprüngen limitiert, bevor ein Paket sein Ziel erreicht. Eine Erhöhung dieses Wertes kann unter Umständen die Systemleistung beeinträchtigen.
- `ip_forward` — Erlaubt Schnittstellen im System, Pakete zu einer anderen weiterzuleiten. Standardmäßig ist diese Datei auf `0` gesetzt, um das Weiterleiten auszuschalten. Eine `1` aktiviert die Paketweiterleitung.
- `ip_local_port_range` — legt die Ports fest, die von TCP oder UDP benutzt werden, wenn ein lokaler Port gebraucht wird. Die erste Zahl ist der niedrigste Port und die zweite Zahl steht für den höchsten benutzten Port. Jedes System, für das erwartet wird, dass es mehr als die Standard Ports 1024 bis 4999 benötigt, sollte die Werte 32768 bis 61000 verwenden.
- `tcp_syn_retries` — Bietet eine Grenze dafür an, wie oft Ihr System ein SYN Paket versucht zu übertragen, wenn eine Verbindung versucht wird.
- `tcp_retries1` — Stellt die Anzahl von zugelassenen Neu-Übertragungen ein, wenn versucht wird einer eingehenden Verbindung zu antworten. Standardwert ist hier `3`.
- `tcp_retries2` — Stellt die Anzahl von erlaubten Neu-Übertragungen von TCP Paketen ein. Standardwert ist `15`.

Die Datei `/usr/src/linux-2.4/Documentation/networking/ip-sysctl.txt` enthält eine komplette Liste der im Verzeichnis `/proc/sys/net/ipv4/` verfügbaren Dateien und Optionen.

Eine Anzahl anderer Verzeichnisse in `/proc/sys/net/ipv4` behandeln spezifische Inhalte. Das Verzeichnis `/proc/sys/net/ipv4/conf/` erlaubt jeder der Systemschnittstellen eine unterschiedliche Konfiguration und lässt Standard Werte für nicht-konfigurierte Schnittstellen (im Unterverzeich-

nis /proc/sys/net/ipv4/conf/default/), und Einstellungen, die alle anderen Konfigurationen überschreiben (im Verzeichnis /proc/sys/net/ipv4/conf/all/), zu.

Um Verbindungen zwischen direkten Nachbarn (hier jedes andere System, das direkt an das System angeschlossen ist) zu überwachen, bietet das Verzeichnis /proc/sys/net/ipv4/neigh/ (steht für neighbors) spezielle Konfigurationen für jede Schnittstelle an. Das erlaubt Ihnen, Systeme denen Sie aufgrund ihrer örtlichen Nähe mehr vertrauen, anders zu behandeln. Es macht es gleichzeitig aber auch möglich, örtlich entfernte Systeme mit festen Regeln zu belegen.

Das Routen über IPV4 besitzt auch ein eigenes Verzeichnis /proc/sys/net/ipv4/route/. Im Gegensatz zu conf und neigh, enthält das /proc/sys/net/ipv4/route/ Verzeichnis Spezifikationen, die das Routing auf allen Systemschnittstellen beeinflusst. Viele dieser Einstellungen, wie z.B. max_size, max_delay und min_delay, hängen mit der Einstellung des Routing Caches zusammen. Um den Routing Cache zu löschen, schreiben Sie einen beliebigen Inhalt in die Datei flush.

Zusätzliche Informationen über diese Verzeichnisse und die möglichen Werte zur Konfiguration finden Sie unter /usr/src/linux-2.4/Documentation/filesystems/proc.txt.

5.3.9.5. /proc/sys/vm/

Dieses Verzeichnis erleichtert die Konfiguration des virtuellen Speicher-Subsystems des Linux Kernels (VM). Der Kernel macht ausgiebigen und intelligenten Gebrauch von virtuellem Speicher, der auch Swap-Speicher genannt wird.

Die folgenden Dateien findet man normalerweise im Verzeichnis /proc/sys/vm/:

- bdflush — Setzt verschiedene Werte, in Bezug auf den bdflush Kernel-Daemon.
- buffermem — Erlaubt es Ihnen, den Wert des gesamten System-Speichers einzustellen, der zum Puffern verwendet wird. Eine typische Ausgabe dieser Datei sieht wie folgt aus:
  ```
  2       10      60
  ```
  Die ersten und letzten Werte setzen den minimalen und maximalen Prozentsatz des Speichers, der als Pufferspeicher verwendet wird. Der mittlere Wert setzt den Prozentsatz von Systemspeicher, der als Puffer verwendet wird, ab dem das Memory Management anfängt, Puffer mehr als andere Speichertypen zu löschen, um Speichermangel auszugleichen.
- kswapd — Stellt verschiedene Werte, in Zusammenhang mit dem Kernel-Swap-Daemon ein; kswapd. Diese Datei hat drei Werte:
  ```
  512 32 8
  ```
  Der erste Wert setzt die maximale Anzahl von Seiten, die kswapd in einem Versuch zu löschen versucht. Je größer diese Zahl, desto schneller kann der Kernel auf freie Seiten zurückgreifen. Der zweite Wert setzt die minimale Anzahl von Versuchen, die kswapd versucht, eine Seite zu löschen. Der dritte Wert setzt die Anzahl von Seiten, die kswapd in einem Versuch zu schreiben versucht. Ein richtiges Einstellen des letzten Wertes kann die Systemleistung auf Kosten einer Menge Swap-Platzes erhöhen, indem der Kernel Seiten in großen Blöcken schreibt und dabei die Anzahl der Plattenzugriffe verringert.
- max_map_count — Konfiguriert die maximale Anzahl von Speicher-Map-Bereichen, die ein Prozess haben darf. In den meisten Fällen ist ein Standardwert von 65536 angemessen.
- overcommit_memory — wenn dies auf den Standardwert von 0 gesetzt ist, schätzt der Kernel einen verfügbaren Speicherumfang und lässt Anfragen scheitern, die eindeutig ungültig sind. Da bei der Speicherzuordnung eher ein heuristischer als ein genauer Algorithmus verwendet wird, kann es manchmal zu einer Überlastung des Systems kommen.

  Wenn overcommit_memory auf 1 gesetzt ist, erhöht sich die Wahrscheinlichkeit einer Systemüberlastung. Das gleiche gilt für die Durchführung von speicherintensiven Aufgaben, wie die, die von einigen wissenschaftlichen Softwareprogrammen verwendet werden.

Für Kunden, die ein geringeres Risiko einer Systemüberladung eingehen wollen, wurden folgende zwei Optionen hinzugefügt. Setzt man `overcommit_memory` auf `2` schlägt dies fehl, wenn eine Speicheranfrage mehr als die Hälfte des physischen RAM plus Swap ausmacht. Beim Setzen auf `3` scheitert dies, wenn eine Speicheranfrage größer ist, als Swap alleine fassen kann.

- `pagecache` — Stellt die Menge von Speicher ein, die vom Seiten-Cache verwendet wird. Die Werte in `pagecache` sind Prozentsätze, und funktionieren ähnlich wie in `buffermem` um die minimale und maximale Anzahl von verfügbarem Seiten-Cache zu erzwingen.
- `page-cluster` — Stellt die Anzahl von Seiten, die auf einmal gelesen werden sollen, ein. Der Standardwert `4`, der sich eigentlich auf 16 Seiten bezieht, reicht für die meisten Systeme aus.
- `pagetable_cache` — Stellt die Anzahl von Seiten ein, die auf Pro-Prozessor Basis zwischengespeichert werden, ein. Der erste und zweite Wert beziehen sich auf die minmale und die maximale Anzahl von Seitentabellen.

Zusätzliche Informationen hierzu finden Sie in `/usr/src/linux-2.4/Documentation/sysctl/vm.txt`.

5.3.10. `/proc/sysvipc/`

Dieses Verzeichnis enthält Informationen über die System V IPC-Ressourcen. Die Dateien in diesem Verzeichnis hängen mit den System V IPC-Aufrufen zusammen (`msg`), Semaphores (`sem`) und gemeinsam benutzter Speicher (`shm`).

5.3.11. `/proc/tty/`

Dieses Verzeichnis enthält Informationen über die verfügbaren und zur Zeit benutzten TTY-Geräte im System. Früher *teletype device* genannt, werden heute alle Buchstaben-orientierten Daten Terminals als TTY-Geräte bezeichnet.

Unter Linux gibt es drei verschiedene Arten von TTY-Geräten. *Serielle Geräte* werden mit seriellen Verbindungen benutzt, wie z.B. mit Modems oder seriellen Kabeln. *Virtuelle Terminals* erzeugen die normalen Konsolenverbindungen, wie die virtuellen Konsolen, die verfügbar sind, wenn Sie [Alt]-[<F-key>] auf einer Systemkonsole drücken. *Pseudo Terminals* erzeugen eine zwei-Wege Kommunikation, die von einigen höherrangigen Applikationen, wie z.B. XFree86 verwendet werden.

Die Datei `drivers` enthält eine Liste der TTY-Geräte, die zur Zeit benutzt werden:

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

Die Datei `/proc/tty/driver/serial` listet die Nutzungs-Statistik und den Status jedes der seriellen TTY-Geräte auf.

Damit TTY-Geräte ähnlich wie Netzwerk-Geräte benutzt werden können, stellt der Kernel *line discipline* für das Gerät ein. Das erlaubt dem Treiber, einen bestimmten Headertyp mit jedem Datenblock, der über das Gerät geht, zu transferieren; dieser Header macht das Paket zu einem Paket in einem

Stream. SLIP und PPP sind allgemein bekannte Line Disciplines und werden vor allem benutzt, um Systeme über eine serielle Verbindung zu koppeln.

Registrierte Line Disciplines werden in der Datei `ldiscs` gespeichert; detaillierte Informationen finden Sie im Verzeichnis `ldisc`.

5.4. Benutzen von `sysctl`

Der Befehl `/sbin/sysctl` wird zum Betrachten, Setzen und Automatisieren von Kerneleinstellungen im Verzeichnis `/proc/sys` verwendet.

Um einen schnellen Überblick über alle konfigurierbaren Einstellungen im Verzeichnis `/proc/sys` zu bekommen, geben Sie den Befehl `/sbin/sysctl -a` als root ein. Dies gibt eine lange, umfassende Liste aus; ein kleiner Teil dieser Liste könnte z.B. so aussehen:

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

Das ist im Prinzip diesselbe Information, die Sie auch sähen, wenn Sie jede Datei einzeln betrachteten. Der einzige Unterschied ist der Ort der Datei. Die Datei `/proc/sys/net/ipv4/route/min_delay` wird durch `net.ipv4.route.min_delay` angesprochen, die Schrägstriche im Verzeichnis werden durch Punkte ersetzt, und der Teil `proc.sys` als allgemeiner Teil weggelassen.

Der Befehl `sysctl` kann anstelle von `echo` für das Zuweisen von Werten zu schreibbaren Dateien im Verzeichnis `/proc/sys/` verwendet werden. Statt diesen Befehl zu verwenden:

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

können Sie den Befehl `sysctl` verwenden:

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

Auch wenn das schnelle Setzen von Werten, wie bei diesem in `/proc/sys` nützlich zum Testen ist, funktioniert das nicht gut auf einem Produktionssystem, weil alle Einstellungen aus `/proc/sys` bei einem Neustart verloren gehen. Um permanente Einstellungen zu sichern, fügen Sie diese zu der Datei `/etc/sysctl.conf` hinzu.

Jedes Mal, wenn das System gestartet wird, wird das Skript `/etc/rc.d/rc.sysinit` von `init` aufgerufen. Dieses Skript enthält einen Befehl um `sysctl` auszuführen und verwendet `/etc/sysctl.conf` zur Vorgabe der Werte, die an den Kernel gegegeben wurden. Alle Werte, die zu `/etc/sysctl.conf` hinzugeführt wurden, werden nach jedem Neustart aktiviert.

5.5. Zusätzliche Ressourcen

Nachstehend finden Sie zusätzliche Quellenangaben für Informationen über das Dateisystem `/proc`.

5.5.1. Installierte Dokumentation

Das meiste an guter Dokumentation zu `/proc` ist wahrscheinlich schon auf Ihrem System installiert.

- `/usr/src/linux-2.4/Documentation/filesystems/proc.txt` — Enthält bestimmte, jedoch eingeschränkte Dokumentation zu den Aspekten von `/proc`.

- /usr/src/linux-2.4/Documentation/sysrq.txt — Ein Überblick über die System Request Key Optionen.
- /usr/src/linux-2.4/Documentation/sysctl/ — Ein Verzeichnis, dass eine Vielzahl von Tips zu sysctl enthält, inklusive Optionen, die den Kernel angehen (kernel.txt), zu den Dateisystemen (fs.txt) und zum virtuellen Speicher (vm.txt).
- /usr/src/linux-2.4/Documentation/networking/ip-sysctl.txt — Ein Blick auf verschiedene IP-Netzwerk Optionen.
- /usr/src/linux-2.4/ — Die vielleicht wichtigste Informationsquelle zu /proc ist der Linux Kernel Sourcecode. Wenn Sie das RPM Paket kernel-source installiert haben, finden Sie diesen im Verzeichnis /usr/src/linux-2.4/.

5.5.2. Hilfreiche Websites

- http://www.linuxhq.com — Diese Seite wartet eine komplette Datenbank mit Quellcode, Patches und Dokumentation für verschiedene Versionen des Linux Kernels.

Kapitel 6.

Benutzer und Gruppen

Die *Benutzer-* und *Gruppen*-Kontrolle ist eine grundlegendes Element der Red Hat Linux-Systemadministration.

Benutzer können sowohl Personen sein, d.h. Accounts, die an einen bestimmten Benutzer gebunden sind, als auch Accounts, die für bestimmte Anwendungen gedacht sind.

Gruppen sind der logische Ausdruck einer Zusammenfassung von Benutzern zu einem bestimmten Zweck. Alle Benutzer in der selben Gruppe, können Dateien dieser Gruppe Lesen, Schreiben und Ausführen.

Jeder Benutzer und jede Gruppe hat eine eindeutige numerische Identifikationsnummer, *Benutzer-ID* (*UID*) und *Gruppen-ID* (*GID*) genannt.

Jeder Datei wird bei ihrer Erstellung ein Benutzer oder eine Gruppe zugewiesen. Darüber hinaus werden dem Dateibesitzer, der Gruppe und allen anderen getrennte Berechtigungen zum Lesen, Schreiben und Ausführen zugewiesen. Die Benutzer und Gruppen einer bestimmten Datei sowie die Zugriffsberechtigungen für diese Datei können durch den root geändert werden oder in den meisten Fällen vom Ersteller der Datei.

Eine gute Verwaltung von Benutzern und Gruppen sowie eine effektive Verwaltung der Dateiberechtigungen gehören zu den wichtigsten Aufgaben eines System-Administrators. Für einen detaillierten Überblick der Strategien zum Management von Benutzern und Gruppen, sehen Sie das Kapitel *Managing Accounts and Group* im *Red Hat Linux System Administration Primer*.

6.1. Tools zum Management von Benutzern und Gruppen

Die Verwaltung von Benutzern und Gruppen kann sehr langwierig sein, Red Hat Linux liefert allerdings ein paar Tools und Konventionen, die dem Systemadministratoren diese Aufgabe erleichtern sollen.

Der einfachste Weg, Benutzer und Gruppen zu verwalten, ist mit Hilfe der grafischen Applikation **User-Manager** (`redhat-config-users`). Für mehr Informationen zu **User-Manager**, sehen Sie das Kapitel *Benutzer- und Gruppenkonfiguration* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

Auch können die folgenden Befehlszeilentools zum Verwalten von Benutzern und Gruppen verwendet werden:

- `useradd`, `usermod`, und `userdel` — Methoden des Industriestandards zum Hinzufügen, Löschen und Ändern von Benutzeraccounts.
- `groupadd`, `groupmod`, und `groupdel` — Methoden des Industriestandards zum Hinzufügen, Löschen und Ändern von Gruppen.
- `gpasswd` — Methode des Industriestandards zum Verwalten der Datei `/etc/group`.
- `pwck`, `grpck` — Tools zum Überprüfen von Passwort, Gruppe, und zugehörigen Shadow-Dateien.
- `pwconv`, `pwunconv` — Tools zur Konvertierung zu Shadow-Passwörtern und zurück zu Standard-Passwörtern.

Für einen Überblick zum Management von Benutzern und Gruppen, sehen Sie den *Red Hat Linux System Administration Primer*. Für eine detaillierte Beschreibung dieser Befehlszeilentools, sehen Sie das Kapitel *Benutzer- und Gruppenkonfiguration* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

6.2. Standardbenutzer

Tabelle 6-1 zeigt die Standardbenutzer, die während des Installationsvorgangs in der Datei `/etc/passwd` eingerichtet werden. Die Gruppen-ID (GID) in der Tabelle gibt die *Hauptgruppe* des Benutzers an. Eine Auflistung der Standardgruppen finden Sie in Abschnitt 6.3.

Benutzer	UID	GID	Benutzer-Verzeichnis	Shell
root	0	0	`/root`	`/bin/bash`
bin	1	1	`/bin`	`/sbin/nologin`
daemon	2	2	`/sbin`	`/sbin/nologin`
adm	3	4	`/var/adm`	`/sbin/nologin`
lp	4	7	`/var/spool/lpd`	`/sbin/nologin`
sync	5	0	`/sbin`	`/bin/sync`
shutdown	6	0	`/sbin`	`/sbin/shutdown`
halt	7	0	`/sbin`	`/sbin/halt`
mail	8	12	`/var/spool/mail`	`/sbin/nologin`
news	9	13	`/var/spool/news`	
uucp	10	14	`/var/spool/uucp`	`/sbin/nologin`
operator	11	0	`/root`	`/sbin/nologin`
games	12	100	`/usr/games`	`/sbin/nologin`
gopher	13	30	`/usr/lib/gopher-data`	`/sbin/nologin`
ftp	14	50	`/var/ftp`	`/sbin/nologin`
nobody	99	99	`/`	`/sbin/nologin`
rpm	37	37	`/var/lib/rpm`	`/bin/bash`
vcsa	69	69	`/dev`	`/sbin/nologin`
ntp	38	38	`/etc/ntp`	`/sbin/nologin`
canna	39	39	`/var/lib/canna`	`/sbin/nologin`
nscd	28	28	`/`	`/bin/false`
rpc	32	32	`/`	`/sbin/nologin`
postfix	89	89	`/var/spool/postfix`	`/bin/true`
named	25	25	`/var/named`	`/bin/false`
amanda	33	6	`var/lib/amanda/`	`/bin/bash`
postgres	26	26	`/var/lib/pgsql`	`/bin/bash`
sshd	74	74	`/var/empty/sshd`	`/sbin/nologin`
rpcuser	29	29	`/var/lib/nfs`	`/sbin/nologin`
nsfnobody	65534	65534	`/var/lib/nfs`	`/sbin/nologin`

Benutzer	UID	GID	Benutzer-Verzeichnis	Shell
pvm	24	24	/usr/share/pvm3	/bin/bash
apache	48	48	/var/www	/bin/false
xfs	43	43	/etc/X11/fs	/sbin/nologin
desktop	80	80	/var/lib/menu/kde	/sbin/nologin
gdm	42	42	/var/gdm	/sbin/nologin
mysql	27	27	/var/lib/mysql	/bin/bash
webalizer	67	67	/var/www/html/usage	/sbin/nologin
mailman	41	41	/var/mailman	/bin/false
mailnull	47	47	/var/spool/mqueue	/sbin/nologin
smmsp	51	51	/var/spool/mqueue	/sbin/nologin
squid	23	23	/var/spool/squid	/dev/null
ldap	55	55	/var/lib/ldap	/bin/false
netdump	34	34	/var/crash	/bin/bash
pcap	77	77	/var/arpwatch	/sbin/nologin
ident	98	98	/	/sbin/nologin
privoxy	100	101	/etc/privoxy	
radvd	75	75	/	/bin/false
fax	78	78	/var/spool/fax	/sbin/nologin
wnn	49	49	/var/lib/wnn	/bin/bash

Tabelle 6-1. Standardbenutzer

6.3. Standardgruppen

In Tabelle 6-2 sind die vom Installationsprogramm eingestellten Standardgruppen aufgeführt. Im Red Hat Linux werden Gruppen in der Datei `/etc/group` gespeichert.

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

Gruppe	GID	Mitglieder
kmem	9	
wheel	10	root
mail	12	mail
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	
lock	54	
nobody	99	
users	100	
rpm	37	rpm
utmp	22	
floppy	19	
vcsa	69	
ntp	38	
canna	39	
nscd	28	
rpc	32	
postdrop	90	
postfix	89	
named	25	
postgres	26	
sshd	74	
rpcuser	29	
nfsnobody	65534	
pvm	24	
apache	48	
xfs	43	
desktop	80	
gdm	42	
mysql	27	
webalizer	67	

Gruppe	GID	Mitglieder
mailman	41	
mailnull	47	
smmsp	51	
squid	23	
ldap	55	
netdump	34	
pcap	77	
ident	98	
privoxy	101	
radvd	75	
fax	78	
slocate	21	
wnn	49	

Tabelle 6-2. Standardgruppen

6.4. Benutzereigene Gruppen

Red Hat Linux verwendet ein Schema für *benutzereigene Gruppen* (*UPG*), welche die Benutzung von UNIX-Gruppen wesentlich vereinfacht.

Eine UPG wird erzeugt, wenn ein neuer Benutzer zum System hinzugefügt wird. UPGs haben den selben Namen wie der Benutzer, für welchen diese erzeugt wurden und lediglich dieser Benutzer ist Mitglied der Gruppe.

Die Verwendung von UPGs macht es problemlos möglich, dass die Default-Rechte von Dateien, erzeugt von einem Benutzer, schreibbar von beiden, Benutzer und Gruppe sind, da der Benutzer das einzige Mitglied der Gruppe ist.

Die Einstellung, die festlegt, welche Rechte einer neu erzeugten Datei oder einem Verzeichnis zugewiesen werden, wird *umask* gennannt und ist in der Datei `/etc/bashrc` enthalten. Auf UNIX-Systemen ist die umask, traditionell, 022, was andere Benutzer *und andere Mitglieder der Gruppe des Benutzers* davon abhält, diese Dateien zu ändern. Da jeder Benutzer ihre/seine eigene private Gruppe im UPG Schema hat, ist dieser "Gruppenschutz" nicht notwendig.

6.4.1. Gruppenverzeichnisse

Viele IT-Organisationen ziehen es vor, eine Gruppe für jedes größere Projekt zu erstellen, und dann Mitarbeiter zu dieser Gruppe zuzuweisen, wenn diese die Dateien des Projekts bearbeiten müssen. Unter dieser traditionellen Methode ist das Management von solchen Dateien schwierig, da, wenn jemand eine Datei erzeugt, diese mit der Hauptgruppe des Benutzers assoziiert ist. Wenn ein einzelner Benutzer an mehreren Projekten gleichzeitig arbeitet, ist es schwierig die entsprechenden Dateien der richtigen Gruppe zuzuweisen. Unter Verwendung des UPG Schemas, werden Gruppen automatisch Dateien zugewiesen, die in Verzeichnissen erstellt werden, welche das setgid Bit gesetzt haben. Dies Vereinfacht das Management von Gruppenprojekten, welche sich ein Verzeichnis teilen, erheblich.

Lass uns, zum Beispiel, sagen, dass eine Gruppe von Mitarbeitern an Dateien im Verzeichnis `/usr/lib/emacs/site-lisp/` arbeitet. Einigen dieser Mitarbeiter ist es zugetraut das Verzeichnis

zu ändern, aber sicherlich nicht allen. Erstellen Sie zuerst eine Gruppe `emacs`, wie im folgenden Beispiel gezeigt:

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

Um den Verzeichnisinhalt mit der `emacs` Gruppe zu verknüpfen, geben Sie Folgendes ein:

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

Nun können Sie mit Hilfe von `gpasswd` die richtigen Benutzer zur Gruppe hinzufügen:

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

Gestatten Sie den Benutzern mit folgendem Befehl, Dateien im Verzeichnis erstellen zu können:

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

Wenn ein Benutzer eine neue Datei erstellt, wird diese der benutzereigenen Standardgruppe zugeordnet. Um dies zu verhindern, müssen Sie folgenden Befehl ausführen, der dafür sorgt, dass alle Dateien im Verzeichnis mit der Gruppe des Verzeichnis selbst (`emacs`) erstellt werden:

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

Zu diesem Zeitpunkt, da die Default-umask aller Benutzer 002 ist, können die Mitglieder der `emacs`-Gruppe Dateien im Verzeichnis `/usr/lib/emacs/site-lisp/` ändern, ohne dass der Administrator Rechte ändern müsste, jedesmal wenn eine neue Datei erzeugt wird.

6.5. Shadow-Utilities

In Mehrbenutzer-Umgebungen ist es sehr wichtig Shadow-Utilities zu verwenden (auch als *Shadow Passwörter* bekannt), da diese erweiterten Schutz für die Authentifizierungsdateien des Systems bereitstellen. Während der Installation von Red Hat Linux, werden Shadow-Passwörter als Default eingeschaltet.

Shadow-Passwörter bieten über die herkömmliche, auf UNIX-basierten Systemen verwendete Weise, folgende Vorteile:

- Shadow-Passwörter erhöhen die Systemsicherheit dadurch, dass die verschlüsselten Passwörter (normalerweise in der Datei `/etc/passwd` abgelegt) im Verzeichnis `/etc/shadow` abgelegt werden, das nur von root gelesen werden kann.
- Liefern Informationen über das Altern von Passwörtern.
- Die Möglichkeit unter Verwendung der Datei `/etc/login.defs` die Sicherheitsbestimmungen besonders im Bezug auf veraltete Passwörter umzusetzen.

Shadow-Utilities arbeiten ordnungsgemäß, unabhängig davon, ob Shadow-Passwörter aktiviert sind oder nicht und diese unterstützen das privaten Gruppen-Schema des Benutzers.

redhat

Kapitel 7.

Das X Window System

Während der Kernel das Herz von Red Hat Linux darstellt, ist die vom *X Window System*, kurz *X* genannt, bereitgestellte grafische Umgebung für viele Benutzer das Gesicht des Betriebssystems.

In der UNIX™-Welt gibt es seit Jahrzehnten Umgebungen mit Fenstergestaltung, womit sie vielen der momentan gebräuchlichsten Betriebssystemen voraus war. Das X Window System ist nun die gebräuchlichste GUI für Unix-ähnliche Betriebssysteme.

Die graphische Umgebung von Red Hat Linux wird von XFree86™ bereitgestellt, einem Open Source Softwareprojekt, an dem Hunderte von Entwicklern in der ganzen Welt arbeiten. XFree86 zeichnet sich durch eine schnelle Entwicklung, einen umfangreichen Support für verschiedene Hardware-Geräte und Architekturen sowie die Fähigkeit aus, unter verschiedenen Betriebssystemen und Plattformen zu laufen.

Das X Window System verwendet eine Client-Server-Architektur. Dabei wird ein *X-Server*-Prozess gestartet, mit dem sich *X-Client*-Prozesse über ein Netzwerk oder eine lokale Verbindung verknüpfen können. Der Serverprozess verwaltet die Kommunikation mit der Hardware wie zum Beispiel mit der Grafikkarte, dem Monitor, der Tastatur und der Maus. Der X-Client existiert im Benutzerbereich, und erstellt eine graphische Benutzerschnittstelle (*graphical user interface*, *GUI*) für den Benutzer, und gibt Anfragen an den X-Server weiter.

7.1. Der XFree86-Server

Red Hat Linux 9 verwendet XFree86 Version 4.x als Basis-X Window System, welches viele Cutting-Edge XFree86 Technologien beinhaltet. Dazu gehören 3D Hardwarebeschleunigung, XRender-Erweiterung für anti-aliased Fonts, ein modulares Treiber-basiertes Design und Unterstützung für moderne Video-Hardware und Eingabegeräte.

Wichtig

Red Hat Linux stellt keine Serverpakete von XFree86 Version 3 mehr zur Verfügung. Ehe Sie auf die letzte Version von Red Hat Linux aktualisieren, stellen Sie sicher, dass Ihre Grafikkarte mit der Version 4 von XFree86 kompatibel ist. Überprüfen Sie dies auf der Red Hat-HCL (Hardwarekompatibilitätsliste) unter dem URL http://hardware.redhat.com.

Das X Window System befindet sich hauptsächlich an zwei Speicherorten im Dateisystem:

/usr/X11R6/

Ein Verzeichnis mit X-Client-Binärdateien, bestimmten Headerdateien, Bibliotheken, man-Seiten und weiterer X-Dokumentation.

`/etc/X11/`

Enthält alle Konfigurationsdateien für die verschiedenen Komponenten des X Window Systems. Hierzu gehören Konfigurationsdateien für den X-Server, den älteren X-Font-Server (`xfs`), X-Display Manager und zahlreiche weitere grundlegende Komponenten.

Es ist wichtig zu beachten, dass die Konfigurationsdatei für die neuere Fontconfig-basierte Font-Architektur `/etc/fonts/fonts.conf` ist (was die Datei `/etc/X11/XftConfig` überflüssig macht). Für weitere Informationen zur Konfiguration und zum Hinzufügen von Fonts, sehen Sie Abschnitt 7.4.

Da der XFree86-Server eine Reihe von fortgeschrittenen Tasks auf einer Vielzahl an Hardware durchführt, benötigt dieser eine detaillierte Konfiguration. Das Red Hat Linux Installationsprogramm installiert und automatisch konfiguriert XFree86, solange die XFree86 Pakete zur Installation ausgewählt sind. Wenn sich allerdings der Monitor oder die Grafikkarte ändert, muss XFree86 neu konfiguriert werden. Am besten verwenden Sie hierzu **X Konfigurationstool** (`redhat-config-xfree86`).

Wenn Sie **X Konfigurationstool** in einer aktiven X-Sitzung starten möchten, wechseln Sie zur **Schaltfläche des Hauptmenüs** (im Panel) => **Systemtools** => **Anzeigen**. Wenn Sie **X Konfigurationstool** während einer X-Sitzung verwendet haben, müssen Sie sich von der aktuellen X-Sitzung abmelden und erneut anmelden, damit die Änderungen wirksam werden. Für weitere Informationen zur Verwendung von **X Konfigurationstool** sehen Sie das Kapitel *Audio, Video und Multimedia* im *Red Hat Linux Handbuch Erster Schritte*.

In einigen Fällen kann es notwendig sein die Konfigurationsdatei des XFree86 Server, `/etc/X11/XF86Config`, manuell zu bearbeiten. Für weitere Informationen zur Struktur dieser Datei sehen Sie Abschnitt 7.3.

7.2. Desktop-Umgebungen und Window Manager

Wenn der XFree86-Server erst einmal läuft, können X-Client-Applikationen zu diesem verbinden und eine GUI für den Benutzer erzeugen. Eine Anzahl von GUIs sind in Red Hat Linux möglich, vom rudimentären *Tab Window Manager* zum hochentwickelten, interaktiven *GNOME* Desktop, mit welcher die meisten Red Hat Linux Benutzer vertraut sind.

Um die letztere, weiter entwickelte GUI zu erzeugen, müssen zwei X-Client-Applikationen zum XFree86-Server verbinden: Eine *Desktop-Umgebung* und ein *Window Manager*.

7.2.1. Desktop-Umgebungen

Eine Desktop-Umgebung umfasst eine Anzahl verschiedenster X-Clients. Diese zusammengenommen stellen die graphische Benutzeroberfläche und Entwicklungsplattform dar.

Desktop-Umgebungen enthalten erweiterte Merkmale, die es X-Clients und anderen laufenden Prozessen ermöglichen, miteinander zu kommunizieren. Auf diese Weise können alle Applikationen, die für diese Umgebung geschrieben wurden, integriert und auf weitere Arten verwendet werden, wie beispielsweise die Drag-and-Drop Funktionen.

Red Hat Linux liefert zwei Desktop-Umgebungen:

- *GNOME* — Die standardmäßige Desktop-Umgebung für Red Hat Linux, welche auf dem GTK+ 2 graphischen Toolkit basiert.
- *KDE* — Eine weitere Desktop-Umgebung, welche auf dem Qt 3 graphischen Toolkit basiert.

Sowohl GNOME als auch KDE besitzen erweiterte Applikationen wie textverarbeitende Prozessoren, elektronische Kalkulationstabellen und Bedienerkonsolen-Geräte, mit denen Sie das Look and Feel vollständig steuern können. Beide Umgebungen können standardmäßige X-Clientanwendungen ausführen. Die meisten KDE-Anwendungen können auch in GNOME ausgeführt werden, wenn die Qt-Bibliotheken installiert sind.

Im *Red Hat Linux Handbuch Erster Schritte* finden Sie weitere Informationen über die benutzerdefinierte Konfiguration der Desktop-Umgebungen GNOME und KDE.

7.2.2. Window Manager

Window Manager sind X-Clientprogramme, die die Art und Weise steuern, in der andere X-Clients positioniert, in ihrer Größe verändert oder bewegt werden. Window Manager liefern darüber hinaus

auch Titelleisten, Tastaturspezifizierung nach Tastatur oder Maus sowie benutzerspezifische Tasten- und Maustastenbindungen.

Fünf Window Manager sind in Red Hat Linux enthalten:

- `kwin` — Der *KWin* Window Manager ist der Default bei der Auswahl der KDE Desktop-Umgebung. Dies ist ein effizienter Window Manager, der benutzerdefinierte Themen unterstützt.
- `metacity` — Der *Metacity* Window Manager ist der Default bei der Auswahl der GNOME Desktop-Umgebung. Es ist ein einfacher und effizienter Window Manager, der benutzerdefinierte Themen unterstützt.
- `mwm` — Der *Motif* Window Manager ist ein Standalone Window Manager, mit grundlegenden Funktionen. Da dieser als Standalone entwickelt wurde, sollte er weder mit der GNOME noch mit der KDE Desktop-Umgebung ausgeführt werden.
- `sawfish` — Der *Sawfish* Window Manager ist ein kompletter Window Manager mit zahlreichen Funktionen. Dieser war der Default für die GNOME Desktop-Umgebung bis zu Red Hat Linux 8.0. Er kann als Standalone, oder zusammen mit einer Desktop-Umgebung ausgeführt werden.
- `twm` — Ein minimalistischer *Tab Window Manager*, der im Vergleich am wenigsten Funktionalität bietet. Er kann als Standalone, oder zusammen mit einer Desktop-Umgebung ausgeführt werden und wird als Teil von XFree86 installiert.

Diese Window Manager können als einzelne X-Clients ausgeführt werden, womit auch die Unterschiede deutlicher werden. Geben Sie den Befehl `xinit <Pfad-zum-Window-Manager>` ein, wobei `<Pfad-zum-Window-Manager>` der Speicherort der Binärdatei des Window Managers ist. Die Binärdatei kann ermittelt werden, indem Sie `which <Window-Manager-Name>` eingeben.

7.3. XFree86-Server-Konfigurationsdateien

Der XFree86 Server ist eine einzelne ausführbare Binärdatei (`/usr/X11R6/bin/XFree86`), welche alle benötigten X Server Module zur Laufzeit vom Verzeichnis `/usr/X11R6/lib/modules/` lädt. Einige dieser Module werden automatisch geladen, während andere in der Konfigurationsdatei von XFree86 Server angegeben werden müssen.

Die XFree86 Server und damit zusammenhängende Konfigurationsdateien sind im Verzeichnis `/etc/X11/` abgelegt. Die Konfigurationsdatei für XFree86 Server ist `/etc/X11/XF86Config`. Wenn Red Hat Linux installiert ist, werden die Konfigurationsdateien für XFree86 mithilfe der während der Installation gesammelten Informationen erstellt.

7.3.1. `XF86Config`

Auch wenn Sie `/etc/X11/XF86Config` kaum manuell bearbeiten müssen, ist es sinnvoll, deren einzelnen Bereiche und optionalen Parameter zu kennen. Dies ist vor allem während der Fehlersuche vorteilhaft.

7.3.1.1. Die Struktur

Die Datei `/etc/X11/XF86Config` besteht aus zahlreichen Abschnitten, welche einen jeweils spezifischen Teil der System-Hardware ansprechen.

Jeder Abschnitt beginnt mit einer `Section "<Sektionsname>"`- Zeile und endet mit einer `EndSection`-Zeile. Innerhalb jedes einzelnen Abschnitts befinden sich verschiedene Zeilen mit einem Optionsnamen und mindestens einem Optionswert, der auch in Anführungszeichen angegeben sein kann.

Mit einem Hash-Symbol [#] beginnende Zeilen werden vom XFree86 Server nicht gelesen und stellen Kommentare für den Benutzer dar.

Einige der Optionen in `/etc/X11/XF86Config` akzeptieren boolesche Werte, was die gegebene Funktion entweder ein oder aus schaltet. Verwendbare boolesche Werte sind:

- `1`, `on`, `true`, oder `yes` — Schaltet die Option ein.
- `0`, `off`, `false`, oder `no` — Schaltet die Option aus.

Folgend sind einige der wichtigeren Abschnitte aufgelistet, wie diese in einer typischen `/etc/X11/XF86Config` Datei vorkommen. Genauere Informationen zur Konfigurationsdatei des XFree86 Server können in den man-Seiten zu `XF86Config` gefunden werden.

7.3.1.2. `ServerFlags`

Der optionale Abschnitt `ServerFlags` enthält verschiedene allgemeine XFree86 Server-Einstellungen. Diese Einstellungen können mit Optionen des Abschnitts `ServerLayout` überschrieben werden (sehen Sie Abschnitt 7.3.1.3 für genaueres).

Jeder Eintrag im Abschnitt `ServerFlags` ist jeweils in einer eigenen Zeile, welche mit dem Term `Option` beginnt und von einer in doppelte Anführungszeichen ["] eingeschlossenen Option gefolgt wird.

Folgend ist ein Beispiel eines `ServerFlags`-Abschnitts:

```
Section "ServerFlags"
      Option "DontZap" "true"
EndSection
```

Folgend ist eine Liste der nützlichsten Optionen:

- `"DontZap" "<`*`boolean`*`>"` — Wenn der Wert von <*boolean*> auf true gesetzt ist, verhindert dies, dass die Tastenkombination [Strg]-[Alt]-[Rücktaste] verwendet wird, die den XFree86-Server sofort beendet.
- `"DontZoom" "<`*`boolean`*`>"` — Wenn der Wert von <*boolean*> true ist, verhindert, dass die Tastenkombinationen [Strg]-[Alt]-[Zehnertastatur-Plus] und [Strg]-[Alt]-[Zehnertastatur-Minus] verwendet werden, um sich durch konfigurierte Grafikauflösungen zu bewegen.

7.3.1.3. `ServerLayout`

Der Abschnitt `ServerLayout` bindet Eingabe- und Ausgabegeräte, die vom XFree86 Server kontrolliert werden. Dieser Abschnitt muss zumindest ein Ausgabegerät und zwei Eingabegeräte (Tastatur und Maus) angeben.

Das folgende Beispiel zeigt einen typischen `ServerLayout`-Abschnitt:

```
Section  "ServerLayout"
        Identifier     "Default Layout"
        Screen      0  "Screen0" 0 0
        InputDevice    "Mouse0" "CorePointer"
        InputDevice    "Keyboard0" "CoreKeyboard"
EndSection
```

Die folgenden Einträge sind die in einem `ServerLayout`-Abschnitt am häufigsten verwendeten:

- `Identifier` — Ein eindeutiger Name, der für die Beschreibung dieses `ServerLayout`-Abschnitts verwendet wird.
- `Screen` — Der Name eines `Screen`-Abschnitts, der mit dem XFree86 Server verwendet wird. Es können mehr als eine `Screen`-Option vorkommen.

  Folgend ist ein Beispiel eines typischen `Screen`-Eintrags:
  ```
  Screen      0  "Screen0" 0 0
  ```

  Die erste Zahl in diesem Beispiel eines `Screen`-Eintrags (`0`) gibt an, dass der erste *Anschluss* auf der Grafikkarte die im `Screen`-Abschnitt angegebene Konfiguration mit dem Identifier `"Screen0"` verwendet.

  Sollte die Grafikkarte mehr als einen Anschluss haben, sind weitere `Screen`-Einträge mit unterschiedlichen Nummern und Identifiern für `Screen`-Abschnitte von Nöten.

  Die Nummern auf der rechten Seite liefern die X- und Y-Koordinaten für die linke obere Ecke des Bildschirms (standardmäßig `0 0`).
- `InputDevice` — Gibt den Namen eines `InputDevice`-Abschnitts an, der mit dem XFree86 Server verwendet wird.

  Es muss zumindest zwei `InputDevice`-Einträge geben: Einer für die Standardmaus und einer für die Standardtastatur. Die Optionen `CorePointer` und `CoreKeyboard` weisen darauf hin, dass es sich um primäre Maus und Tastatur handelt.
- `Option "<`*`option-name`*`>"` — Ein optionaler Eintrag, der weitere Parameter für diesen Abschnitt angibt. Jede der hier aufgeführten Optionen überschreibt die Optionen im Abschnitt `ServerFlags`.

  Ersetzen Sie <*`option-name`*> hier mit einer der in den XF86Config man-Seiten aufgelisteten Optionen.

Es ist möglich mehr als einen `ServerLayout`-Abschnitt anzugeben. Der Server wird jedoch nur den ersten einlesen, außer, es wird eine anderer `ServerLayout`-Abschnitt als Befehlszeilenargument angegeben.

7.3.1.4. `Files`

Der `Files`-Abschnitt legt für XFree86 Server wichtige Pfade wie zum Beispiel den Fontpfad fest.

Das folgende Beispiel zeigt einen typischen `Files`-Abschnitt:

```
Section "Files"
        RgbPath      "/usr/X11R6/lib/X11/rgb"
        FontPath     "unix/:7100"
EndSection
```

Folgende Einträge sind die in einem `Files`-Abschnitt am häufigsten verwendeten:

- `RgbPath` — Gibt den Speicherort der RGB Farbdatenbank an. Diese Datenbank definiert alle in XFree86 gültigen Farbnamen und bindet diese deren entsprechenden RGB-Werten.
- `FontPath` — Gibt an, wo der XFree86 Server verbinden muss, um Fonts vom `xfs` Font-Server zu erhalten.

  Standardmäßig ist `FontPath unix/:7100`. Auf diese Weise wird der XFree86 Server angewiesen, Font-Informationen mithilfe von UNIX-Domänen-Sockets für die Kommunikation zwischen den Prozessen (IPC) abzurufen.

  In Abschnitt 7.4 finden Sie weitere Informationen über XFree86 und Fonts.
- `ModulePath` — Ermöglicht Ihnen (optional) die Einstellung von mehreren Verzeichnissen, die für die Speicherung von XFree86 Server Modulen verwendet werden.

7.3.1.5. `Module`

Der Abschnitt `Module` gibt dem XFree86 Server an, welche Module des `/usr/X11R6/lib/modules`-Verzeichnisses zu laden sind. Die Module statten den XFree86 Server mit zusätzlichen Funktionen aus.

Folgend ist ein Beispiel eines typischen `Module`-Abschnitts:

```
Section "Module"
 Load  "dbe"
 Load  "extmod"
 Load  "fbdevhw"
 Load  "glx"
 Load  "record"
 Load  "freetype"
 Load  "typel"
 Load  "dri"
EndSection
```

7.3.1.6. `InputDevice`

Jeder `InputDevice`-Abschnitt konfiguriert ein Input-Gerät wie eine Maus oder eine Tastatur, das für die Eingabe von Informationen in das System mithilfe des XFree86 Servers verwendet wird. Die meisten Systeme besitzen mindestens zwei `InputDevice`-Abschnitte, Tastatur und Maus.

Das folgende Beispiel zeigt einen typischen `InputDevice`-Abschnitt für eine Maus:

```
Section "InputDevice"
 Identifier  "Mouse0"
 Driver      "mouse"
 Option     "Protocol" "IMPS/2"
 Option     "Device" "/dev/input/mice"
 Option     "Emulate3Buttons" "no"
EndSection
```

Die folgenden Einträge werden am häufigsten in einem `InputDevice`-Abschnitt verwendet:

- `Identifier` — Gibt einen eindeutigen Namen für diesen `InputDevice`-Abschnitt an. Dieser Eintrag ist notwendig.
- `Driver` — Gibt XFree86 den Namen des Treibers an, der für die Verwendung des Geräts zu laden ist.
- `Option` — Gibt Geräte-bezogene Optionen an.

  Für eine Maus, enthalten diese Optionen Folgende:

  - `Protokoll` — Gibt das von der Maus verwendete Protokoll an, wie `IMPS/2`.
  - `Device` — Gibt den Ort des physischen Geräts an.
  - `Emulate3Buttons` — Gibt an, ob eine Zwei-Tasten-Maus eine dritte Taste, wenn beide Tasten gleichzeitig gedrückt werden, emulieren soll.

  Sehen Sie die XF86Config man-Seiten für eine Liste der gültigen Optionen.

Der Abschnitt `InputDevice` enthält einige Kommentare, die dem Benuzter das Konfigurieren weiterer Optionen ermöglicht.

7.3.1.7. `Monitor` Abschnitt

Jeder `Monitor`-Abschnitt konfiguriert einen Typ von Monitor, der vom System verwendet wird. Mindestens ein `Monitor`-Abschnitt muss vorhanden sein, zusätzliche können bestehen, einen für jeden vom Rechner verwendeten Typ von Monitor.

Der beste Weg, einen Monitor einzurichten, ist beim Konfigurieren von X während des Installationsprozesses oder durch Verwendung von **X Konfigurationstool**. Für weiteres zur Verwendung von **X Konfigurationstool**, sehen Sie da Kapitel *Audio, Video und Multimedia* im *Red Hat Linux Handbuch Erster Schritte*.

Das folgende Beispiel zeigt einen typischen `Monitor`-Abschnitt:

```
Section "Monitor"
 Identifier   "Monitor0"
 VendorName   "Monitor Vendor"
 ModelName    "DDC Probed Monitor - ViewSonic G773-2"
 DisplaySize  320 240
 HorizSync    30.0 - 70.0
 VertRefresh  50.0 - 180.0
EndSection
```

Warnung

Seien Sie vorsichtig, wenn Sie die Werte im `Monitor`-Abschnitts der Datei `/etc/X11/XF86Config` manuell bearbeiten. Falsche Werte in diesem Abschnitt können Ihren Monitor beschädigen. Schlagen Sie in der Dokumentation Ihres Monitors die verfügbaren sicheren Parameter nach.

Folgend sind häufig im `Monitor`-Abschnitt verwendete Einträge:

- `Identifier` — Verleiht dem Monitor einen eindeutigen Namen. Dieser Eintrag ist erforderlich.
- `VendorName` — Ein optionaler Eintrag, welcher den Hersteller des Monitors angibt.
- `ModelName` — Ein optionaler Eintrag, welcher den Namen des Models des Monitors angibt.
- `DisplaySize` — Ein optionaler Eintrag, welcher, in Millimetern, die physische Größe des Bildschirmbereichs angibt.
- `HorizSync` — Gibt XFree86 die Bandbreite der Horizontalfrequenz in kHz an, die mit dem Monitor kompatibel ist. Diese Werte werden vom XFree86 Server als Richtlinie verwendet, so dass dieser weiß, ob bestimmte Werte eines `Modeline`-Eintrags für den Monitor zu verwenden sind.
- `VertRefresh` — Listet die vom Monitor unterstützten vertikalen Bildwiederholfrequenzen in kHz auf. Diese Werte werden vom XFree86 Server als Richtlinie verwendet, so dass dieser weiß, ob bestimmte Werte eines `Modeline`-Eintrags für den Monitor zu verwenden sind.
- `Modeline` — Dient der optionalen Angabe der Grafikmodi des Monitors bei besonderen Auflösungen mit bestimmten Horizontal- und Vertikalfrequenzen. Sehen Sie die man-Seiten zu `XF86Config` für eine genauere Beschreibung der `Modeline`-Einträge.
- `Option "<option-name>"` — Ein optionaler Eintrag, der weitere Parameter für diesen Abschnitt angibt. Ersetzen Sie *<option-name>* mit einer gültigen, in den man-Seiten zu XF86Config aufgelisteten Option.

7.3.1.8. Device

Jeder Device-Abschnitt konfiguriert eine Grafikkarte für das System. Ein Device-Abschnitt muss vorhanden sein. Weitere können bestehen, einer für jede auf dem Rechner installierte Grafikkarte.

Der beste Weg eine Grafikkarte einzurichten, ist beim Konfigurieren von X während des Installationsprozesses oder durch Verwendung von **X Konfigurationstool**. Für weiteres zur Verwendung von **X Konfigurationstool**, sehen Sie da Kapitel *Audio, Video und Multimedia* im *Red Hat Linux Handbuch Erster Schritte*.

Das folgende Beispiel zeigt einen typischen Device-Abschnitt für eine Grafikkarte:

```
Section "Device"
 Identifier  "Videocard0"
 Driver      "mga"
 VendorName  "Videocard vendor"
 BoardName   "Matrox Millennium G200"
 VideoRam    8192
        Option      "dpms"
EndSection
```

Die folgenden Einträge sind häufig in einem Device-Abschnitt verwendet:

- Identifier — Ein eindeutiger Name für diesen Device-Abschnitt. Dies ist ein notwendiger Eintrag.
- Driver — Gibt an, welchen Treiber der XFree86 Server laden muss, um die Grafikkarte verwenden zu können. Eine Liste von Treibern kann in der Datei /usr/X11R6/lib/X11/Cards gefunden werden, welche mit dem Paket hwdata installiert wird.
- VendorName — Gibt (optional) den Hersteller der Grafikkarte an.
- BoardName — Gibt (optional) den Namen der Grafikkarte an.
- VideoRam — Der RAM-Speicher (optional) der Grafikkarte in Kilobytes. Diese Einstellung ist normalerweise nicht notwendig, da der XFree86-Server gewöhnlich die Grafikkarte automatisch auf den verfügbaren Speicher prüft. Es gibt jedoch Grafikkarten, die XFree86 nicht automatisch erkennen kann, weswegen Ihnen diese Option die Möglichkeit bietet, manuell den Grafik-RAM anzugeben.
- BusID — Gibt (optional) den Bus an, in dem sich die Grafikkarte befindet. Diese Option ist nur bei Systemen mit mehreren Karten notwendig.
- Screen — Ein optionaler Eintrag, der angibt, welchen Anschluss der Grafikkarte dieser Device-Abschnitt konfiguriert. Diese Option ist nur bei Grafikkarten mit mehr als einem Anschluss nützlich.

  Wenn mehrere Monitore an eine Grafikkarte angeschlossen sind, dann müssen auch verschiedene Device-Abschnitte mit einem jeweils unterschiedlichen Screen-Wert zur Verfügung stehen.

  Der Wert eines Screen-Eintrags ist eine ganzzahlige Nummer. Der erste Anschluss hat den Wert 0 und für jeden weiteren Anschluss wird diese Zahl um eins erhöht.
- Option "<*option-name*>" — Ein optionaler Eintrag, der weitere Parameter für diesen Abschnitt angibt. Ersetzen Sie <*option-name*> mit einer gültigen, in den man-Seiten zu XF86Config aufgelisteten Option.

  Eine der häufiger verwendeten Optionen ist "dpms", welches die Service Star Energy Compliance für den Monitor einschaltet.

7.3.1.9. `Screen`

Jeder `Screen`-Abschnitt bindet eine Grafikkarte (oder einen Anschluss auf einer Grafikkarte) an einen Monitor, indem dieser den `Device`-Abschnitt und den jeweiligen `Monitor`-Abschnitt für jeden der Anschlüsse referenziert. Ein `Screen`-Abschnitt muss vorhanden sein, weitere bestehen für jede zusätzliche Kombination von Grafikkarte (oder Anschluss) zu Monitor auf dem gegebenen Rechner.

Folgend ist ein Beispiel eines typischen `Screen`-Abschnitts:

```
Section "Screen"
 Identifier "Screen0"
 Device     "Videocard0"
 Monitor    "Monitor0"
 DefaultDepth     16
 SubSection "Display"
  Depth     24
  Modes    "1280x1024" "1280x960" "1152x864" "1024x768" "800x600" "640x480"
 EndSubSection
 SubSection "Display"
  Depth     16
  Modes    "1152x864" "1024x768" "800x600" "640x480"
 EndSubSection
EndSection
```

Folgende Einträge sind häufig in einem `Screen`-Abschnitt verwendet:

- `Identifier` — Ein eindeutiger Name für diesen `Screen`-Abschnitt. Dies ist ein notwendiger Eintrag.
- `Device` — Gibt einen eindeutigen Namen eines `Device`-Abschnitts an. Dieser Eintrag ist erforderlich.
- `Monitor` — Gibt einen eindeutigen Namen eines `Monitor`-Abschnitts an. Dieser Eintrag ist notwendig.
- `DefaultDepth` — Gibt die Farbtiefe in Bits an. Im vorangegangenen Beispiel ist `16`, was mehrere tausende von Farben ermöglicht, der Default-Wert. Mehrere `DefaultDepth`-Einträge sind zulässig, aber einer muss mindestens vorhanden sein.
- `SubSection "Display"` — Gibt die Bildschirmmodi an, die bei einer spezifischen Farbtiefe zur Verfügung stehen. Ein `Screen`-Abschnitt kann mehrere `Display`-Unterabschnitte haben, es muss allerdings zumindest einer für die in `DefaultDepth` angegebene Farbtiefe bestehen.
- `Option "<option-name>"` — Ein optionaler Eintrag, der weitere Parameter für diesen Abschnitt angibt. Ersetzen Sie *<option-name>* mit einer gültigen, in den man-Seiten zu XF86Config aufgelisteten Option.

7.3.1.10. `DRI`

Beim optionalen `DRI`-Abschnitt *Direct Rendering Infrastructure* (*DRI*) handelt es sich um eine Schnittstelle, die es 3D-Software-Applikationen ermöglicht, die 3D-Hardwarebeschleunigung moderner und unterstützter Grafikhardware zu nutzen. Darüber hinaus verbessert DRI die Leistung der 2D-Hardwarebeschleunigung, wenn Treiber verwendet werden, die für den Gebrauch von DRI mit 2D-Vorgängen erweitert wurden.

Dieser Abschnitt wird ignoriert, es sei denn, DRI wird im `Module`-Abschnitt aktiviert.

Das folgende Beispiel zeigt einen typischen `DRI`-Abschnitt:

```
Section "DRI"
        Group        0
        Mode         0666
```

```
EndSection
```

Unterschiedliche Grafikkarten verwenden DRI auf unterschiedliche Weise. Bevor Sie DRI-Werte ändern, lesen Sie bitte zuerst die Datei `/usr/X11R6/lib/X11/doc/README.DRI`.

7.4. Fonts

Red Hat Linux verwendet zwei Methoden, um Fonts und die Anzeige unter XFree86 zu regeln. Das neuere Fontconfig Font-Subsystem vereinfacht das Font-Management und liefert erweitere Anzeigefunktionen, wie Anti-Aliasing. Dieses System wird automatisch für Applikationen verwendet, welche unter Verwendung entweder des Qt 3 oder des GTK+ 2 graphischen Toolkits entwickelt wurden.

Aus Gründen der Kompatibilität, enthält Red Hat Linux auch das originale, Core X, Font-Subsystem. Dieses System, welches mehr als 15 Jahre alt ist, ist um den *X Font Server* (*xfs*) basiert.

Dieser Abschnitt beschreibt das Konfigurieren von Fonts unter Verwendung beider Systeme.

7.4.1. Fontconfig

Das Fontconfig Font-Subsystem erlaubt Applikationen den Zugriff auf Fonts des Systems und die Verwendung von Xft oder eines anderen Render-Mechanismus, um Fontconfig Fonts mit einem fortgeschrittenen Anti-Aliasing zu versehen. Graphische Applikationen können die Xft-Library mit Fontconfig dazu benutzen, Text auf dem Bildschirm darzustellen.

Mit der Zeit wird das Fontconfig/Xft Font-Subsystem das Core X Font-Subsystem vollständig ablösen.

Wichtig

Das Fontconfig Font-Subsystem arbeitet noch nicht mit **OpenOffice.org** und **Abiword**, welche eigene Font-Render-Technologien verwenden.

Es ist wichtig zu beachten, dass Fontconfig die Konfigurationsdatei `/etc/fonts/fonts.conf` teilt, was das alte `/etc/X11/XftConfig` ersetzt. Die Fontconfig Konfigurationsdatei sollte nicht manuell bearbeitet werden.

Tipp

Während dem Übergang zum neuen Font-System, werden GTK+ 1.2 Applikationen von Änderungen, welche über den **Font Preferences** Dialog (**Main Menu Button** [auf dem Panel] => **Preferences** => **Font**) getätigt werden, nicht betroffen. Für diese Applikationen kann eine Font durch Hinzufügen der folgenden Zeile zur Datei `~/.gtkrc.mine` konfiguriert werden:

```
style "user-font" {

fontset = "<font-specification>"

}

widget_class "*" style "user-font"
```

Ersetzen Sie *<font-specification>* mit einer Fontangabe im traditionellen, von X Applikationen verwendeten, Format, wie `-adobe-helvetica-medium-r-normal--*-120-*-*-*-*-*-*`. Eine vollständige Liste der Core-Fonts kann durch Ausführen von `xlsfonts` erhalten oder durch Verwendung von `xfontsel` interaktiv erzeugt werden.

7.4.1.1. Hinzufügen von Fonts zu Fontconfig

Das Hinzufügen von neuen Fonts zum Fontconfig-Subsystem ist ein einfacher und direkter Vorgang.

1. Um Fonts systemweit hinzuzufügen, kopieren Sie die neuen Fonts in das Verzeichnis `/usr/share/fonts/local/`.

   Um Fonts für einen gewissen Benutzer hinzuzufügen, kopieren Sie die Fonts in das Unterverzeichnis `.fonts/` im Hauptverzeichnis des Benutzers.

2. Benutzen Sie den Befehl `fc-cache` um die Font-Information im Cache zu aktualisieren, wie Folgend beschrieben:

   `4fc-cache <path-to-font-directory>`

   Ersetzen Sie *<path-to-font-directory>* mit dem Verzeichnis, das die neuen Fonts enthält (entweder `/usr/share/fonts/local/` oder `~/.fonts/`).

Tipp

Individuelle Benutzer können Fonts auch graphisch installieren, indem Sie den Nautilus-Browser zu `fonts:///` navigieren, und neue Font-Dateien über Drag-and-Drop dort hinein kopieren.

Wichtig

Wenn der Font-Dateiname in `.gz` ended, ist dies eine komprimierte Datei und diese kann nicht direkt verwendet werden. Die darin enthaltenen Dateien müssen zuerst extrahiert werden. Verwenden Sie dazu den Befehl `gunzip` oder doppel-klicken Sie die Datei und kopieren Sie die Font mittels Drag-and-Drop in ein Verzeichnis in **Nautilus**.

7.4.2. Core X Font-System

Aus Gründen der Kompatibilität, stellt Red Hat Linux das Core X Font-Subsystem, welches den X Font Server (`xfs`) verwendet, auch weiterhin zur Verfügung, um den X Client Applikationen Fonts bereitzustellen.

Der XFree86 Server sucht nach den im `FontPath`-Eintrag des `Files`-Abschnitt der Konfigurationsdatei `/etc/X11/XF86Config` angegebenen Fonts. Sehen Sie Abschnitt 7.3.1.4 für weitere Information zum `FontPath`-Eintrag.

Der XFree86 Server verbindet zum `xfs` Server auf einem angegebenen Port um Font-Informationen zu erfragen. Aus diesem Grund muss der `xfs` Service laufen, damit X starten kann. Für weitere Informationen zum Konfigurieren von Services für einen bestimmten Runlevel, sehen Sie das Kapitel *Zugriffskontrolle von Services* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

7.4.2.1. `xfs`-Konfiguration

Das `/etc/rc.d/init.d/xfs`-Skript startet den `xfs`-Server. In der Datei `/etc/X11/fs/config` können verschiedene Optionen konfiguriert werden.

Die Folgende ist eine Liste der häufiger verwendeten Optionen:

- `alternate-servers` — Stellt eine Liste alternativer Font-Server ein, die verwendet werden können, wenn dieser Server nicht verfügbar ist. Die einzelnen Font-Server sind durch Kommas zu trennen.
- `catalogue` — Eine geordnete Liste mit zu verwendenden Font-Pfaden mit Font-Dateien. Dabei muss nach jedem Font-Pfad, und bevor ein neuer Font-Pfad gestartet werden kann, ein Komma gesetzt werden.

  Sie können die Zeichenkette `:unscaled` unmittelbar nach dem Font-Pfad verwenden, um die nicht nicht skalierten Fonts dieses Pfades zuerst zu laden. Anschließend können Sie den gesamten Pfad erneut angeben, um andere skalierte Fonts zu laden.
- `client-limit` — Stellt die Anzahl an Clients ein, die dieser Server verwaltet, bevor er weitere Bearbeitungsvorgänge verweigert. Der Standardwert lautet `10`.
- `clone-self` — Gibt an, ob der Font-Server eine neue Version von sich selbst klont, wenn `client-limit` erreicht ist. Standardmäßig ist diese Option auf `on` eingestellt.
- `default-point-size` — Stellt die standardmäßige Punktgröße für alle Fonts ein, die keinen spezifischen Wert aufweisen. Der Standardwert von `120` entspricht 12-Punkt-Fonts.
- `default-resolutions` — Gibt eine Liste mit vom XFree86-Server unterstützten Auflösungen an. Die Auflösungen der Liste müssen dabei durch Kommas getrennt sein.
- `deferglyphs` — Gibt an, ob mit dem Laden von *glyphs* (der Grafik, die eine Font visuell darstellt) gewartet werden soll. Diese Option kann mit `none` deaktiviert werden. Alternativ kann sie auch für alle Fonts, `all`, oder nur für 16-Bit-Fonts, `16`, aktiviert werden.
- `error-file` — Hiermit können Sie den Pfad- und Dateinamen von Speicherorten eingeben, wo `xfs`-Fehler protokolliert werden können.
- `no-listen` — Weist `xfs` an, nicht mithilfe eines bestimmten Protokolls zu warten. Standardmäßig ist diese Option auf `tcp` eingestellt, um zu verhindern, dass `xfs` an TCP-Ports wartet, dies vor allem aus Sicherheitsgründen. Wenn Sie `xfs` verwenden möchten, um Fonts an vernetzte Workstations in einem LAN weiterzuleiten, müssen Sie diese Zeile entfernen.
- `port` — Gibt den TCP-Port an, an dem `xfs` wartet, wenn `no-listen` entweder nicht vorhanden ist oder auskommentiert wurde.
- `use-syslog` — Gibt an, ob das Fehlerprotokoll des Systems zu verwenden ist.

7.4.2.2. Hinzufügen von Fonts zu `xfs`

Um dem Core X Font-Subsystem (`xfs`) Fonts hinzuzufügen, folgen Sie diesen Schritten:

1. Erstellen Sie ein Font-Verzeichnis, sofern nicht vorhanden, mit dem Namen `/usr/share/fonts/local/` unter Verwendung des folgenden Befehls als root:
   ```
   mkdir /usr/share/fonts/local/
   ```
   Sollte es nötig sein, das Verzeichnis `/usr/share/fonts/local/` zu erstellen, muss dieses zum `xfs`-Pfad hinzugefügt werden. Dies geschieht durch Aufrufen des folgenden Befehls als root:
   ```
   chkfontpath --add /usr/share/fonts/local/
   ```
2. Kopieren Sie die neuen Font-Dateien in das Verzeichnis `/usr/share/fonts/local/`.

3. Aktualisieren Sie die Font-Information durch Ausführen des folgenden Befehls als root:
   `ttmkfdir -d /usr/share/fonts/local/ -o /usr/share/fonts/local/fonts.scale`
4. Starten Sie den `xfs` Font-Server neu. Benutzen Sie dazu den folgenden Befehl als root:
   `service xfs reload`

7.5. Runlevels und XFree86

In den meisten Fällen konfiguriert eine Standardinstallation von Red Hat Linux einen Rechner zum Booten in die graphische Oberfläche, als Runlevel 5 bekannt. Es ist allerdings möglich, in eine textbasierte Oberfläche, auch Runlevel 3 genannt, zu Booten und eine X Session von dort zu beginnen.

Für mehr Informationen zu Runlevels, sehen Sie Abschnitt 1.4.

Dieser Abschnitt behandelt das Starten von XFree86 in beide, Runlevel 3 und Runlevel 5.

7.5.1. Runlevel 3

Wenn Sie sich im Runlevel 3 befinden, ist es empfehlenswert X mit dem Befehl `startx` zu starten. `startx` ist ein Front-End zum Befehl `xinit`, das den XFree86-Server startet und ihn mit X-Clients verbindet. Da Sie bereits im Runlevel 3 im System angemeldet sein müssen, startet `startx` weder den Display-Manager, noch authentifiziert er Benutzer. Sehen Sie Abschnitt 7.5.2 für weitere Informationen zu einem Display-Manager.

Wenn `startx` startet, wird nach der Datei `.xinitrc` im Home-Verzeichnis des Benutzers gesucht, um die auszuführenden X-Clients zu definieren. Ist diese Datei nicht vorhanden, wird das Standardskript `/etc/X11/xinit/xinitrc` ausgeführt.

Das standardmäßige `xinitrc`- Skript sucht anschließend im Home-Verzeichnis des Benutzers nach benutzerdefinierten Dateien und standardmäßigen Systemdateien, einschließlich `.Xresources`, `.Xmodmap` und `.Xkbmap`, und nach `Xresources`, `Xmodmap` und `Xkbmap` im Verzeichnis `/etc/X11/`. Die Dateien `Xmodmap` und `Xkbmap` werden, sofern sie vorhanden sind, vom Dienstprogramm `xmodmap` verwendet, um die Tastatur zu konfigurieren. Die `Xresources`-Dateien werden gelesen, um bestimmten Applikationen spezifische Präferenzwerte zuzuweisen.

Nachdem diese Optionen eingestellt sind, führt das Skript `xinitrc` alle Skripte im Verzeichnis `/etc/X11/xinit/xinitrc.d` aus. Ein wichtiges Skript dieses Verzeichnisses ist `xinput`, womit Einstellungen wie die zu verwendende Standardsprache und Desktop-Umgebung konfiguriert werden.

Anschließend versucht das Skript `xinitrc`, `.Xclients` im Home-Verzeichnis des Benutzers auszuführen, und kehrt zu `/etc/X11/xinit/Xclients` zurück, wenn diese Datei nicht gefunden wird. Der Zweck der Datei `Xclients` ist der Start der Desktop-Umgebung oder, wenn möglich, nur eines einfachen Window Managers. Das Skript `.Xclients` des Home-Verzeichnisses startet die vom Benutzer angegebene Desktop-Umgebung oder den Window Manager in der Datei `.Xclients-default`. Wenn `.Xclients` nicht im Home-Verzeichnis vorhanden ist, versucht das Standardskript `/etc/X11/init/Xclients`, eine andere Desktop-Umgebung zu starten und verwendet hierzu zunächst GNOME, dann KDE und anschließend `twm`.

Wenn der Benutzer sich aus X abmeldet, wird dieser sich wieder im Textmodus des Runlevel 3 befinden.

7.5.2. Runlevel 5

Wenn das System in den Runlevel 5 bootet, wird eine spezielle X Client Applikation, Display Manager genannt, gestartet. Ein Benutzer muss sich gegen den Display Manager authentifizieren, bevor Desktop-Umgebungen oder Window Manager gestartet werden.

Je nach den auf Ihrem System installierten Desktop-Umgebungen stehen drei verschiedene Display Manager für die Benutzer-Authentifizierung zur Verfügung.

- `gdm` — Der in Red Hat Linux standardmäßig ausgewählte Display Manager. `gdm` erlaubt dem Benutzer Spracheinstellungen zu ändern, den Computer herunterzufahren, neu zu starten oder sich im System anzumelden.
- `kdm` — Der KDE Display Manager erlaubt dem Benutzer, den Computer herunterzufahren, neu zu starten oder sich im System anzumelden.
- `xdm` — Ein sehr einfacher Display Manager, welcher es dem Benutzer lediglich erlaubt sich im System anzumelden.

Wenn das System in den Runlevel 5 bootet, bestimmt das Skript `prefdm` den bevorzugten Display Manager für die Benutzer-Authentifizierung. Hierzu wird die Datei `/etc/sysconfig/desktop` verwendet. Sehen Sie die Datei `/usr/share/doc/initscripts-<version-number>/sysconfig.txt` (wobei *<version-number>* die Versionsnummer des `initscripts`-Pakets ist) für eine Liste der für diese Datei verfügbaren Optionen.

Jeder Display Manager verwendet die Datei `/etc/X11/xdm/Xsetup_0`, um den Anmeldebildschirm einzurichten. Sobald sich der Benutzer am System anmeldet, wird das Skript `/etc/X11/xdm/GiveConsole` ausgeführt, um dem Benutzer die Konsole als Eigentum zuzuweisen. Dann wird das Skript `/etc/X11/xdm/Xsession` ausgeführt, um viele der Aufgaben auszuführen, die in der Regel vom Skript `xinitrc` beim Start von X in Runlevel 3 ausgeführt werden. Dazu gehören u.a. das Festlegen der System- und Benutzerressourcen oder das Ausführen der Skripte im Verzeichnis `/etc/X11/xinit/xinitrc.d/`.

Der Benutzer kann mithilfe des `gdm`- oder `kdm`-Display Managers angeben, welche Desktop-Umgebung bei der Authentifizierung verwendet werden sollen. Die Display Manager können im Menü **Sitzung** ausgewählt werden. Ist die Desktop-Umgebung nicht im Display Manager angegeben, prüft das Skript `/etc/X11/xdm/Xsession` die Dateien `.xsession` und `.Xclients` im Home-Verzeichnis, um zu entscheiden, welche Desktop-Umgebung geladen werden soll. Als letzte Möglichkeit wird die Datei `/etc/X11/xinit/Xclients` verwendet, um eine Desktop-Umgebung oder einen Window Manager zu wählen, der auf die gleiche Weise wie in Runlevel 3 benutzt wird.

Wenn der Benutzer eine X-Sitzung in der Standardanzeige beendet (`:0`) und sich abmeldet, wird das Skript `/etc/X11/xdm/TakeConsole` ausgeführt und weist dem root die Konsole neu zu. Der ursprüngliche Display Manager, der nach der Anmeldung weiter ausgeführt wurde, übernimmt die Steuerung und erzeugt einen neuen Display Manager. Auf diese Weise wird der XFree86-Server neu gestartet, ein neuer Anmeldebildschirm angezeigt und der gesamte Prozess neu gestartet.

Wenn sich der Benutzer aus X (Runlevel 5) abmeldet, wird dieser sich wieder im Display Manager befinden.

Für weitere Informationen darüber, wie Display Manger die Benutzerauthentifizierung steuern, sehen Sie die Datei /usr/share/doc/gdm-*<version-number>*/README (wobei *<version-number>* die Versionsnummer des installierten `gdm`-Pakets ist) und die `xdm` man-Seiten.

7.6. Zusätzliche Ressourcen

Über den XFree86-Server, die damit verbundenen Clients und die entsprechenden Desktop-Umgebungen sowie Window Manager ist noch lange nicht alles gesagt. Für erfahrene Benutzer können daher die zusätzlichen Ressourcen von großem Nutzen sein.

7.6.1. Installierte Dokumentation

- `/usr/X11R6/lib/X11/doc/README` — Beschreibt kurz die XFree86-Architektur und wie Einsteiger zusätzliche Informationen über das XFree86-Projekt erhalten.
- `>/usr/X11R6/lib/X11/doc/RELNOTES` — Für erfahrene Benutzer, die sich über die Neuheiten von XFree86 informieren möchten.
- `man XF86Config` — Enthält Informationen über die Konfigurationsdateien von XFree86, einschließlich der Bedeutung und der Syntax für die verschiedenen Abschnitte innerhalb der Dateien.
- `man XFree86` — Die wichtigste man-Seite für alle Informationen in Bezug auf XFree86. Hier werden der Unterschied zwischen den X-Serververbindungen auf lokaler Ebene und über ein Netzwerk detailliert beschrieben, übliche Umgebungsvariablen dargestellt, Optionen von Befehlszeilen erläutert und hilfreiche administrative Schlüsselkombinationen gegeben.
- `man Xserver` — Beschreibt den X Display Server.

7.6.2. Nützliche Webseiten

- http://www.xfree86.org — Die Home-Page des XFree86-Projekts, die die XFree86 Open Source-Version des X Window Systems bietet. XFree 86 steuert gemeinsam mit Red Hat Linux die notwendige Hardware und stellt die GUI-Umgebung zur Verfügung.
- http://dri.sourceforge.net — Home-Page des DRI-Projekts (Direct Rendering Infrastructure). DRI ist die wesentliche 3D-Hardwarebeschleunigungskomponente von XFree86.
- http://www.redhat.com/mirrors/LDP/HOWTO/XFree86-HOWTO — Ein HOWTO-Dokument mit einer detaillierten Beschreibung der manuellen Installation und der benutzerdefinierten Konfiguration von XFree86.
- http://www.gnome.org/ — Home-Page des GNOME Projekts.
- http://www.kde.org/ — Home-Page für die KDE Desktop-Umgebung.
- http://nexp.cs.pdx.edu/fontconfig/ — Home-Page des Fontconfig Font-Subsystems für XFree86.

7.6.3. Zusätzliche Literatur

- *The Concise Guide to XFree86 for Linux* von Aron Hsiao; Que — Der Kommentar eines Experten über die Funktionsweise von XFree86 auf Linux-Systemen.
- *The New XFree86* von Bill Ball; Prima Publishing — Liefert einen guten und umfassenden Überblick über XFree86 in Zusammenhang mit den beliebtesten Desktop-Umgebungen wie GNOME und KDE.
- *Beginning GTK+ and GNOME* von Peter Wright; Wrox Press, Inc. — Eine Einführung für Programmierer in GNOME-Architektur und eine Erläuterung von GTK+.
- *GTK+/GNOME Application Development* von Havoc Pennington; New Riders Publishing — Fortgeschrittene Kenntnisse der GTK+-Programmierung, insbesondere über den Sample-Code und verfügbare APIs.
- *KDE 2.0 Development* von David Sweet und Matthias Ettrich; Sams Publishing — Leitet noch unerfahrene und erfahrene Entwickler an, wie die vielen Umgebungsrichtlinien am besten genutzt werden können, um QT-Anwendungen für KDE zu erstellen.

II. Netzwerk-Services

Unter Red Hat Linux ist es möglich eine große Bandbreite von Netzwerk-Services einzusetzen. Dieser Teil beschreibt wie Netzwerk-Services konfiguriert werden, und gibt detailierte Informationen zu kritischen Netzwerk-Services wie NFS, Apache HTTP-Server, Sendmail, Fetchmail, Procmail, BIND und LDAP.

Inhaltsverzeichnis

redhat.

Kapitel 8.

Netzwerk-Schnittstellen

Bei der Verwendung von Red Hat Linux verläuft die gesamte Netzwerkkommunikation zwischen konfigurierten Software-*Schnittstellen* und den Netzwerkgeräten, die mit dem System verbunden sind.

Die Konfigurationsdateien für die verschiedenen Netzwerkschnittstellen und die Skripts zu deren Aktivierung oder Deaktivierung befinden sich im `/etc/sysconfig/network-scripts/`-Verzeichnis. Die bestimmten Schnittstellendateien können je nach System zwar unterschiedlich sein, es gibt aber grundsätzlich drei verschiedene Dateitypen in diesem Verzeichnis:

- *Schnittstellenkonfigurationsdateien*
- *Schnittstellenkontrollskripte*
- *Netzwerkfunktionsdateien*

Die Dateien in jeder dieser Kategorien arbeiten zusammen, um es Red Hat Linux zu ermöglichen, auf die verschiedenen Netzwerkgeräte zurückzugreifen.

Dieses Kapitel beschäftigt sich mit den Verbindungen zwischen diesen Dateien und ihrer Verwendungsweise.

8.1. Netzwerk-Konfigurationsdateien

Bevor wir die Schnittstellen-Konfigurationsdateien an sich nochmals untersuchen, führen wir die von Red Hat Linux zur Netzwerk-Konfiguration verwendeten Primär-Konfigurationsdateien einzeln auf. Das Verständnis der Rolle, die diese Dateien bei der Einrichtung des Netzwerk-Stack spielen, kann beim benutzerdefinieren eines Red Hat Linux Systems nützlich sein.

Folgende sind primäre Netzwerk-Konfigurationsdateien:

- `/etc/hosts` — Hauptzweck dieser Datei ist es, Host-Namen zu lösen, die nicht anderweitig gelöst werden können. Sie kann auch zur Lösung von Host-Namen auf kleineren Netzwerken ohne DNS-Server verwendet werden. Unabhängig davon, an welchem Netzwerk der Computer angeschlossen ist, sollte diese Datei eine Zeile enthalten, die die IP-Adresse des Loopback-Gerätes (`127.0.0.1`) als `localhost.localdomain` angibt. Weitere Informationen finden Sie unter den Hosts im Handbuch.
- `/etc/resolv.conf` — diese Datei gibt die IP-Adressen von DNS-Servern und die Suchdomäne an. Wenn nicht anders konfiguriert, ist diese Datei voll von Initialisierungs-Skripts. Weitere Informationen zu dieser Datei finden Sie auf den man-Seiten von `resolv.conf`.
- `/etc/sysconfig/network` — gibt Routing- und Host-Informationen für alle Netzwerk-Schnittstellen an. Weitere Informationen zu dieser Datei und darüber, welche Anweisungen sie akzeptiert, finden Sie unter Abschnitt 4.1.23.
- `/etc/sysconfig/network-scripts/ifcfg-<interface-name>` — für jede Netzwerk-Schnittstelle eines Red Hat Linux-Systems gibt es ein entsprechendes Schnittstellen-Konfigurationsskript. Jede dieser Dateien liefert Informationen, die für eine besondere Netzwerk-Schnittstelle spezifisch sind. Unter Abschnitt 8.2 finden Sie weitere Informationen zur Art der Datei und welche Anweisungen sie akzeptiert.

Achtung

Das Verzeichnis `/etc/sysconfig/networking/` wird vom **Netzwerk-Verwaltungstool** (`redhat-config-network`) verwendet, und sein Inhalt sollte nicht manuell bearbeitet werden. Weitere Informationen zur Konfiguration von Netzwerk-Schnittstellen anhand von **Netzwerk-Verwaltungstool** finden Sie im Kapitel *Netzwerk-Konfiguration* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

8.2. Schnittstellen-Konfigurationsdateien

Schnittstellen-Konfigurationsdateien steuern die Software-Schnittstellen der einzelnen Netzwerkschnittstellengeräte. Wenn das System bootet, verwendet es diese Dateien, um zu erfahren, welche Schnittstellen automatisch gestartet werden und wie diese zu konfigurieren sind. Diese Dateien heißen normalerweise `ifcfg <Gerät>`, wobei `<Gerät>` sich auf den Namen des Geräts bezieht, das von der Konfigurationsdatei gesteuert wird.

8.2.1. Ethernet- Schnittstellen

Zu den am meisten verwendeten Schnittstellendateien gehört auch `ifcfg-eth0`, mit der die erste Ethernet *Netzwerk-Schnittstellen-Karte* im System, auch *NIC* genannt, gesteuert wird. In einem System mit mehreren NICs gibt es entsprechend mehrere `ifcfg eth<X>` Dateien (wobei `<X>` eine eindeutige Nummer ist, je nach der entsprechenden Schnittstelle). Da jedes Gerät über eine eigene Konfigurationsdatei verfügt, können Sie die Funktionalität jeder einzelnen Schnittstelle steuern.

Nachfolgend eine Muster-`ifcfg-eth0` für ein System mit einer festen IP-Adresse:

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.1.0
NETMASK=255.255.255.0
IPADDR=10.0.1.27
USERCTL=no
```

Die in einer Schnittstellen-Konfigurationsdatei benötigten Werte können sich auf der Grundlage von anderen Werten ändern. Die `ifcfg-eth0`-Datei für eine Schnittstelle mit DHCP sieht beispielsweise etwas anders aus, weil die IP-Information vom DHCP-Server zur Verfügung gestellt wird:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Sie werden wahrscheinlich meistens ein GUI-Dienstprogramm, wie z.B. **Netzwerk-Verwaltungstool** (`redhat-config network`), verwenden, um in den verschiedenen Schnittstellen-Konfigurationsdateien Änderungen vorzunehmen. Anleitungen zur Verwendung dieses Tools finden Sie im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*

Sie können die Konfigurationsdatei für eine bestimmte Netzwerkschnittstelle auch manuell bearbeiten.

Folgend ist eine Liste mit konfigurierbaren Parametern für eine Konfigurationsdatei einer Ethernet-Schnittstelle:

- `BOOTPROTO=<Protokoll>`, wobei `<Protokoll>` für eine der folgenden Varianten stehen kann:
  - `none` — Es sollte kein Boot-Time-Protokoll verwendet werden.

  - `bootp` — Das BOOTP-Protokoll sollte verwendet werden.
  - `dhcp` — Das DHCP-Protocoll sollte verwendet werden.

- `BROADCAST=<Adresse>`, wobei `<Adresse>` für die Broadcast-Adresse steht. Diese Anweisung wird missbilligt.
- `DEVICE=<Name>`, wobei `<Name>` der der Name des physischen Geräts ist (ausgenommen dynamisch-zugewiesene PPP- Geräte, bei denen es der *logische Name*) ist.
- `DNS{1,2}=<Adresse>`, wobei `<Adresse>` eine Name-Server-Adresse ist, die in `/etc/resolv.conf` gesetzt wird, wenn die Anweisung `PEERDNS` auf `yes` steht.
- `IPADDR=<Adresse>`, wobei `<Adresse>` die IP-Adresse ist.
- `NETMASK=<Maske>`, wobei `<Make>` der Wert der Netzmaske ist.
- `NETWORK=<Adresse>`, wobei `<Adresse>` die Netzwerkadresse ist. Diese Anweisung wird nicht länger verwendet.
- `ONBOOT=<Antwort>`, wobei `<Antwort>` Folgendes bedeuten kann:
  - `yes` — Dieses Gerät sollte beim Booten aktiviert werden.
  - `no` — Dieses Gerät sollte nicht beim Booten aktiviert werden.

- `PEERDNS=<Antwort>`, wobei `<Antwort>` eine der folgenden ist:
  - `yes` — Ändern Sie `/etc/resolv.conf`, wenn die DNS-Anweisung gesetzt ist. Verwenden Sie DCHP, dann ist `yes` Standard.
  - `no` — ändern Sie `/etc/resolv.conf` nicht.
  - `SRCADDR=<Adresse>`, wobei `<Adresse>` die angegebene Ausgangs-IP-Adresse für ausgehende Pakete ist.
  - `USERCTL=<Antwort>`, wobei `<Antwort>` Folgendes bedeuten kann:
    - `yes` — Nicht-root dürfen dieses Gerät kontrollieren.
    - `no` — Nicht-root dürfen dieses Gerät nicht kontrollieren.

8.2.2. Schnittstellen für den Verbindungsaufbau

Wenn Sie über einen Dialup-Account mit dem Internet verbinden, brauchen Sie eine Konfigurationsdatei für diese Schnittstelle.

PPP-Schnittstellendateien haben das Format `ifcfg-ppp<X>` (wobei `<X>` eine eindeutige, einer spezifischen Schnittstelle entsprechende Nummer ist).

Die Konfigurationsdatei der PPP-Schnittstelle wird automatisch erzeugt, wenn Sie `wvdial`, **Netzwerk-Verwaltungstool** oder **Kppp** verwenden, um einen Dialup-Account zu erzeugen. Das *Red Hat Linux Handbuch Erster Schritte* enthält Anweisungen für die Verwendung dieser GUI-basierten Dialup-Verbindungstools. Sie können diese Datei aber auch manuell erstellen und bearbeiten.

Folgend ist eine typische `ifcfg-ppp0`-Datei:

```
DEVICE=ppp0
NAME=test
WVDIALSECT=test
```

```
MODEMPORT=/dev/modem
LINESPEED=115200
PAPNAME=test
USERCTL=true
ONBOOT=no
PERSIST=no
DEFROUTE=yes
PEERDNS=yes
DEMAND=no
IDLETIMEOUT=600
```

Serial Line Internet Protocol (SLIP) ist eine weitere Dialup-Schnittstelle, wird im allgemeinen aber seltener verwendet. Ein typischer Name für die Schnittstellen-Konfigurationsdatei der SLIP-Dateien ist z.B. `ifcfg-sl0`.

Folgende Optionen können in diesen Dateien verwendet werden:

- `DEFROUTE=<`*`Antwort`*`>`, wobei <*Antwort*> Folgendes bedeuten kann:
  - `yes` — Stellt diese Schnittstelle als Standardroute ein.
  - `no` — Stellt diese Schnittstelle nicht als Standardroute ein.

- `DEMAND=<`*`Antwort`*`>`, wobei <*Antwort*> Folgendes bedeuten kann:
  - `yes` — Mit dieser Schnittstelle kann `pppd` eine Verbindung starten.
  - `no` — Verbindungen mit dieser Schnittstelle müssen manuell hergestellt werden.

- `IDLETIMEOUT=<`*`Wert`*`>`, wobei <*Wert*> die Sekunden ohne Aktivität darstellt, nach denen die Schnittstelle die Verbindung selbst unterbricht.
- `INITSTRING=<`*`Zeichenkette`*`>`, wobei <*Zeichenkette*> die erste Zeichenfolge ist, die an das Modem übergeben wird. Diese Option wird hauptsächlich von SLIP-Schnittstellen verwendet.
- `LINESPEED=<`*`Wert`*`>`, wobei <*Wert*> die Baudrate des Gerätes angibt. Zu den möglichen Standardwerten gehören `57600`, `38400`, `19200` und `9600`.
- `MODEMPORT=<`*`Gerät`*`>`, wobei <*Gerät*> der Name des Serial-Geräts ist, das die Verbindung für die Schnittstelle herstellt.
- `MTU=<`*`Wert`*`>`, wobei <*Wert*> die *Maximum Transfer Unit (MTU)*-Einstellung für die Schnittstelle ist. Die MTU bezieht sich auf die größtmögliche Zahl von Daten (in Bytes), die ein Frame übertragen kann, die Header-Information nicht mitgezählt. Bei einigen Dial-up-Situationen hat die Einstellung dieses Werts auf `576` zur Folge, dass weniger Pakete ausgelassen werden (DROP) und die Durchlässigkeit für Verbindungen leicht erhöht wird.
- `NAME=<`*`Name`*`>`, wobei <*Name*> sich auf den Oberbegriff der Konfigurationssammlung für Dialup-Verbindungen bezieht.
- `PAPNAME=<`*`Name`*`>`, wobei <*Name*> für den Benutzernamen steht, der während der Änderung des *Password Authentication Protocol (PAP)* vergeben wurde und Ihnen die Verbindung zu einem Remote-System ermöglicht.
- `PEERDNS=<`*`Antwort`*`>`, wobei <*Antwort*> Folgendes bedeuten kann:
  - `yes` — Ändern Sie diese Dateieinträge von `/etc/resolv.conf` in Ihrem System, um die DNS-Server zu verwenden, die vom Remote-System nach der Herstellung der Verbindung zur Verfügung gestellt werden.
  - `no` — Die `/etc/resolv.conf` Datei wird nicht geändert.

- `PERSIST=<Antwort>`, wobei `<Antwort>` Folgendes bedeuten kann:
  - `yes` — Diese Schnittstelle sollte ständig aktiviert sein, auch wenn nach einem Abbruch das Modem deaktiviert wird.
  - `no` — Diese Schnittstelle sollte nicht ständig aktiv sein.

- `REMIP=<Adresse>`, wobei `<Adresse>` die IP-Adresse des Remote-Systems ist. Wird üblicherweise nicht festgelegt.
- `WVDIALSECT=<Name>`, wobei `<Name>` dieser Schnittstelle in `/etc/wvdial.conf` eine Anwähl-Konfiguration zuweist, die die anzuwählende Telefonnummer und andere wichtige Informationen für die Schnittstelle enthält.

8.2.3. Weitere Schnittstellen

Weitere übliche Schnittstellen-Konfigurationsdateien, die diese Optionen verwenden, sind die folgenden:

- `ifcfg-lo` — Ein lokale *Loopback-Schnittstelle* wird oft zum Testen verwendet, wie auch in Applikationen, die eine zum System zurückweisende IP-Adresse benötigen. Jegliche Daten, die zum Loopback-Gerät gesendet werden, werden augenblicklich zur Netzwerkschicht des Host zurückgegeben.

  
  Warnung

  Bearbeiten Sie niemals das Loopback-Schnittstellenskript `/etc/sysconfig/network-scripts/ifcfg-lo` von Hand. Andernfalls kann die richtige Funktionsweise des Systems beeinträchtigt werden.
- `ifcfg-irlan0` — Eine *Infrarot-Schnittstelle* sorgt dafür, dass Informationen zwischen Geräten wie Laptop und Drucker über einen Infrarot-Link fließen, welcher ähnlich arbeitet wie ein Ethernet-Gerät, mit dem Unterschied, dass es normalerweise über eine Peer-to-Peer-Verbindung läuft.
- `ifcfg-plip0` — Eine *parallele Zeilenschnittstellen-Protokoll (PLIP)*-Verbindung arbeitet auf ähnliche Weise, mit dem Unterschied, dass sie eine parallelen Schnittstelle verwendet.
- `ifcfg-tr0` — *Token Ring* Topologien sind nicht mehr so verbreitet auf *Local Area Networks* (*LANs*), da sie durch Ethernet verdrängt wurden.

8.2.4. Alias- und Clone-Dateien

Zwei weniger verwendete Arten von Schnittstellen-Konfigurationsdateien im `/etc/sysconfig/network-scripts` Verzeichnis sind *Alias*- und *Clone* Dateien.

Die Namen von Alias-Schnittstellen-Konfigurationsdateien haben Namen im Format von `ifcfg-<wenn-Name>:<Alias-Wert>` und erlaubt es einem Alias, auf eine Schnittstelle zu verweisen. Eine `ifcfg-eth0:0`-Datei kann z.B. so konfiguriert werden, dass sie `DEVICE=eth0:0` und eine statische IP-Adresse 10.0.0.2 spezifieren kann und somit als Alias einer bereits konfigurierten Ethernet-Schnittstelle dienen kann, um ihre IP- Informationen über DHCP in `ifcfg-eth0` zu empfangen. An dieser Stelle ist das `eth0`-Gerät mit einer dynamischen IP-Adresse verknüpft, kann aber jederzeit über die feste 10.0.0.2 IP-Adresse auf das System zurückgreifen.

Bei der Namensgebung einer Schnittstellen-Konfigurationsdatei sollten folgende Konventionen eingehalten werden: `ifcfg-<wenn-Name>-<Clone-Name>`. Während mit einer Alias-Datei auf eine

bereits bestehende Schnittstellen-Konfigurationsdatei zurückgegriffen werden kann, wird eine Clone-Datei zum Festlegen zusätzlicher Optionen während der Spezifizierung einer Schnittstelle verwendet. Die standardmäßige DHCP Ethernet-Schnittstelle mit dem Namen `eth0` kann deshalb wie folgt oder ähnlich aussehen:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
```

Da `USERCTL` auf `no` eingestellt ist, können Benutzer wenn nichts anderes angegeben wird, diese Schnittstelle nicht starten oder beenden. Um den Benutzern dies zu ermöglichen, erstellen Sie einen Clone durch Kopieren von `ifcfg-eth0` in `ifcfg-eth0-user` und fügen Sie folgende Zeile hinzu:

```
USERCTL=yes
```

Wenn ein Benutzer mit dem Befehl `ifup eth0-user` die `eth0`-Schnittstelle startet, werden die Konfigurationsoptionen von `ifcfg-eth0` und `ifcfg-eth0-user` kombiniert. Dies ist zwar nur ein sehr einfaches Beispiel, diese Methode kann über für viele verschiedene Optionen und Schnittstellen verwendet werden.

Der einfachste Weg zur Erstellung von Alias- und Clone Schnittstellen-Konfigurationsdateien ist die Verwendung des grafischen **Netzwerk-Verwaltungstool**. Weitere Informationen zur Verwendung dieses Tools finden Sie im Kapitel *Netzwerk-Konfiguration* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

8.3. Schnittstellen-Kontrollskripts

Die Schnittstellen-Kontrollskripts aktivieren und deaktivieren Systemschnittstellen. Die zwei wichtigsten Schnittstellen-Kontroll-Skripts sind `/sbin/ifdown` und `/sbin/ifup`, die verschiedene andere Kontrollskripte aus dem `/etc/sysconfig/network scripts/`-Verzeichnis verwenden.

`ifdown` und `ifup` sind symbolische Links zu den Skripte im `/sbin/`-Verzeichnis. Wenn eines der beiden Skripte aufgerufen wird, verlangen sie, dass ein Schnittstellenwert angegeben wird, wie z.B.:

```
ifup eth0
Determining IP information for eth0... done.
```

An dieser Stelle werden `/etc/sysconfig/network-scripts/network functions` und `/etc/rc.d/init.d/functions` dazu verwendet, eine ganze Reihe von Aufgaben zu erfüllen. Weitere Informationen finden Sie unter Abschnitt 8.4.

Nachdem sichergestellt ist, dass eine Schnittstelle angegeben wurde und dass der Benutzer, der diese Anfrage ausführt, die Berechtigung zur Steuerung der Schnittstelle hat, wird das richtige Skript für diesen Schnittstellengerätetyp aufgerufen. Zu den gängigsten Schnittstellen-Kontrollskripten gehören die folgenden:

- `ifup-aliases` — Konfiguriert die IP-Aliase der Schnittstellen-Konfigurationsdateien, wennn einer Schnittstelle mehr als eine IP-Adresse zugeordnet ist.
- `ifdown-cipcb` und `ifup-cipcb` — Werden zum Starten und Beenden von *Crypto IP Encapsulation (CIPE)*-Verbindungen verwendet.
- `ifdown-ipv6` und `ifup-ipv6` — Enthalten IPv6-ähnliche Funktionen, die Umgebungsvariablen in verschiedenen Schnittstellen-Konfigurationsdateien und `/etc/sysconfig/network` verwenden.
- `ifup-ipx` — Wird zum Starten einer IPX-Schnittstelle verwendet.

- `ifup-plip` — Wird zum Starten einer PLIP-Schnittstelle verwendet.
- `ifup-plusb` — Wird zum Starten einer USB-Schnittstelle für Netzwerkverbindungen verwendet.
- `ifdown-post` und `ifup-post` — Enthalten Befehle, die nach dem Starten oder Beenden einer Schnittstelle ausgeführt werden müssen.
- `ifdown-ppp` und `ifup-ppp` — Werden zum Starten oder Beenden einer PPP-Schnittstelle verwendet.
- `ifup-routes` — Fügt statische Routes für ein bestimmtes Gerät hinzu, wenn dessen Schnittstelle aktiviert wird.
- `ifdown-sit` und `ifup-sit` — Enthalten eine Funktion, die zum Aktivieren und Deaktivieren eines IPv6- Tunnels in einer IPv4-Verbindung aufgerufen wird.
- `ifdown-sl` und `ifup-sl` — Wird zum Starten und Beenden einer SLIP Schnittstelle verwendet.

Warnung

Achten Sie darauf, dass das Entfernen oder Modifizieren irgendeines Skripts im `/etc/sysconfig/network-scripts/`-Verzeichnis dazu führen kann, dass Schnittstellenverbindungen seltsam reagieren oder scheitern, da sie von diesen Skripts abhängig sind. Nur erfahrene Benutzer sollten daher Skripts verändern, die für eine Netzwerkschnittstelle relevant sind.

Der einfachste Weg, alle Netzwerk-Skripte gleichzeitig zu ändern ist es, den Befehl `/sbin/service` auf dem Netzwerk-Service (`/etc/rc.d/init.d/network`) wie folgt auszuführen:

```
/sbin/service network <action>
```

<*Aktion*> steht entweder für `start`, `stop` oder `restart`.

Um eine Liste der konfigurierten Geräte und der augenblicklich aktiven Netzwerk-Schnittstellen anzuzueigen, benutzen Sie folgenden Befehl:

```
/sbin/service/network status
```

8.4. Netzwerkfunktionsdateien

Red Hat Linux nutzt verschiedene Dateien, die wichtige Informationen enthalten, mit denen Schnittstellen aktiviert und deaktiviert werden. Diese Funktionen werden in einigen wenigen Dateien in geeigneter Weise gruppiert und können bei Bedarf einfach abgerufen werden.

Die gängigste Netzwerkfunktionsdatei ist `/etc/sysconfig/network-scripts/network-functions`. Diese Datei enthält eine Vielzahl von allgemeinen IPv4-Funktionen, die für viele Schnittstellenkontrollskripts hilfreich sind. Hierzu gehört das Kontaktieren laufender Programme, die Informationen zu den Änderungen des Schnittstellenstatus benötigen, das Einrichten von Host-Namen, die Suche eines Gateway-Gerätes, das Prüfen, ob ein bestimmtes Gerät ausgefallen ist oder nicht, und das Hinzufügen einer Standard-Route.

Da die Funktionen, die für die IPv6-Schnittstellen benötigt werden, sich von denen für IPv4-Schnittstellen unterscheiden, gibt es eine `network functions-ipv6`-Datei, in der speziell diese Informationen enthalten sind. Der IPv6-Support muss im Kernel aktiviert sein, um über dieses Protokoll kommunizieren zu können. In der Datei `network-functions` ist eine Funktion enthalten, die überprüft, ob Ipv6-Support vorhanden ist. In dieser Datei finden Sie außerdem auch noch Funktionen, die statische IPv6-Routs konfigurieren und löschen, Tunnel erstellen und entfernen,

IPvC-Adressen einer Schnittstelle hinzufügen oder sie von dort entfernen und Dateien zum Testen, ob auf der Schnittstelle eine IPv6-Adresse existiert.

8.5. Zusätzliche Ressourcen

Die folgenden Resssourcen enthalten mehr Informationen zu Netzwerk-Skripten und können an den Folgenden Stellen gefunden werden:

- `/usr/share/doc/initscripts-<version>/sysconfig.txt` — Ein verständlicher Leitfaden zu verfügbaren Optionen für Netzwerk-Konfigurationsdateien, einschließlich IPv6-Optionen, die in diesem Kapitel nicht behandelt werden.
- `/usr/share/doc/iproute-<version>/ip-cref.ps` — Diese Postscript™ Datei enthält eine Vielzahl an Informationen zu `ip`, die u.a. zur Bearbeitung von Routing-Tabellen verwendet werden können. Werfen Sie einen Blick auf diese Datei mit **ghostview** oder **kghostview**.

redhat

Kapitel 9.

Network File System (NFS)

Mit *NFS (Network File System)* können Hosts Partitionen auf einem Remote-System mounten und verwenden, als wären sie ein lokales Dateisystem. Dadurch können Dateien an einem zentralen Ort organisiert werden, während entsprechend berechtigte Benutzer kontinuierlichen Zugriff auf sie haben.

Zur Zeit werden zwei Versionen von NFS verwendet. Die Version 2 von NFS (NFSv2), die seit mehreren Jahren verwendet wird, wird umfassend von verschiedenen Betriebssystemen unterstützt. Die Version 3 von NFS (NFSv3) verfügt über mehr Features, einschließlich einer variablen Dateigröße und einem besseren Fehlerreport. Red Hat Linux unterstützt beide Versionen und verwendet NFSv3 standardmäßig für die Verbindung mit einem Server, der es ebenfalls unterstützt.

Dieses Kapitel betrachtet die Version 2 von NFS, obwohl viele Konzepte auch für die Version 3 gelten. Weiterhin stehen nur grundsätzliche Konzepte und ergänzende Informationen zur Verfügung. Spezielle Anweisungen bezüglich der Konfiguration und Funktionsweise eines NFS auf Clients oder Servern finden Sie im Kapitel *Network File System (NFS)* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

9.1. Methodologie

Linux verwendet für das NFS Datei-Sharing eine Kombination aus dem Kernel-Level-Support und den ständig ausgeführten Daemon-Prozessen, wobei der Support für das NFS im Linux-Kernel aktiviert sein muß. NFS verwendet *Remote Procedure Calls (RPC)*, um Anfragen zwischen Clients und Servern zu senden. Dazu muss der Dienst `portmap` sowie die korrekten Runlevel für die NFS- Kommunikation aktiviert sein. Wenn Sie mit `portmap` arbeiten, wird durch verschiedene andere Prozesse sichergestellt, dass eine bestimmte NFS-Verbindung zugelassen und ohne Fehler ausgeführt werden kann:

- `rpc.mountd` — Der ausgeführte Prozess empfängt die Anfrage des NFS-Clients für das Mounten und kontrolliert, ob diese mit einem aktuell exportierten Dateisystem übereinstimmt.
- `rpc.nfsd` — Der Prozess, der die Benutzerplatz-Komponenten des NFS-Dienstes implementiert. Er verwendet den Linux-Kernel, um mit den dynamischen Vorgaben des NFS-Clients übereinzustimmen. Zum Beispiel zusätzliche Server-Threads für NFS- Clients.
- `rpc.lockd` — Ein Daemon, der bei neueren Kernels nicht benötigt wird. Das Sperren von NFS-Dateien wird nun vom Kernel durchgeführt. Für Benutzer, die einen älteren Kernel verwenden, der standardmäßig diese Funktion nicht enthält, ist der Daemon im Paket `nfs-utils` enthalten.
- `rpc.statd` — Implementiert das *Network Status Monitor (NSM)*-RPC- Protokoll. Es liefert die reeboot-Meldung, wenn ein NFS-Server neu gestartet wird, der nicht korrekt beendet wurde.
- `rpc.rquotad` — Ein RPC-Server, der Remote- Benutzern Informationen über die Benutzerquote liefert.

Für den NFS-Dienst sind nicht alle diese Programme notwendig. Die einzigen Dienste, die aktiviert sein müssen, sind `rpc.mountd` , `rpc.nfsd` und `portmap`. Die anderen Daemonen bieten zusätzliche Funktionen; sie sollten nur verwendet werden, wenn die Serverumgebung dies erfordert.

Die Version 2 von NFS verwendet das *User Datagram Protocol (UDP)*, um Netzwerk-Verbindung ohne Status zwischen dem Client und dem Server herzustellen. Die Version 3 von NFS kann UDP oder TCP verwenden, wenn sie über ein IP ausgeführt wird. Die UDP- Verbindung minimiert den Netzwerkverkehr, da der NFS-Server dem Client ein Cookie schickt, nachdem dieser für den Zugriff auf die gemeinsamen Dateien autorisiert worden ist. Dieses Cookie ist ein zufälliger Wert, der im Server gespeichert ist und mit allen RPC-Anfragen vom Client zum Server übermittelt wird. Der

NFS-Server kann ohne Auswirkung auf die Clients neu gestartet werden, das Cookie beleibt dabei intakt.

NFS führt Authentifizierungen nur dann durch, wenn ein Client versucht, ein Remote-Dateisystem zu mounten. Der NFS-Server verwendet zuerst TCP-Wrapper, um den Zugriff einzuschränken. Die TCP-Wrapper lesen die Dateien `/etc/hosts.allow` und `/etc/hosts.deny`, um festzulegen, ob einem bestimmten Host der Zugriff auf den NFS-Server erlaubt oder verwehrt wird. Weitere Informationen zum Konfigurieren der Zugriffssteuerung mit TCP-Wrapper finden Sie unter Kapitel 15.

Erhält der Client die Berechtigung, die TCP-Wrapper zu passieren, verweist der NFS-Server auf die Konfigurationsdatei `/etc/exports`, um festzulegen, ob der Client über ausreichende Privilegien zum Mounten der exportierten Dateisysteme verfügt. Ist der Zugriff gewährt, werden alle Datei- und Verzeichnisvorgänge mit Hilfe von RPC zum Server gesendet.

Warnung

Die NFS-Mount-Privilegien werden speziell für einen Client und nicht für einen Benutzer gewährt. Auf exportierte Dateisysteme kann von allen Benutzern auf dem Remote-Rechner zugegriffen werden.

Sie müssen beim Konfigurieren der Datei `/etc/exports` besonders vorsichtig sein, wenn Sie die Lese/Schreibberechtigung (`rw`) für das exportierte Dateisystem setzen.

9.1.1. NFS und `portmap`

NFS benötigt Remote Procedure Calls (RPC), um zu funktionieren. `portmap` wird benötigt, um die RPC-Anfragen den korrekten Dienste zuzuordnen. `portmap` wird von den RPC-Prozessen benachrichtigt, wenn sie starten. Des Weiteren teilen die Anfragen die überwachte Port-Nummer sowie die Nummern des RPS-Programms mit, die aufgerufen werden. Der Client kontaktiert `portmap` auf dem Server mit einer bestimmten RPC-Programmnummer. `portmap` leitet dann den Client zur richtigen Port-Nummer um, damit er mit dem gewünschten Dienst kommunizieren kann.

Da RPC-basierte Dienste für die Verbindungen mit ankommenden Client-Anfragen von `portmap` abhängig sind, muss `portmap` verfügbar sein, bevor einer dieser Dienste gestartet wird. Wenn `portmap` aus irgendeinem Grund unerwartet abgebrochen wird, starten Sie `portmap` und alle Dienste, die beim Start ausgeführt wurden, neu.

Der `portmap`-Dienst kann zusammen mit den Hosts- Zugriffsdateien von TCP Wrappers (`/etc/hosts.allow` und `/etc/hosts.deny`) verwendet werden, um zu steuern, welche Remote-Systeme RPC-basierte Dienste auf dem Server verwenden dürfen. Unter Kapitel 15 finden Sie weitere Informationen. Die Regeln für die Zugriffssteuerung für `portmap` gelten für alle RPC-basierten Dienste. Alternativ können Sie auch jeden der NFS-RPC-Daemonen einzeln bestimmen, auf den sich eine bestimmte Regel für die Zugriffssteuerung beziehen soll. Die man-Seiten für `rpc.mountd` und `rpc.statd` enthalten Informationen über die genaue Syntax dieser Regeln.

9.1.1.1. Troubleshooting NFS mit `portmap`

Da `portmap` die Koordination zwischen RPC- Diensten und den Port-Nummern übernimmt, die für die Kommunikation mit den Diensten verwendet werden, ist es beim Lösen von Problemen sehr hilfreich, eine Übersicht über die aktuellen RPC- Dienste zu haben, die `portmap` verwenden. Der Befehl `rpcinfo` zeigt jeden RPC-basierten Dienst mit Port-Nummer, RPC-Programmnummer, Version und dem Typ des IP- Protokolls (TCP oder UDP) an.

Sie können `rpcinfo -p` verwenden, um sicherzustellen, dass die richtigen NFS-RPC-basierten Dienste für `portmap` aktiviert sind:

```
program vers proto   port
```

```
100000    2   tcp    111  portmapper
100000    2   udp    111  portmapper
100024    1   udp   1024  status
100024    1   tcp   1024  status
100011    1   udp    819  rquotad
100011    2   udp    819  rquotad
100005    1   udp   1027  mountd
100005    1   tcp   1106  mountd
100005    2   udp   1027  mountd
100005    2   tcp   1106  mountd
100005    3   udp   1027  mountd
100005    3   tcp   1106  mountd
100003    2   udp   2049  nfs
100003    3   udp   2049  nfs
100021    1   udp   1028  nlockmgr
100021    3   udp   1028  nlockmgr
100021    4   udp   1028  nlockmgr
```

Die Option `-p` prüft den Portmapper auf einem bestimmten Host bzw. schlägt standardmäßig localhost vor, wenn kein spezieller Host aufgeführt ist. Auf der `rpcinfo`-man-Seite stehen weitere Optionen zur Verfügung.

Im oben aufgeführten Output werden NFS-Dienste angezeigt, die ausgeführt werden. Wenn einer der NFS-Dienste nicht korrekt startet, kann `portmap` die RPC-Anfragen von Clients für diesen Dienst nicht dem richtigen Port zuordnen. In vielen Fällen führt das Neustarten von NFS als Root (`/sbin/service nfs restart`) dazu, dass der Dienst korrekt in `portmap` registriert werden und arbeiten kann.

9.2. NFS-Server-Konfigurationsdateien

Das Konfigurieren eines Systems zur gemeinsamen Nutzung von Dateien und Verzeichnisse mithilfe von NFS ist einfach. Jedes Dateisystem, das via NFS an Remote-Benutzer exportiert wurde, sowie die Zugriffsrechte für diese Dateisysteme werden in der Datei `/etc/exports` abgelegt. Diese Datei wird mit dem Befehl `exportfs` gelesen. Dadurch erhalten `rpc.mountd` und `rpc.nfsd` die notwendigen Informationen, die benötigt werden, um das Remote-Mounting eines Dateisystems durch einen autorisierten Host zuzulassen.

Mit dem Befehl `exportfs` können Sie Verzeichnisse exportieren, ohne die verschiedenen NFS-Dienste neu starten zu müssen. Wenn `exportfs` die korrekten Optionen erhält, wird das zu exportierende Dateisystem in `/var/lib/nfs/xtab` gespeichert. Da `rpc.mountd` sich für das Festlegen der Privilegien für den Zugriff auf ein Dateisystem auf die Datei `xtab` bezieht, werden Änderungen an der Liste der exportierten Dateisysteme sofort wirksam.

Bei der Verwendung des Befehls `exportfs` stehen verschiedene Optionen zur Verfügung:

- `-r` — Alle, in `/etc/exports` aufgelistete Verzeichnisse werden exportiert und in `/etc/lib/nfs/xtab` wird eine neue Exportliste erstellt. Durch diese Option wird die Exportliste einschließlich aller Änderungen, die in `/etc/exports` vorgenommen wurden, aktualisiert.
- `-a` — Alle Verzeichnisse werden exportiert oder nicht exportiert, je nachdem, welche anderen Optionen in `exportfs` gewählt wurden.
- `-o` *`Optionen`* — Ermöglicht dem Benutzer, Verzeichnisse zum Exportieren festzulegen, die nicht in `/etc/exports` aufgeführt sind. Diese zusätzlichen Dateisystem-Shares müssen auf dieselbe

Weise gespeichert werden, wie sie in `/etc/exports` angegeben sind. Diese Option wird verwendet, um exportierte Dateisysteme zu testen, bevor sie endgültig zu der Liste der zu exportierenden Dateisysteme hinzugefügt werden.

- `-i` — Weist `exportfs` an, `/etc/exports` zu übergehen; in diesem Fall werden nur die Optionen, die von der Befehlszeile aus eingegeben wurden, zum Definieren der exportierten Dateisystems verwendet.
- `-u` — Exportiert keine Verzeichnisse, die von Remote-Benutzern gemountet wurden. Der Befehl `exportfs -ua` unterbricht das NFS-Datei-Sharing und führt die verschiedenen NFS-Daemonen weiter aus. Geben Sie den Befehl `exportfs -r` ein, um das NFS-Datei-Sharing fortzusetzen.
- `-v` — Verbose Operation, bei der exportierte oder nicht exportierte Dateisysteme detaillierter angezeigt werden, wenn der Befehl `exportfs` ausgeführt wird.

Wenn für den Befehl `exportfs` keine Optionen eingegeben werden, wird eine Liste der aktuell exportierten Dateisysteme angezeigt.

Änderungen in `/etc/exports` können gelesen werden, indem der NFS-Dienst mithilfe des Befehls `service nfs reload` neu geladen wird. Dabei wird der NFS-Daemon weiterhin ausgeführt, während die Datei `/etc/exports` erneut exportiert wird.

9.2.1. `/etc/exports`

Die Datei `/etc/exports` wird standardmäßig verwendet, um zu kontrollieren, welche Dateisysteme an welchen Host exportiert werden. Weiterhin wird sie verwendet, um bestimmte Optionen einzustellen, mit denen alles kontrolliert werden kann. Leere Zeilen werden ignoriert, Kommentare können mithilfe von `#` eingegeben werden, und lange Zeilen können durch einen Backslash (`\`) umgebrochen werden. Jedes exportierte Dateisystem sollte eine eigene Zeile haben. Listen von nicht autorisierten Hosts, die nach einem exportierten Dateisystem platziert sind, müssen durch Leerzeichen getrennt werden. Die Optionen für alle Hosts müssen in Klammern direkt nach der Hostbezeichnung stehen. Zwischen dem Host und der ersten Klammen ist kein Leerzeichen.

`/etc/exports` benötigt in seiner einfachsten Form nur das Verzeichnis, das exportiert wird und den Host, der es verwenden kann:

```
/some/directory bob.example.com
/another/exported/directory 192.168.0.3
```

Nachdem `/etc/exports` erneut mit dem Befehl `/sbin/service nfs reload` exportiert wurde, kann der Host `bob.example.com` die Datei `/some/directory` sowie `192.168.0.3` die Datei `/another/exported/directory` mounten. Da in diesem Beispiel keine Optionen festgelegt sind, werden verschiedene NFS-Präferenzen aktiviert:

- `ro` — Schreibgeschützt. Hosts, die dieses Dateisystem mounten, können es nicht ändern. Wenn Sie zulassen möchten, dass in dem Dateisystem Änderungen vorgenommen werden können, müssen Sie die Option `rw` verwenden (read-write, lesen-schreiben).
- `async` — Ermöglicht dem Server, in einer bestimmten Situation Daten auf die Platte zu schreiben. Diese Option ist in dem Fall uninteressant, wenn der Host nur schreibgeschützt auf Daten zugreifen kann. Wenn jedoch ein Host ein Dateisystem im Read-Write-Modus ändert, können im Fall eines Absturzes des Servers Daten verloren gehen. Bei der Option `sync` werden alle Dateien auf der Platte gesichert, bevor der Schreibschutz- Modus aufgehoben wird. Dadurch könnte die Leistung verlangsamt werden.
- `wdelay` — Weist den NFS-Server an, das Schreiben auf einer Platte zu verzögern, wenn das Aufheben des Schreibschutz-Modus bevorsteht. Dies kann die Leistung verbessern, indem die Anzahl der einzelnen Schreibbefehle für die Platte verringert wird. Mit der Option `no_wdelay` kann diese Funktion deaktiviert werden, die nur funktioniert, wenn Sie die Option `sync` verwenden.

- `root_squash` — Nimmt Root-Benutzern, welche Remote verbunden sind, deren Root-Rechte, indem diese die "nobody" Userid erhalten. Auf diese Weise wird die Kontrolle des Remote-Roots auf den niedrigsten lokalen Benutzer reduziert, was verhindert, dass der Remote-Benutzer auf dem lokalen System als Root agiert. Alternativ können Sie mit der Option `no_root_squash` das "Sqashing" des Roots deaktivieren. Um jeden Remote-Benutzer, einschließlich Root zu squashen, verwenden Sie die Option `all_squash`. Um die Benutzer und Gruppen-IDs festzulegen, die mit Remote-Benutzern eines bestimmten Hosts verwendet werden sollen, benutzen Sie die Optionen `anonuid` und `anongid`. Auf diese Weise können Sie ein spezielles Benutzer-Konto für Remote-NFS- Benutzer erstellen, um die Option `(anonuid=` *<UID-Wert>*`, anongid=` *<GID-Wert>*`)` festzulegen und gemeinsam zu verwenden. Hierbei steht *<UID-Wert>* für die ID-Nummer des Benutzers und *<GID-Wert>* für die ID-Nummer der Gruppe.

Um diese Standards zu übersteuern, müssen Sie eine Option festlegen, die diese Standards ersetzt. Wenn Sie zum Beispiel die Option `rw` nicht festlegen, werden exportierte Dateisysteme im Schreibschutzmodus verwendet. Für jedes exportierte Dateisystem müssen die Standardeinstellungen explizit übersteuert werden. Wo keine Standardwerte angegeben sind, stehen zusätzliche Optionen zur Verfügung. Diese bieten die Möglichkeit, das Überprüfen der Sub-Trees zu deaktivieren, erlauben unsicheren Ports den Zugriff sowie das Sperren unsicherer Dateien (für bestimmte frühere NFS-Client-Implementierungen notwendig). Auf der `exports`-man-Seite finden Sie weitere Details über diese weniger verwendeten Optionen.

Es gibt verschiedene Möglichkeiten, festzulegen, dass Hosts ein bestimmtes exportiertes Dateisystem verwenden können:

- *single host* — Ein bestimmter Host, einschließlich des kompletten Domain-Names, des Hostnamens oder der IP-Adresse wird festgelegt.
- *wildcards* — Die Zeichen `*` oder `?` werden verwendet, um eine Gruppierung von FQDNs, IP-Adressen oder solchen Namen zu berücksichtigen, die mit einer bestimmten Buchstabenkette übereinstimmen.

  Seien Sie jedoch im Umgang mit Wildcards im Zusammenhang mit FQDNs vorsichtig, da sie eine große Genauigkeit verlangen. So erlaubt die Verwendung von `*.example.com` als Wildcard zum Beispiel sales.example.com den Zugriff auf das exportierte Dateisystem, aber nicht bob.sales.example.com. Um beide Möglichkeiten zu erfassen wie auch sam.corp.example.com, muss die Option wie folgt aussehen: `*.example.com *.*.example.com`.
- *IP networks* — Erlaubt das Matching von Hosts auf der Basis ihrer IP-Adressen in einem großen Netzwerk. `192.168.0.0/28` läßt zum Beispiel die ersten 16 IP-Adressen von 192.168.0.0 bis 192.168.0.15 zu, um auf das exoprtierte Dateisystem zuzugreifen, aber nicht 192.168.0.16 und höher.
- *netgroups* — Lässt einen NIS-Netgroup-Namen zu, der wie folgt geschrieben wird: `@`*<Gruppenname>*. Dadurch übernimmt der NIS-Server die Kontrolle für den Zugriff auf diese exportierten Dateisysteme, und Benutzer können ohne Auswirkung auf `/etc/exports` zu einer NFS- Gruppe hinzugefügt oder aus einer solchen entfernt werden.

Warnung

Es ist sehr wichtig, wie die Datei `/etc/exports` formatiert ist, besonders im Bezug auf Leerzeichen. Denken Sie daran, exportierte Dateisystem immer getrennt von Hosts aufzuführen und Hosts durch Leerzeichen voneinander trennen. Es sollten jedoch keine weiteren Leerzeichen in der Datei sein, es sei denn, sie werden in Kommentarzeilen verwendet.

So bedeuten zum Beispiel die folgenden beiden Zeilen nicht das gleiche:

```
/home bob.example.com(rw)
/home bob.example.com (rw)
```

Die erste Zeile erlaubt nur Benutzern von `bob.example.com` den Zugriff im Read-Write-Modus auf das Verzeichnis `/home`. Die zweite Zeile erlaubt Benutzern von `bob.example.com`, das Verzeichnis im schreibgeschützten Modus zu mounten (der Standard), alle anderen können es im Read-Write-Modus mounten.

9.3. NFS-Client-Konfigurationsdateien

Jedes NFS-Share, das von einem Server ermöglicht wird, kann auf verschiedene Weise gemountet werden. Das Share kann natürlich auch manuell, mit dem Befehl `mount`, gemountet werden, um das exportierte Dateisystem an einem bestimmten Mount-Punkt zu erhalten. Dazu ist es jedoch erforderlich, dass der Root bei jedem Neustart den Befehl `mount` eingeben muß. Zwei Methoden, NFS-Mounts zu konfigurieren, sind das Modifizieren von `/etc/fstab` oder das Verwenden des `autofs` -Dienstes.

9.3.1. `/etc/fstab`

Das Einfügen einer korrekt formatierten Zeile in die Datei `/etc/fstab` hat den gleichen Effekt, wie das manuelle Mounten des exportierten Dateisystems. Die `/etc/fstab`-Datei wird während des Systemstarts von dem Skript `/etc/rc.d/init.d/netfs` gelesen, und die darin enthaltenen NFS-Shares werden gemountet.

Zum Beispiel sieht die Zeile `/etc/fstab` zum Mounten eines NFS-Exports wie folgt aus:

`<server>:</path/of/dir> </local/mnt/point> nfs <options> 0 0`

<Server-Host> bezieht sich auf den Hostnamen, die IP-Adresse oder den kompletten Domain-Name des Servers, der das Dateisystem exportiert.

</Pfad/zum/gemeinsam genutzten/Verzeichnis> gibt dem Server an, was gemountet werden soll.

</lokaler/Mount-Punkt> legt fest, wo das exportierte Verzeichnis im lokalen Dateisystem gemountet werden soll. Dieser Mount-Punkt muss vorhanden sein, bevor `/etc/fstab` gelesen wird oder das Mounten fehlschlägt.

Die Option `nfs` gibt den Typ des gemounteten Dateisystems an.

Der *<Optionen>*- Bereich gibt die Mount-Optionen für das Dateisystem an. Wenn zum Beispiel `rw,suid` angegeben wird, wird das exportierte Dateisystem im Read-Write-Modus gemountet und die Benutzer- sowie die Gruppen-ID von dem verwendeten Server eingestellt. Beachten Sie, dass keine Klammern verwendet werden. Weitere Mount-Optionen finden Sie unter Abschnitt 9.3.3.

9.3.2. `autofs`

Ein Nachteil bei der Verwendung von `/etc/fstab` ist, dass ungeachtet dessen, wie wenig Sie dieses gemountete Dateisystem verwenden, Ihr System Ressourcen zur Verfügung stellen muß, damit der Mount an dieser Stelle verbleibt. Bei einem oder zwei Mounts ist das kein Problem, wenn Ihr System jedoch zur gleichen Zeit Mounts von Dutzenden Systemen warten muß, kann die Leistungsfähigkeit des Systems darunter leiden. Eine Alternative zu `/etc/fstab` ist die Verwendung des Kernel-basierten Dienstprogramms `automount`, das NFS-Dateisysteme automatisch mountet und unmountet und dabei Ressourcen schont.

Das `autofs` Skript, in `/etc/rc.d/init.d/`, wird mithilfe der primären Konfigurationsdatei `/etc/auto.master` zur Kontrolle von `automount` verwendet. Da `automount` über die Befehlszeile festgelegt werden kann, ist es einfacher, die Mount-Punkte, Hostnamen, exportierte

Verzeichnisse und Optionen in einer Reihe von Dateien festzulegen als all diese Angaben von Hand einzugeben. Wenn `autofs` als Dienst ausgeführt wird, der auf bestimmten Runlevel starten und stoppen kann, können die Mount-Konfigurationen in den verschiedenen Dateien automatisch implementiert werden.

Die Konfigurationsdateien `autofs` sind in einem übergeordneten-untergeordneten Verhältnis angeordnet. Die wichtigste Konfigurationsdatei (`/etc/auto.master`) verweist auf Mount-Punkte in Ihrem System, die mit einem bestimmten *Zuordnungstyp* verlinkt sind, die z.B andere Konfigurationsdateien, Programme, NIS-Maps oder weniger bekannte Methoden zum Mounten sind. Die Datei `auto.master` enthält Zeilen, die auf diese Mount-Punkte verweisen und wie folgt aussehen:

```
<mount-point>    <map-type>
```

Das <*Mount-Punkt*> Element in dieser Zeile zeigt an, wo das Gerät oder das exportierte Dateisystem in Ihrem lokalen Dateisystem gemountet werden soll. <*Zuordnungstyp*> bezieht sich auf die Art, wie der Mount-Punkt gemountet wird. Üblicherweise wird zum automatischen Mounten von NFS-Exporten eine Datei als Zuordnungstyp für einen bestimmten Mount-Punkt verwendet. Die Zuordnungsdatei wird normalerweise wie folgt bezeichnet: `auto.`<*Mount-Punkt*>, wobei <*Mount-Punkt*> der in `auto.master` bezeichnete Mount-Punkt ist, der folgende Zeilen enthält:

```
<directory>  <mount-options>  <host>:<exported-file-system>
```

<*Verzeichnis*> bezieht sich auf das Verzeichnis im Mount-Punkt, wo das exportierte Dateisystem gemountet werden soll. In <*Host*>: <*exportiertes-Dateisystem*> wird der Standardbefehl `mount`, der Host, der das Dateisystem exportiert sowie das exportierte Dateisystem eingegeben. Zum Festlegen bestimmter Optionen, die beim Mounten des exportierten Dateisystems verwendet werden, plazieren Sie diese Optionen, durch Komma voneinander getrennt, in den Teil <*Mount-Optionen*>. Für NFS-Mounts, die den Befehl `autofs` verwenden, sollten Sie die Option `-fstype=nfs` im Teil <*Mount-Optionen*> angeben.

Da die `autofs`-Konfigurationsdateien für eine Anzahl verschiedener Mounts und viele Arten von Geräten und Dateisystemen verwendet werden können, sind sie für die Erstellung von NFS-Mount sehr hilfreich. Einige Organisationen speichern zum Beispiel das Benutzerverzeichnis `/home/` mithilfe eines NFS-Shares auf einem zentralen Server. Anschließend wird die Datei `auto.master` auf jeder Workstation konfiguriert, um auf eine `auto.home`-Datei zu verweisen, die genaue Angaben enthalten, wie das Verzeichnis `/home/` via NFS zu mounten ist. Der Benutzer erhält Zugriff auf persönliche Daten und Konfigurationsdateien im Verzeichnis `/home/`, indem er sich irgendwo im internen Netzwerk anmeldet. In diesem Fall würde die Datei `auto.master` wie folgt aussehen:

```
/home   /etc/auto.home
```

Der `/home/`-Mount-Punkt wird auf dem lokalen System eingestellt und mit der Datei `/etc/auto.home` konfiguriert:

```
*  -fstype=nfs,soft,intr,rsize=8192,wsize=8192,nosuid  server.example.com:/home
```

Diese Zeile gibt an, dass jeder Versuch eines Benutzers, im lokalen `/home/`-Verzeichnis (aufgrund des Sternchens) auf irgendein Verzeichnis zuzugreifen, einen NFS-Mount auf dem server.example.com-System innerhalb des exportierten Dateisystems zur Folge hat. Die Mount-Optionen geben an, dass bei jedem NFS-Mount des `/home/` -Verzeichnisses bestimmte Einstellungen verwendet werden. Weitere Informationen über Mount-Optionen, einschließlich der in diesem Beispiel verwendeten, finden Sie unter Abschnitt 9.3.3.

9.3.3. Allgemeine NFS-Mount-Optionen

Neben dem Mounten eines Dateisystems auf einem Remote-Host via NFS, können eine Anzahl verschiedener Optionen zum Zeitpunkt des Mountens festgelegt werden. Diese Optionen können ge-

meinsam mit den manuellen `mount`-Befehlen, `/etc/fstab`- Einstellungen, `autofs` und anderen Mount-Methoden verwendet werden.

Im Folgenden sind die bekanntesten Optionen für NFS-Mounts aufgeführt:

- `hard` oder `soft` — Legt fest, ob das Programm, das über eine NFS-Verbindung eine Datei verwendet, anhalten und auf den Server warten soll (`hard`), bis dieser wieder online ist, wenn der Host, der das exportierte Dateisystem liefert, nicht zur Verfügung steht oder einen Fehler meldet (`soft`).

  Wenn Sie `hard` festlegen, können Sie den Prozess des Wartens auf eine NFS-Verbindung nicht unterbrechen, es sei denn, Sie haben ebenfalls die Option `intr` festgelegt.

  Wenn Sie die Option `soft` bestimmen, können Sie eine weitere `timeo=`<*Wert*> Option einstellen, wobei <*Wert*> die Zeit (in Sekunden) festlegt, die vergeht, bevor ein Fehler gemeldet wird.
- `intr` — Ermöglicht, dass die NFS-Anfragen unterbrochen werden können, wenn der Server ausfällt oder nicht nicht erreicht werden kann.
- `nolock` — Wird unter Umständen für die Verbindung zu einem alten NFS-Server benötigt. Zum Sperren verwenden Sie die Option `lock` option.
- `noexec` — Verhindert das Ausführen von Binärdateien auf dem gemounteten Dateisystem. Diese Option ist hilfreich, wenn Ihr System ein Nicht-Linux Dateisystem über NFS mountet, welches inkompatible Binärdateien enthält.
- `nosuid` — Set-user-identifier oder set-group- identifier-Bits werden nicht wirksam.
- `rsize=8192` und `wsize=8192` — Können NFS-Kommunikationen zum Lesen (`rsize`) und Schreiben (`wsize`) beschleunigen, indem das Ausmaß des Datenblocks (in Bytes) vergrößert wird, der übertragen wird. Beim Ändern dieser Werte sollten Sie beachten, dass einige ältere Linux-Kernel und Netzwerkkarten eventuell mit einem größeren Datenblock nicht korrekt arbeiten könnten.
- `nfsvers=2` oder `nfsvers=3` — Legen fest, welche Version des NFS-Protokolls verwendet wird.

Auf der `mount`-man-Seite stehen noch weitere Optionen zur Verfügung, einschließlich Optionen die beim Mounten eines Nicht-NFS-Dateisystems verwendet werden.

9.4. NFS Sichern

Die Art, wie NFS bei der gemeinsamen Verwendung ganzer Dateisysteme mit einer großen Anzahl bekannter Hosts arbeitet, ist gut zu durchschauen. Viele Benutzer haben über einen NFS-Mount-Zugriff auf Dateien, wobei sie nicht wissen, dass sich diese Dateisysteme nicht auf ihrem lokalen System befinden. Aus diesem Vorteil können sich jedoch auch eine Reihe potenzieller Sicherheitsprobleme ergeben.

Folgende Punkte sollten beim Exportieren von NFS-Dateisystemen auf einem Server oder beim Mounten dieser Dateisysteme auf einem Client beachtet werden. Dadurch können die Sicherheitsrisiken von NFS verringert und Ihre Daten besser geschützt werden.

9.4.1. Host-Zugriff

NFS steuert anhand des Hosts, der die Anfrage zum Mounten stellt, wer ein exportiertes Dateisystem mounten kann (und nicht anhand des Benutzers, der das Dateisystem tatsächlich verwendet). Die Hosts müssen über die Berechtigung verfügen, exportierte Dateisysteme zu mounten. Für Benutzer ist keine Zugriffskontrolle möglich, mit Ausnahme der Berechtigungen für Dateien und Verzeichnisse. Mit anderen Worten, wenn Sie ein Dateisystem via NFS auf einen Remote- Host exportieren, haben Sie die Berechtigung zum Mounten dieses Dateisystems. Weiterhin erlauben Sie jedem Benutzer,

der Zugriff auf diesen Host hat, Ihr Dateisystem zu verwenden. Die dadurch entstehenden Risiken können kontrolliert werden, z.B. wenn nur im schreibgeschützten Modus gemountet werden kann oder Benutzer zu einer allgemeinen Benutzer- und Gruppen-ID zusammengefasst werden. Diese Lösungen können jedoch auch Auswirkungen auf die ursprünglich beabsichtige Art des Mountens haben.

Wenn eine nicht berechtigte Person die Kontrolle über den DNS-Server erlangt, der vom System zum Exportieren des NFS-Dateisystems verwendet wird, kann das System, dem ein bestimmter Hostname zugeordnet ist oder der komplette Domain-Name auf einen nicht autorisierten Computer hinweisen. An diesem Punkt *ist* dieser nicht autorisierte Computer das System, das das NFS-Share mounten kann, bis zu dem Zeitpunkt, an dem die Informationen über den Benutzernamen oder das Passwort zur zusätzlichen Sicherheit der NFS-Mounts geändert werden. Für NIS-Server bestehen die gleichen Risiken, wenn NIS-Netzgruppen verwendet werden, um bestimmten Hosts das Mounten eines NFS-Shares erlauben. Wenn in `/etc/exports` IP-Adressen verwendet werden, ist das Risiko geringer.

Wildcards sollten sparsam verwendet werden, wenn Zugriff auf ein NFS-Share gewährt wird, da sich der Anwendungsbereich von Wildcards auf Systeme erstrecken kann, von denen Sie nicht einmal wissen, dass es sie gibt.

Für mehr Informationen zur Sicherung von NFS, sehen Sie das Kapitel *Server Security* in der *Red Hat Linux Security Guide*.

9.4.2. Dateiberechtigungen

Wenn ein Remote-Host das NFS-Dateisystem im Read-Write-Modus gemountet hat, umfasst der Schutz der Share-Dateien auch deren Berechtigungen, die Benutzer- und die Gruppen-ID. Zwei Benutzer, die die gleiche Benutzer-ID zum Mounten des gleichen NFS-Dateisystems verwenden, können die Dateien gegenseitig modifizieren. Jeder, der als Root angemeldet ist, kann den Befehl `su -` verwenden, um über das NFS-Share Zugang zu bestimmten Dateien zu erlangen. Für mehr zu NFS und Userid-Konflikten, sehen Sie Kapitel *Managing Accounts and Groups* im *Red Hat Linux System Administration Primer*.

Standardmäßig wird beim Exportieren eines Dateisystems via NFS *Root-Squashing* verwendet. Dies setzt die Benutzer-ID von jedem, der auf die NFS-Share zugreift, auf dem jeweiligen lokalen Rechner auf einen Wert des "Nobody"-Accounts. Schalten Sie Root-Squashing niemals aus.

Wenn Sie eine NFS-Share als Nur-Lesen exportieren, verwenden Sie die Option `all_squash`, wodurch alle Benutzer, die auf Ihr exportiertes Dateisystem Zugriff haben, die Benutzer-ID "Nobody" erhalten.

9.5. Zusätzliche Ressourcen

Das Verwalten eines NFS-Servers kann eine Herausforderung sein. Es gibt viele Optionen, einschließlich solcher, die nicht in diesem Kapitel beschrieben wurden, um NFS-Dateisysteme zu exportieren oder zu mounten. Weitere Informationen darüber finden Sie in den angegebenen Quellen.

9.5.1. Installierte Dokumentation

- `/usr/share/doc/nfs-utils-<Versionsnummer>/` (*<version-number>* steht hierbei für die Versionsnummer des NFS-Pakets) — Beschreibt, wie NFS in Linux implementiert ist, gibt einen kurzen Überblick über die verschiedenen NFS-Konfigurationen einschließlich deren Auswirkungen auf die Übertragungen von Dateien.
- `man mount` — Enthält einen umfassenden Überblick über die Mount-Optionen für NFS Server- und Client-Konfigurationen.

- `man fstab` — Bietet Details über das Format der Datei `/etc/fstab`, die beim Booten des Systems Dateisysteme mountet.
- `man nfs` — Liefert Details über den Export von NFS-spezifischen Dateisystemen und Mount-Optionen.
- `man exports` — Zeigt allgemeine Optionen, die während des Exportierens von NFS-Dateisystemenin der Datei `/etc/exports` verwendet werden.

9.5.2. Zusätzliche Literatur

- *Managing NFS and NIS* von Hal Stern, Mike Eisler und Ricardo Labiaga; O'Reilly & Associates — Ein hervorragendes Referenzhandbuch für die vielen verschiedenen NFS-Exporte und die zur Verfügung stehenden Mount-Optionen.
- *NFS Illustrated* von Brent Callaghan; Addison-Wesley Publishing Company — Vergleicht NFS mit anderen Netzwerk-Dateisystemen und zeigt, wie die NFS- Kommunikation zustande kommt.

Kapitel 10.

Apache

Apache HTTP-Server ist ein von der Apache Software Foundation (http://www.apache.org) entwickelter Open Source Web-Server, welcher herausragende Stabilität bietet und kommerziellen Web-Servern in nichts nachsteht. Apache HTTP-Server Version 2.0, wie auch eine Reihe von Server-Modulen, welche zur Steigerung dessen Funktionalität entwickelt wurden, sind in Red Hat Linux inbegriffen.

Die mit Apache HTTP-Server installierte Standardkonfigurationsdatei ist in den meisten Situationen unverändert einsetzbar. Dieses Kapitel zeigt, wie die Apache HTTP-Server Konfigurationsdatei (`/etc/httpd/conf/httpd.conf`) für Situationen angepasst werden kann, die eine benutzerdefinierte Konfiguration erfordern, oder in denen eine Konfigurationsdatei vom älteren Apache HTTP-Server 1.3 Format konvertiert werden muss.

Warnung

Wenn Sie vorhaben, das graphische **HTTP Konfigurationstool** (`redhat-config-httpd`) zu verwenden, editieren Sie *nicht* die Apache HTTP-Server Konfigurationsdatei, da das **HTTP Konfigurationstool** diese Datei jedes Mal neu erstellt, wenn sie verwendet wird.

Weitere Informationen zum **HTTP Konfigurationstool** finden Sie im Kapitel *Apache HTTP-Server Konfiguration* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

10.1. Apache HTTP-Server 2.0

Es gibt einige wichtige Unterschiede zwischen Apache HTTP-Server Version 2.0 und Version 1.3 (mit Red Hat Linux 7.3 und früher ausgeliefert). Dieser Abschnitt gibt einen Überblick über einige der neuen Merkmale von Apache HTTP-Server 2.0 und weist auf wichtige Änderungen hin. Möchten Sie eine Konfigurationsdatei der Version 1.3. in das neue Format migrieren, sehen Sie Abschnitt 10.2.

10.1.1. Merkmale von Apache HTTP-Server 2.0

Die Einführung von Apache HTTP-Server 2.0 bringt eine Reihe neuer Merkmale mit sich. Einige davon sind:

- *Neue Apache API* — Eine Reihe neuer, verbesserter Application Programming Interfaces (APIs) für Module.

  

  Wichtig

  Für Apache HTTP-Server 1.3 erstellte Module funktionieren nicht, wenn diese nicht auf die neue API angepasst wurden. Wenn Sie sich nicht sicher sind, ob ein bestimmtes Modul angepasst wurde oder nicht, wenden Sie sich an die für die Paket-Pflege zuständige Stelle *bevor* Sie aktualisieren.

- *Filtering* — Module sind in der Lage, Inhalte zu filtern. Weitere Informationen dazu finden Sie unter Abschnitt 10.2.4.
- *IPv6 Support* — IP-Adressfunktionen der nächsten Generation werden unterstützt.

- *Vereinfachte Anweisungen* — Eine Reihe verwirrender Anweisungen wurden entfernt und andere vereinfacht. Informationen zu speziellen Anweisungen finden Sie unter Abschnitt 10.5.
- *Mehrsprachige Fehlermeldungen* — Bei der Verwendung von *Server Side Include* (*SSI*) Dokumenten, können benutzerdefinierbare Seiten zu Fehlermeldungen in mehreren Sprachen verschickt werden.
- *Multiprotocol Support* — Mehrere Protokolle werden unterstützt.

Eine vollständige Liste der Änderungen finden Sie online unter http://httpd.apache.org/docs-2.0/.

10.1.2. Paketänderungen bei Apache HTTP-Server 2.0

Mit Red Hat Linux 8.0 beginnend wurden die Apache HTTP-Server-Pakete umbenannt. Außerdem wurden einige verwandte Pakete umbenannt, verworfen oder in andere Pakete aufgenommen.

Es folgt eine Liste der Paketänderungen:

- Die Pakete `apache`, `apache-devel` und `apache-manual` wurden in `httpd`, `httpd-devel` und `httpd-manual` umbenannt.
- Das Paket `mod_dav` wurde in `httpd` integriert.
- Die Pakete `mod_put` und `mod_roaming` wurden entfernt, da deren Funktionalität in `mod_dav` enthalten ist.
- Die Pakete `mod_auth_any` und `mod_bandwidth` wurden entfernt.
- Die Versionsnummer für das Paket `mod_ssl` wurde jetzt mit dem Paket `httpd` in Einklang gebracht. Dies bedeutet, dass das Paket `mod_ssl` für Apache HTTP-Server 2.0 eine *niedrigere* Versionsnummer hat als das Paket `mod_ssl` für Apache HTTP-Server 1.3.

10.1.3. Dateisystemänderungen bei Apache HTTP-Server 2.0

Bei der Aktualisierung auf Apache HTTP-Server 2.0 ergeben sich folgende Änderungen am Layout des Dateisystems:

- *Ein neues Konfigurationsverzeichnis `/etc/httpd/conf.d/` wurde hinzugefügt.* — Dieses neue Verzeichnis wird zur Hinterlegung von Konfigurationsdateien für Module in Einzelpakete verwendet wie `mod_ssl`, `mod_perl` und `php`. Der Server wird angewiesen, anhand der Anweisung `Include conf.d/*.conf` in der Apache HTTP-Server Konfigurationsdatei `/etc/httpd/conf/httpd.conf` Konfigurationsdateien aus diesem Speicherplatz zu laden.

  
  Wichtig

  Es ist sehr wichtig, dass diese Zeile beim Migrieren einer bestehenden Konfiguration eingefügt wird.

- *Die Programme `ab` und `logresolve` wurden verschoben.* — Diese Dienstprogramme wurden vom Verzeichnis `/usr/sbin/` in das Verzeichnis `/usr/bin/` umgelagert. Dies hat zur Folge, dass Skripts mit absoluten Pfaden für diese Binärdateien scheitern.
- *Der Befehl `dbmmanage` wurde ersetzt.* — Der Befehl `dbmmanage` wurde durch `htdbm` ersetzt. Weitere Informationen erhalten Sie unter Abschnitt 10.2.4.4.
- *Die Konfigurationsdatei `logrotate` wurde umbenannt.* — Die Konfigurationsdatei `logrotate` wurde von `/etc/logrotate.d/apache` umbenannt in `/etc/logrotate.d/httpd`.

Der nächste Abschnitt zeigt, wie eine Apache HTTP-Server 1.3 Konfiguration in das neue Format 2.0 migriert werden kann.

10.2. Migrieren von Apache HTTP-Server 1.3 Konfigurationsdateien

Wurde Ihr Server von Red Hat Linux 7.3 oder früher aktualisiert, auf der Apache HTTP-Server bereits installiert war, dann wird die neue Stock-Konfigurationsdatei für das Apache HTTP-Server 2.0-Paket als `/etc/httpd/conf/httpd.conf.rpmnew` installiert und Ihre Originalversion 1.3 `httpd.conf` beibehalten. Es liegt natürlich ganz bei Ihnen, ob Sie die neue Konfigurationsdatei verwenden möchten und Ihre alten Einstellungen dorthin migrieren oder die vorhandene Datei als Basis verwenden und sie entsprechend anpassen; einige Bereiche der Datei haben sich jedoch mehr als andere verändert, deshalb ist ein gemischtes Vorgehen normalerweise die beste Lösung. Die Stock-Konfigurationsdateien sowohl für Version 1.3 als auch für Version 2.0 werden in drei Abschnitte unterteilt. Ziel dieses Leitfadens ist es, den hoffentlich einfachsten Weg aufzuzeigen.

Handelt es sich bei `/etc/httpd/conf/httpd.conf` um eine modifizierte Version der Standard Red Hat Linux Version und Sie haben eine Kopie des Originals gespeichert, dann ist es vielleicht am einfachsten, wenn Sie den Befehl `diff` aufrufen, wie in folgendem Beispiel gezeigt:

```
diff -u httpd.conf.orig httpd.conf | less
```

Dieser Befehl hebt die von Ihnen durchgeführten Änderungen hervor. Besitzen Sie keine Kopie der Originaldatei, entnehmen Sie sie anhand der Befehle `rpm2cpio` und `cpio` einem RPM-Paket, wie in folgendem Beispiel gezeigt:

```
rpm2cpio apache-<version-number>.i386.rpm | cpio -i --make
```

<version-number> ist hierbei mit der Versionsnummer des `apache` Pakets zu ersetzen.

Es ist hilfreich zu wissen, dass Apache HTTP-Server über einen Testmodus zur Prüfung Ihrer Konfigurations auf Fehler verfügt. Der Zugriff erfolgt über folgenden Befehl:

```
apachectl configtest
```

10.2.1. Konfiguration der globalen Umgebung

Der Abschnitt zur globalen Umgebung der Konfigurationsdatei enthält Anweisungen, die sich insgesamt auf die Funktionsweise von Apache HTTP-Server auswirken, wie die Anzahl konkurrierender Anfragen, die abgefertigt werden und die Speicherplätze der verschiedenen verwendeten Dateien. Bei diesem Abschnitt ist im Vergleich zu den anderen eine große Anzahl an Änderungen notwendig. Es empfiehlt sich deshalb, dass dieser Abschnitt seine Basis in der Apache HTTP-Server 2.0 Konfigurationsdatei hat und Sie Ihre alten Einstellungen dorthin migrieren.

10.2.1.1. Auswahl der zu verknüpfenden Schnittstellen und Ports

Die Anweisungen `BindAddress` und `Port` existieren nicht mehr; ihre Funktionen wurde durch eine flexiblere `Listen` Anweisung ersetzt.

Wenn Sie in Ihrer 1.3. Version die Konfigurationsdatei auf `Port 80` gesetzt haben, sollten Sie diese auf `Listen 80` umändern. Hatten Sie `Port` auf einen Wert gesetzt *der ungleich 80 ist*, dann müssen Sie auch die Port-Nummer an den Inhalt Ihrer `ServerName` Anweisung anhängen.

Folgendes ist ein Beispiel einer Apache HTTP-Server 1.3 Anweisung:

```
Port 123
ServerName www.example.com
```

Verwenden Sie folgende Struktur, um diese Einstellung nach Apache HTTP-Server 2.0 zu migrieren:

```
Listen 123
ServerName www.example.com:123
```

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- `http://httpd.apache.org/docs-2.0/mod/mpm_common.html#listen`
- `http://httpd.apache.org/docs-2.0/mod/core.html#servername`

10.2.1.2. Server-Pool Größeneinstellung

Die Verantwortung der Handhabung von Annahmen und Versenden von Kind-Prozessen wurde in Apache HTTP-Server 2.0 in einer Modulgruppe mit dem Namen *Multi-Processing Modules* (*MPMs*) zusammengefasst. Im Gegensatz zu anderen Modulen kann nur ein Modul der MPM-Gruppe von Apache HTTP-Server geladen werden, da ein MPM-Modul für grundlegende Anfragebearbeitung und Anfrageverteilung zuständig ist. Drei MPM-Module werden mit der Version 2.0 ausgeliefert: `prefork`, `worker` und `perchild`.

Das Originalverhalten von Apache HTTP-Server 1.3 wurde auf das `prefork` MPM übertragen. Derzeit ist nur das `prefork` MPM auf Red Hat Linux verfügbar, obwohl weitere MPSs für die Zukunft vorgesehen sind.

Das `prefork` MPM akzeptiert die gleichen Anweisungen wie Apache HTTP-Server 1.3. Folgende Anweisungen können direkt migriert werden:

- `StartServers`
- `MinSpareServers`
- `MaxSpareServers`
- `MaxClients`
- `MaxRequestsPerChild`

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mpm.html

10.2.1.3. Support für Dynamic Shared Objects (DSO)

Viele Änderungen sind hier notwendig und es empfiehlt sich für jeden, der versucht, eine Apache HTTP-Server 1.3-Konfiguration an eine Apache HTTP-Server 2.0-Konfiguration anzupassen (im Gegensatz zur Migration Ihrer Änderungen in die 2.0-Konfiguration), diesen Abschnitt aus der Stock-Red Hat Linux-Apache HTTP-Server 2.0-Konfigurationsdatei zu kopieren.

Diejenigen, die diesen Abschnitt nicht kopieren wollen, sollten Folgendes beachten:

- Die `AddModule` und `ClearModuleList`-Anweisungen gibt es nicht länger. Diese Anweisungen wurden verwendet, um sicherzustellen, dass Module in der richtigen Reihenfolge aktiviert wurden. Die Apache HTTP-Server 2.0 API erlaubt Modulen die Reihenfolge zu bestimmen, was diese beiden Anweisungen überflüssig macht.
- Die Reihenfolge der `LoadModule` Zeilen ist nicht mehr von Bedeutung.

- Viele Module wurden hinzugefügt, entfernt, umbenannt, aufgeteilt oder zusammengefasst.
- `LoadModule` Zeilen für Module, die in ihren eigenen RPMs (`mod_ssl`, `php`, `mod_perl` und ähnliche) verpackt sind, sind nicht mehr notwendig, da sie sich in der entsprechenden Datei im `/etc/httpd/conf.d/` Verzeichnis befinden.
- Die verschiedenen `HAVE_XXX` Definitionen werden nicht mehr festgelegt.

Wichtig

Sollten Sie versuchen, Ihre Originaldatei zu ändern, beachten Sie bitte, dass es äußerst wichtig ist, dass Ihre `httpd.conf` folgende Anweisung enthält:

```
Include conf.d/*.conf
```

Das Weglassen dieser Anweisung hat zur Folge, dass alle Module scheitern, die in ihren eigenen RPMs (wie `mod_perl`, `php` und `mod_ssl`) verpackt sind.

10.2.1.4. Sonstige Änderungen der globalen Umgebung

Folgende Anweisungen wurden aus der Apache HTTP-Server 2.0 Konfiguration entfernt:

- *`ServerType`* — Der Apache HTTP-Server kann nur als `ServerType standalone` gestartet werden, womit diese Anweisung keine Bedeutung mehr hat.
- *`AccessConfig`* und *`ResourceConfig`* — Diese Anweisungen wurden herausgenommen, da sie die gleiche Funktion wie die `Include` Anweisung haben. Haben Sie `AccessConfig` und `ResourceConfig` Anweisungen gesetzt, dann müssen sie diese durch `Include` Anweisungen ersetzen.

  Um sicherzustellen, dass die Dateien in der Reihenfolge gelesen werden, die von den älteren Anweisungen vorgesehen war, sollten Sie `Include` Anweisungen an das Ende von `httpd.conf` setzen. Dabei sollte die Anweisung, die `ResourceConfig` entspricht, vor der Anweisung liegen, die `AccessConfig` entspricht. Haben Sie mit Standardwerten gearbeitet, müssen Sie diese ausdrücklich als `conf/srm.conf` und `conf/access.conf` mit aufnehmen.

10.2.2. Hauptserver-Konfiguration

Der Abschnitt zur Hauptserver-Konfiguration der Konfigurationsdatei richtet den Hauptserver ein, der auf alle Anfragen antwortet, die nicht über eine <`VirtualHost`> Definition gehandhabt werden. Die Werte hier liefern auch Standardwerte für alle definierten <`VirtualHost`> Container.

In den Anweisungen dieses Abschnitts gibt es kaum Unterschiede zwischen Apache HTTP-Server 1.3 und Version 2.0. Wenn Ihre Hauptserver-Konfiguration sehr stark benutzerdefiniert ist, ist es vielleicht einfacher für Sie, wenn Sie Ihre bereits existierende Konfiguration an Apache HTTP-Server 2.0 anpassen. Benutzer mit weniger benutzerdefinierten Hauptserver-Abschnitten sollten ihre Änderungen in die Stock-Apache HTTP-Server 2.0 Konfiguration migrieren.

10.2.2.1. UserDir-Abbildung

Die Anweisung `UserDir` wird verwendet, um URLs wie `http://example.com/~bob/` in ein Unterverzeichnis innerhalb des Home-Verzeichnisses des Benutzers `bob` wie `/home/bob/public_html` abzubilden. Als Nebenwirkung erlaubt es diese Eigenschaft einem potentiellen Unbefugten festzustellen, ob ein bestimmter Benutzername im System vorhanden ist.

Aus diesem Grund ist diese Anweisung in der Standardkonfiguration von Apache HTTP-Server 2.0 deaktiviert.

Aktivieren Sie die `UserDir` Abbildung durch Umändern der sich in `httpd.conf` befindlichen Anweisung von:

```
UserDir disable
```

in folgende:

```
UserDir public_html
```

Weitere Informationen zu diesem Thema finden Sie in der Dokumentation auf der Apache Software Foundation Website, unter http://httpd.apache.org/docs-2.0/mod/mod_userdir.html#userdir.

10.2.2.2. Logging

Folgende Log-Anweisungen wurden entfernt:

- `AgentLog`
- `RefererLog`
- `RefererIgnore`

Agent- und Referrer-Logs sind über `CustomLog` und `LogFormat` Anweisungen immer noch verfügbar.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog
- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#logformat

10.2.2.3. Index-Erstellung für Verzeichnisse

Die veraltete Anweisung `FancyIndexing` wurde entfernt. Die gleiche Funktionalität ist über `FancyIndexing` *Option* in der Anweisung `IndexOptions` verfügbar.

Die neue Option `VersionSort` für die `IndexOptions` Anweisung führt dazu, dass Dateien mit Versionsnummern auf natürliche Weise sortiert werden, so dass `httpd-2.0.6.tar` in einer Verzeichnis-Indexseite vor `httpd-2.0.36.tar` erscheinen würde.

Die Standardwerte für die Anweisungen `ReadmeName` und `HeaderName` haben sich geändert, und zwar von `README` und `HEADER` in `README.html` und `HEADER.html`.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#indexoptions
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#readmename
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#headername

10.2.2.4. Inhaltsverhandlung

Die Anweisung `CacheNegotiatedDocs` kann jetzt die Argumente `on` oder `off` haben. Existierende Fälle von `CacheNegotiatedDocs` sollten durch `CacheNegotiatedDocs on` ersetzt werden.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_negotiation.html#cachenegotiateddocs

10.2.2.5. Fehlerdokumente

Um eine hart-kodierte Meldung mit der `ErrorDocument` Anweisung zu verwenden, sollte die Meldung von einem Paar doppelter Anführungszeichen ["] umschlossen sein, anstatt dass nur ein doppeltes Anführungszeichen der Meldung vorangestellt werden, wie in Apache HTTP-Server 1.3. verlangt.

Verwenden Sie folgende Struktur um eine `ErrorDocument` Einstellung nach Apache HTTP-Server 2.0 zu migrieren:

```
ErrorDocument 404 "The document was not found"
```

Beachten Sie, dass in der o.g. Beispiel-Anweisung `ErrorDocument` doppelte Anführungszeichen angehängt wurden.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/core.html#errordocument

10.2.3. Konfiguration des virtuellen Host

Der Inhalt aller `<VirtualHost>` Sektionen sollte auf die gleiche Weise wie der Hauptserver-Abschnitt migriert werden, wie in Abschnitt 10.2.2 beschrieben.

Wichtig

Bitte beachten Sie, dass die SSL/TLS Konfiguration des virtuellen Host aus der Hauptserver-Konfigurationsdatei genommen und in `/etc/httpd/conf.d/ssl.conf` verschoben wurde.

Weitere Informationen zu diesem Thema finden Sie im Kapitel *Konfiguration von Apache HTTP Secure Server* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration* und in der Online-Dokumentation unter:

- http://httpd.apache.org/docs-2.0/vhosts/

10.2.4. Module und Apache HTTP-Server 2.0

In Apache HTTP-Server 2.0 wurde das Modulsystem so geändert, dass Module auf neue und interessante Weise miteinander verknüpft und kombiniert werden können. *Common Gateway Interface* (*CGI*) Skripte sind zum Beispiel in der Lage, Server-parsed HTML-Dokumente zu erzeugen, die dann

von mod_include verarbeitet werden können. Dies eröffnet eine enorme Anzahl von Möglichkeiten in Bezug darauf, wie Module zum Erreichen eines bestimmten Ziels kombiniert werden können.

Das funktioniert so, dass jede Anfrage direkt von einem *handler* Modul bedient wird, gefolgt von null oder mehr *filter* Modulen.

In Apache HTTP-Server 1.3 zum Beispiel würde ein PHP-Skript ganz von einem PHP-Modul gehandhabt werden. In Apache HTTP-Server 2.0 wird die Anfrage zunächst vom Kernmodul — das statische Dateien bedient — *gehandhabt*, und wird dann vom PHP-Modul *gefiltert*.

Die genaue Verwendung und alle anderen diesbezüglichen neuen Eigenschaften von Apache HTTP-Server 2.0 würden den Rahmen dieses Dokumentes sprengen; die Änderung hat jedoch Auswirkungen, wenn Sie PATH_INFO verwendet haben. Darin enthalten sind Pfad-Informationen, die dem echten Dateinamen angehängt werden, in einem Dokument, das von einem jetzt als Filter implementierten Modul gehandhabt wird. Das Kernmodul, das die Anfrage anfangs gehandhabt hat, versteht PATH_INFO standardmäßig nicht und wird 404 Not Found Fehler ausgeben bei Anfragen, die derartige Informationen enthalten. Sie können die Anweisung AcceptPathInfo verwenden, um das Kernmodul dazu zu zwingen, Anfragen mit PATH_INFO zu akzeptieren.

Folgend ist ein Beispiel dieser Anweisung:

```
AcceptPathInfo on
```

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/core.html#acceptpathinfo
- http://httpd.apache.org/docs-2.0/handler.html
- http://httpd.apache.org/docs-2.0/filter.html

10.2.4.1. Das Modul mod_ssl

Die Konfiguration für mod_ssl wurde von httpd.conf in die Datei /etc/httpd/conf.d/ssl.conf verschoben. Damit diese Datei geladen wird und dass folglich mod_ssl funktioniert, müssen Sie die Anweisung Include conf.d/*.conf wie in Abschnitt 10.2.1.3 beschrieben in Ihrer Datei httpd.conf haben.

ServerName Anweisungen in virtuellen Hosts von SSL müssen die Port-Nummer ausdrücklich angeben.

Folgendes ist ein Beispiel einer Apache HTTP-Server 1.3 Anweisung:

```
<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.example.name
    ...
</VirtualHost>
```

Verwenden Sie folgende Struktur, um diese Einstellung nach Apache HTTP-Server 2.0 zu migrieren:

```
<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.host.name:443
    ...
</VirtualHost>
```

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html
- http://httpd.apache.org/docs-2.0/vhosts/

10.2.4.2. Das Modul `mod_proxy`

Zugriffskontrollbefehle für den Proxy befinden sich jetzt in einem `<Proxy>` Block anstatt in einem `<Directory proxy:>`.

Die Cache-Funktionalität der alten Datei `mod_proxy` wurde in folgende drei Module aufgeteilt:

- `mod_cache`
- `mod_disk_cache`
- `mod_file_cache`

Diese verwenden normalerweise die gleichen oder ähnliche Anweisungen wie die älteren Versionen des `mod_proxy` Moduls.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_proxy.html

10.2.4.3. Das Modul `mod_include`

Das Modul `mod_include` ist jetzt als Filter implementiert und wird deshalb anders aktiviert. Weitere Informationen zu Filtern finden Sie in Abschnitt 10.2.4.

Folgendes ist ein Beispiel einer Apache HTTP-Server 1.3 Anweisung:

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Verwenden Sie folgende Struktur, um diese Einstellung nach Apache HTTP-Server 2.0 zu migrieren:

```
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
```

Beachten Sie bitte, dass die Anweisung `Options +Includes` wie bisher für den `<Directory>` Container oder in einer `.htaccess`-Datei verlangt wird.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_include.html

10.2.4.4. Die Module `mod_auth_dbm` und `mod_auth_db`

Apache HTTP-Server 1.3 unterstützte zwei Authentifizierungsmodule, `mod_auth_db` und `mod_auth_dbm`, die jeweils Berkely-Datenbanken und DBM-Datenbanken verwendeten. Diese Module wurden in Apache HTTP-Server 2.0, in ein einziges Modul mit dem Namen `mod_auth_dbm` zusammengefasst, das auf mehrere verschiedene Datenbankformate zugreifen kann. Um von `mod_auth_db` aus Version 1.3 zu migrieren, müssen die Konfigurationsdateien angepasst werden, indem `AuthDBUserFile` und `AuthDBGroupFile` durch die entsprechenden aus `mod_auth_dbm` ersetzt werden: `AuthDBMUserFile` und `AuthDBMGroupFile`. Sie müssen außerdem die Anweisung `AuthDBMType DB` hinzufügen um den Typ der Datenbankdatei anzugeben, der verwendet wird.

Folgendes ist ein Beispiel für eine mod_auth_db Konfiguration in Apache HTTP-Server 1.3:

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBUserFile /var/www/authdb
  require valid-user
</Location>
```

Verwenden Sie folgende Struktur um diese Einstellung zu Apache HTTP-Server 2.0 zu migrieren:

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBMUserFile /var/www/authdb
  AuthDBMType DB
  require valid-user
</Location>
```

Bitte beachten Sie, dass die Anweisung AuthDBMUserFile auch in .htaccess Dateien verwendet werden kann.

Das dbmmanage Perl-Skript, das zur Bearbeitung von Benutzernamen- und Passwort-Datenbanken verwendet wurde, wurde in Apache HTTP-Server 2.0. durch htdbm ersetzt. Das Programm htdbm bietet gleichwertige Funktionalität und kann wie mod_auth_dbm mit einer Reihe von Datenbank-Formaten umgehen; die Option -T kann in der Befehlszeile zur Bestimmung des Formats verwendet werden.

Tabelle 10-1 zeigt, wie man von einer Datenbank im DBM-Format anhand von dbmmanage in das htdbm Format migrieren kann.

Aktion	dbmmanage Befehl (1.3)	Entsprechender htdbm Befehl (2.0)
Benutzer zu Datenbank hinzufügen (angegebenes Passwort verwenden)	`dbmmanage authdb add username password`	`htdbm -b -TDB authdb username password`
Benutzer zu Datenbank hinzufügen (fragt nach Passwort)	`dbmmanage authdb adduser username`	`htdbm -TDB authdb username`
Benutzer aus Datenbank entfernen	`dbmmanage authdb delete username`	`htdbm -x -TDB authdb username`
Benutzer in Datenbank auflisten	`dbmmanage authdb view`	`htdbm -l -TDB authdb`
Passwort prüfen	`dbmmanage authdb check username`	`htdbm -v -TDB authdb username`

Tabelle 10-1. Migrieren von dbmmanage nach htdbm

Die Optionen -m und -s funktionieren sowohl mit dbmmanage als auch mit htdbm und aktivieren damit jeweils die Verwendung von MD5-oder SHA1-Algorithmen zum Haschieren der Passwörter.

Wird mit htdbm eine neue Datenbank erzeugt, muss dies anhand der Option -c erfolgen.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_auth_dbm.html

10.2.4.5. Das Modul `mod_perl`

Die Konfiguration für `mod_perl` wurde von `httpd.conf` in die Datei `/etc/httpd/conf.d/perl.conf` verschoben. Damit diese Datei geladen wird und dass folglich `mod_perl` funktioniert, müssen Sie die Anweisung `Include conf.d/*.conf` wie in Abschnitt 10.2.1.3 beschrieben in Ihrer Datei `httpd.conf` haben.

Alle `Apache::` Einträge in `httpd.conf` müssen durch `ModPerl::` ersetzt werden. Außerdem hat sich die Art und Weise geändert, mit der Handler eingetragen werden.

Dies ist ein Beispiel für eine Apache HTTP-Server 1.3 `mod_perl` Konfiguration:

```
<Directory /var/www/perl>
    SetHandler perl-script
    PerlHandler Apache::Registry
    Options +ExecCGI
</Directory>
```

Dies entspricht `mod_perl` in Apache HTTP-Server 2.0:

```
<Directory /var/www/perl>
    SetHandler perl-script
    PerlModule ModPerl::Registry
    PerlHandler ModPerl::Registry::handler
    Options +ExecCGI
</Directory>
```

Die meisten Module für `mod_perl` 1.x dürften ohne Änderungen mit `mod_perl` 2.x funktionieren. XS-Module erfordern eine Neukompilierung und bedürfen eventuell geringerer Makefile-Änderungen.

10.2.4.6. Das Modul `mod_python`

Die Konfiguration für `mod_python` wurde von `httpd.conf` nach `/etc/httpd/conf.d/python.conf` verschoben. Damit diese Datei geladen wird und folglich dass `mod_python` funktioniert, müssen Sie die Anweisung `Include conf.d/*.conf` wie in Abschnitt 10.2.1.3 beschrieben in Ihrer Datei `httpd.conf` haben.

10.2.4.7. PHP

Die Konfiguration für PHP wurde von `httpd.conf` in die Datei `/etc/httpd/conf.d/php.conf` verschoben. Damit diese Datei geladen wird, müssen Sie die Anweisung `Include conf.d/*.conf` wie in Abschnitt 10.2.1.3 beschrieben in Ihrer Datei `httpd.conf` haben.

PHP ist jetzt als Filter implementiert und deshalb anders aktiviert werden. Weitere Informationen zu Filtern finden Sie unter Abschnitt 10.2.4.

In Apache HTTP-Server 1.3 wurde PHP anhand folgender Anweisungen implementiert:

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

Verwenden Sie dagegen in Apache HTTP-Server 2.0 folgende Anweisungen:

```
<Files *.php>
    SetOutputFilter PHP
```

```
    SetInputFilter PHP
</Files>
```

In PHP 4.2.0 und späteren Versionen haben sich die standardmäßigen vordefinierten Variablen, die im globalen Scope verfügbar waren, geändert. Individuelle Input- und Servervariablen werden nicht mehr standardmäßig direkt in das globale Scope gesetzt. Diese Änderung kann dazu führen, dass Skripts nicht mehr funktionieren. Sie können zum alten Verhalten zurückkehren, indem Sie in der Datei `/etc/php.ini` `register_globals` auf `On` setzen.

Weitere Informationen zu diesem Thema finden Sie im folgenden URL. Darin enthalten sind Einzelheiten zu den Änderungen im globalen Scope:

- http://www.php.net/release_4_1_0.php

10.3. Nach der Installation

Nach der Installation des `httpd`-Pakets finden Sie die Dokumentation zu Ihrem Apache HTTP-Server Server folgendermaßen: Installieren Sie das Paket `httpd-manual` und zeigen Sie mit einem Web-Browser auf http://localhost/manual/ oder Sie können die Apache Dokumentation im Web unter http://httpd.apache.org/docs-2.0/ einsehen.

Die Apache HTTP-Server-Dokumentation enthält Listen und komplette Beschreibungen aller Konfigurationsoptionen. Um Ihnen die Übersicht zu erleichtern, liefert dieses Kapitel kurze Beschreibungen der von Apache HTTP-Server 2.0 verwendeten Konfigurationsanweisungen.

Diese Apache HTTP-Server-Version kann als sicherer Web-Server mit der starken SSL- Verschlüsselung durch die Pakete `mod_ssl` und `openssl` eingerichtet werden. Beim Lesen der Konfigurationsdateien Ihres Web-Servers stellen Sie sicher, dass diese sowohl den Web-Server ohne, als auch mit Verschlüsselung enthält. Der Web-Server wird als virtueller Host ausgeführt, der in der Datei `/etc/httpd/conf.d/ssl.conf` konfiguriert wird. Weitere Informationen über virtuelle Hosts finden Sie unter Abschnitt 10.8. Weitere Informationen zum Secure Server Virtual Host finden Sie unter Abschnitt 10.8.1. Für weitere Informationen zum Einrichten eines Apache HTTP Secure Server sehen Sie das Kapitel *Konfiguration von Apache HTTP Secure Server* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

Anmerkung

Red Hat, Inc. liefert keine FrontPage-Erweiterungen mit aus, da die Lizenz von Microsoft™ deren Lieferung in einem Produkt eines Drittanbieters verbietet. Mehr über FrontPage-Erweiterungen erfahren Sie unter http://www.rtr.com/fpsupport/.

10.4. Starten und Anhalten von `httpd`

Die `httpd` RPM installiert das `/etc/rc.d/init.d/httpd` Skript, auf das Sie mittels des Befehls `/sbin/service` zugreifen können.

Geben Sie den folgenden Befehl als root ein, um den Server zu starten:

```
/sbin/service httpd start
```

Geben Sie den folgenden Befehl als root ein, um den Server anzuhalten:

```
/sbin/service httpd stop
```

Die Option `restart` ist ein abkürzender Befehl zum Anhalten und dann Neustarten von Apache HTTP-Server.

Geben Sie den folgenden Befehl als root ein, um den Server neu zu starten:

```
/sbin/service httpd restart
```

Anmerkung

Wenn Sie Apache HTTP-Server als Secure Server ausführen, werden Sie aufgefordert, bei jedem Verwenden der Option `start` oder `restart`, Ihr Passwort einzugeben.

Auch wenn Sie Änderungen in Ihrer Datei `httpd.conf` vorgenommen haben, ist es nicht nötig, dass Sie den Server anhalten und neu starten. Zu diesem Zweck können Sie die Option `reload` verwenden.

Um die Server-Konfigurationsdatei neu zu laden, geben Sie folgenden Befehl als root ein:

```
/sbin/service httpd reload
```

Anmerkung

Wenn Sie Apache HTTP-Server als Secure Server ausführen, brauchen Sie Ihr Passwort *nicht* anzugeben, wenn Sie die Option `reload` verwenden.

Standardmäßig wird der `httpd` Service beim Booten des Rechners *nicht* automatisch gestartet. Sie müssen den `httpd` Service konfigurieren, um beim Booten starten zu können und zwar anhand eines Initskript-Utilities wie `/sbin/chkconfig`, **/sbin/ntsysv** oder des **Services-Konfigurationstool** Programms. Im Kapitel *Zugriffskontrolle für Dienste* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration* finden Sie weitere Informationen zu diesen Tools.

Anmerkung

Wenn Sie Apache HTTP-Server als Secure Server ausführen, werden Sie nach dem Booten des Rechners nach dem Passwort des Secure Servers gefragt, es sei denn, Sie haben eine besondere Art von Server-Schlüsseldatei erstellt.

Informationen über das Einrichten eines Apache HTTP Secure Server finden Sie im Kapitel *Apache HTTP Secure Server Configuration* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

10.5. Konfigurationsanweisungen in `httpd.conf`

Die Apache HTTP-Server-Konfigurationsdatei ist `/etc/httpd/conf/httpd.conf`. Die Datei `httpd.conf` enthält ausführliche Kommentare und erklärt sich bis zu einem gewissen Grad selbst.

Die Standardkonfiguration Ihres Web-Servers ist für die meisten Situationen ausreichend, Sie sollten sich jedoch mit einigen der wichtigsten Konfigurationsoptionen vertraut machen.

Warnung

Mit der Release von Apache HTTP-Server 2.0 haben sich viele Konfigurationsoptionen geändert. Müssen Sie eine Konfigurationsdatei der Version 1.3 in das neue Format migrieren, studieren Sie Abschnitt 10.2.

10.5.1. Allgemeine Tipps zur Konfiguration

Wenn Sie Apache HTTP-Server konfigurieren müssen, ist lediglich die Datei `/etc/httpd/conf/httpd.conf` zu editieren und anschließend der `httpd`-Prozess neu zu laden oder anzuhalten und neu zu starten. Das Neuladen, Anhalten und Starten von Apache HTTP-Server wird in Abschnitt 10.4 besprochen.

Vor dem Editieren von `httpd.conf` sollten Sie zuerst eine Kopie dieser Datei erstellen. Falls Sie beim Editieren der Konfigurationsdatei einen Fehler machen, steht Ihnen auf diese Weise eine Sicherheitskopie zur Verfügung.

Falls Sie einen Fehler machen und Ihr Web-Server nicht richtig funktioniert, sollten Sie zuerst die Eingaben der gerade editierten Datei `httpd.conf` überprüfen. Stellen Sie sicher, dass diese keine Tippfehler enthält.

Als Nächstes sollten Sie einen Blick auf die Fehlerprotokolldatei Ihres Web-Servers, `/var/log/httpd/error_log`, werfen. 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`, welche allerdings nicht bis ins letzte Detail gehen. Weitere Informationen finden Sie in der Apache-Dokumentation im HTML-Format unter http://localhost/manual/ oder Online unter http://httpd.apache.org/docs-2.0/.

Weitere Informationen zu den `mod_ssl` Anweisungen erhalten Sie aus der Dokumentation im HTML-Format unter http://localhost/mod/mod_ssl.html oder Online unter http://httpd.apache.org/docs-2.0/mod/mod_ssl.html.

10.5.2. `ServerRoot`

`ServerRoot` ist das oberste Verzeichnis, indem sich die Server-Dateien befinden. Sowohl der Server mit Verschlüsselung (Secure Server) als auch der Server ohne Verschlüsselung sind auf die Verwendung von `"/etc/httpd"` als `ServerRoot` eingestellt.

10.5.3. `ScoreBoardFile`

Im `ScoreBoardFile` werden interne Serverprozessinformationen gespeichert, die für die Kommunikation zwischen dem Parent-Serverprozess und seinen Child-Prozessen verwendet werden. Red Hat Linux verwendet gemeinsamen Speicherplatz um `ScoreBoardFile` abzulegen, der Standard `/etc/httpd/logs/apache_runtime_status` wird nur als Fallback verwendet.

10.5.4. PidFile

PidFile gibt die Datei an, in welcher der Server seine Prozess-ID (PID) ablegt. Der Default ist hier /var/run/httpd.pid.

10.5.5. 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 is auf 300 Sekunden eingestellt, eine für die meisten Situationen geeignete Einstellung.

10.5.6. KeepAlive

Mit KeepAlive kann eingestellt werden, ob auf Ihrem Server mehr als eine Anfrage pro Verbindung zugelassen ist (in anderen Worten, werden wiederholte Verbindungen gesichert). KeepAlive kann verwendet werden, um zu verhindern, dass ein einzelner Client zu viele der Serverressourcen verbraucht.

Die Standardeinstellung für Keepalive ist off. Ist Keepalive auf on eingestellt und der Verkehr auf dem Server nimmt spürbar zu, kann der Server schnell die Höchstanzahl von untergeordneten Prozessen erreichen. In dieser Situation lässt die Leistung des Servers deutlich nach. Wenn Keepalive aktiviert ist, ist es ratsam, die Option KeepAliveTimeout niedrig einzustellen (siehe Abschnitt 10.5.8 für weitere Informationen zur KeepAliveTimeout Anweisung) und die Datei /var/log/httpd/error_log auf dem Server zu überwachen. Dieses Protokoll erstellt einen Bericht, wenn dem Server keine untergeordneten Prozesse zur Verfügung stehen.

10.5.7. MaxKeepAliveRequests

Diese Anweisung gibt an, wie viele Anforderungen pro wiederholter Verbindung maximal erlaubt sind. Das Apache Projekt empfiehlt einen hohen Wert. Dadurch wird die Leistung des Servers verbessert. Die Standardeinstellung für MaxKeepAliveRequests ist 100, eine für die meisten Situationen geeignete Einstellung.

10.5.8. KeepAliveTimeout

KeepAliveTimeout gibt in Sekunden an, wie lange der Server wartet, nachdem eine Anforderung bearbeitet wurde. Danach wird die Verbindung getrennt. Nach dem Empfang einer Anforderung gilt stattdessen die Anweisung Timeout. KeepAliveTimeout ist per Default auf 15 Sekunden eingestellt.

10.5.9. MinSpareServers und MaxSpareServers

Der Apache HTTP-Server-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.

10.5.10. 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.

10.5.11. MaxClients

MaxClients gibt eine Obergrenze für die Gesamtzahl von Serverprozessen bzw. Clients an, die gleichzeitig ausgeführt werden können. Der Hauptgrund für das Bestehen von MaxClients ist, dass damit verhindert werden soll, dass Ihr Betriebssystem durch einen überlasteten Apache HTTP-Server zum Absturz gebracht wird. Sie sollten MaxClients auf einer hohen Anzahl belassen; die Standardeinstellung des Servers ist 150. Es ist nicht empfohlen MaxClients auf einen Wert größer als 256 zu setzen.

10.5.12. MaxRequestsPerChild

MaxRequestsPerChild legt die Gesamtzahl der Anfragen fest, die jeder Kind-Server-Prozess benötigt, bevor der Kind-Prozess beendet wird. Der Hauptgrund für die Einstellung von MaxRequestsPerChild ist, dass lang andauernde, durch Prozesse verursachte Speicherprobleme vermieden werden sollen. Die Standardeinstellung für MaxRequestsPerChild für den Server ist 1000.

10.5.13. 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 /etc/httpd/conf.d/ssl.conf, die sämtliche Secure Servers definiert) auf Port 443 auf sichere Web-Kommunikation abhört.

Wenn Sie Apache HTTP-Server so konfigurieren, dass ein Port kleiner als 1024 abgehört wird (Listen-Modus), müssen Sie als root angemeldet sein, um den Prozess zu starten. Für Port 1024 und darüber kann httpd als normaler Benutzer gestartet werden.

Listen kann auch zur Angabe spezieller IP-Adressen verwendet werden, über die der Server Verbindungen annimmt.

10.5.14. Include

Include erlaubt, dass andere Konfigurationsdateien während der Laufzeit mit aufgenommen werden.

Der Pfad zu diesen Konfigurationspfaden kann absolut sein oder sich auf ServerRoot beziehen.

Wichtig

Damit der Server einzeln verpackte Module verwendet wie mod_ssl, mod_perl und php muss sich folgende Anweisung in Section 1: Global Environment von http.conf befinden:

```
Include conf.d/*.conf
```

10.5.15. LoadModule

LoadModule wird verwendet, um Dynamic Shared Objects (DSO)-Modulen zu laden. Weitere Informationen zur DSO-Unterstützung von Apache HTTP-Server einschließlich der genauen Verwendung der Anweisung LoadModule finden Sie in Abschnitt 10.7. Beachten Sie, dass die Ladereihenfolge der Module *nicht mehr* wichtig ist bei Apache HTTP-Server 2.0. Weitere Informationen zur DSO-Unterstützung in Apache HTTP-Server 2.0 finden Sie unter Abschnitt 10.2.1.3.

10.5.16. ExtendedStatus

Die Anweisung ExtendedStatus bestimmt, ob Apache beim Aufruf des server-status-Handler grundlegende (off) oder detaillierte Server-Status-Informationen (on) erstellt. Server-status wird über Location-Tags aufgerufen. Weitere Informationen zum Aufruf von server-status finden Sie in Abschnitt 10.5.63.

10.5.17. 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.

10.5.18. 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.

Anmerkung

Aus Sicherheitsgründen kann Apache HTTP-Server nicht als root ausgeführt werden.

10.5.19. Group

Gibt den Gruppennamen des Apache HTTP-Server-Prozesses an.

Die Standardeinstellung für Group ist apache.

10.5.20. 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` gesetzt.

Meistens ist es am günstigsten, `ServerAdmin` auf `webmaster@example.com` einzustellen. 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.

10.5.21. ServerName

Mit `ServerName` können Sie einen Rechnernamen und eine Port-Nummer (die mit der Anweisung `Listen` übereinstimmt) für Ihren Server angeben. Der Servername kann sich vom wirklichen Namen Ihres Host unterscheiden. Zum Beispiel können Sie so den Namen `www.example.com` angeben, aber der Hostname des Servers ist tatsächlich `foo.example.com`. Beachten Sie, dass `ServerName` einen gültigen Domain Name Service (DNS)-Namen enthalten muss, den Sie auch tatsächlich verwenden dürfen — also nicht einfach etwas ausdenken.

Folgend ist ein Beispiel einer `ServerName`-Anweisung:

```
ServerName www.example.com:80
```

Wenn Sie in `ServerName` einen Servernamen angeben, muss die entsprechende Zuordnung von IP-Adresse und Servername in Ihrer `/etc/hosts`-Datei enthalten sein.

10.5.22. UseCanonicalName

Wenn `UseCanonicalName` auf `on` eingestellt ist, konfiguriert diese Anweisung Apache HTTP-Server sich selbst mit den in `ServerName` und `Port` angegebenen Werten zu referenzieren. 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.

`UseCanonicalName` ist standardmäßig auf `off` gesetzt.

10.5.23. DocumentRoot

`DocumentRoot` ist 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://example.com/foo.html
```

Der Server sucht die folgende Datei im Standardverzeichnis:

```
/var/www/html/foo.html
```

Wenn Sie den Eintrag in `DocumentRoot` ändern möchten, dass dieser nicht vom sicheren und vom unverschlüsselten Web-Server gemeinsam benutzt wird, finden Sie in Abschnitt 10.8 entsprechende Informationen.

10.5.24. `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.

In der Standardeinstellung werden für das root-Verzeichnis mit den Anweisungen `Options` (siehe Abschnitt 10.5.25) und `AllowOverride` (siehe Abschnitt 10.5.26) 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 Apache HTTP-Server auf Dateien in diesem Verzeichnis zugreifen kann.

Der `Directory`-Container kann auch dazu verwendet werden, zusätzliche `cgi-bin`-Verzeichnisse für Applikationen auf der Server-Seite ausserhalb des in der `ScriptAlias`-Anweisung angegebenen Verzeichnisses (sehen Sie Abschnitt 10.5.44 für mehr Information zur `ScriptAlias` Anweisung) anzugeben.

Um dies zu erzielen, muss der `Directory`-Container die `ExecCGI` Option für dieses Verzeichnis setzen.

Wenn sich CGI-Skripte zum Beispiel im Verzeichnis `/home/my_cgi_directory` befinden, fügen Sie der Datei `httpd.conf` folgenden `Directory`-Container hinzu:

```
<Directory /home/my_cgi_directory>
    Options +ExecCGI
</Directory>
```

Als nächstes müssen für die Anweisung `AddHandler` die Kommentare entfernt werden, damit Dateien mit der Endung `.cgi` als CGI-Skripts erkannt werden können. Anleitungen zur Einstellung von `AddHandler` finden Sie in Abschnitt 10.5.59.

Damit dies funktioniert, müssen die Zugriffsberechtigungen für CGI-Skripts und den gesamten Pfad zu den Skripts auf 0755 eingestellt sein.

10.5.25. `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` (z.B. `index.html`) angegeben wird. `Includes` bedeutet, dass server-seitige Includes erlaubt sind. `FollowSymLinks` erlaubt dem Server, in diesem Verzeichnis symbolischen Links zu folgen.

Anmerkung

`Options` Statements aus dem Konfigurationsabschnitt des Hauptservers müssen zu jedem einzelnen `VirtualHost`-Container übertragen werden. Sehen Sie Abschnitt 10.5.69 für zusätzliche Informationen zu `VirtualHost`-Containers.

10.5.26. 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.

10.5.27. Order

Die Anweisung `Order` bestimmt die Reihenfolge, in der die Anweisungen `allow` und `deny` ausgewertet werden. Der Server ist so konfiguriert, dass für Ihr `Allow` Anweisungen vor den `Deny` Anweisungen für Ihr `DocumentRoot` ausgewertet werden.

10.5.28. 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.

10.5.29. Deny

`Deny` funktioniert genauso wie `Allow`, wobei angegeben wird, wem der Zugriff nicht gestattet ist. In Ihrer `DocumentRoot` sind standardmäßig keine `Deny`-Anweisungen enthalten.

10.5.30. 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://`*`example.com`*`/~`*`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 ebenfalls ausreichend). Dateien, die im `public_html`-Verzeichnis der Benutzer zum Abruf angeboten werden, müssen mindestens die Berechtigung 0644 haben.

10.5.31. 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://*example*/*this_directory*/, anfordert, wird entweder die `DirectoryIndex`-Seite (falls vorhanden) oder eine vom Server erstellte Verzeichnisliste angezeigt. Die Standardeinstellung für den `DirectoryIndex` ist `index.html` und die `index.html.var` Type-Map. 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.

10.5.32. `AccessFileName`

`AccessFileName` bestimmt die Datei, die vom Server zur Speicherung von Zugriffskontrollinformationen in jedem Verzeichnis verwendet werden soll. Standardmäßig ist dies `.htaccess`.

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).

10.5.33. `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 Sie `CacheNegotiatedDocs` auf `on` setzen, wird diese Funktion deaktiviert und Proxyserver können Dokumente im Cache halten.

10.5.34. `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.

Weitere Informationen über `AddType` finden Sie in Abschnitt 10.5.58.

10.5.35. `DefaultType`

`DefaultType` definiert einen Default Content-Type, den der Web-Server für Dokumente verwendet, deren MIME-Types nicht bestimmt werden können. Die Standardeinstellung ist `text/plain`.

10.5.36. `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 geladen wurde. Wenn ein Ausrufezeichen [!] vor dem Modulnamen steht, werden die Anweisungen nur verarbeitet, wenn das Modul im ersten <`IfModule`>-Tag *nicht* geladen ist.

Für weitere Informationen zu Apache HTTP-Server Modulen, sehen Sie Abschnitt 10.7.

10.5.37. HostnameLookups

HostnameLookups kann auf on, off oder double 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 Host-Namen zu bestimmen. Wenn Sie HostnameLookups auf double einstellen, stellt Ihr Server einen doppelt-umgekehrten DNS aus, was diesen zusätzlich belastet.

Um Server-Ressourcen zu sparen, sollten Sie die Einstellung für HostnameLookups auf off belassen werden.

Wenn Host-Namen in den Protokolldateien des Servers notwendig sind, verwenden Sie eines der vielen Analyse-Tools für Protokolldateien, mit denen die DNS-Lookups wirkungsvoller und stapelweise erfolgen wenn Sie Ihre Protokolldatein rotieren.

10.5.38. ErrorLog

ErrorLog bestimmt die Datei, in der Server-Fehler protokolliert werden. Diese Anweisung ist standardmäßig auf /var/log/httpd/error_log gesetzt.

10.5.39. LogLevel

LogLevel legt fest, wie ausführlich die Fehlermeldungen im Fehlerprotokoll dargestellt werden. LogLevel kann die Werte (mit steigendem Grade an Detaillierung) emerg, alert, crit, error, warn, notice, info oder debug haben. Der Default-Wert für LogLevel ist warn.

10.5.40. LogFormat

Die LogFormat-Anweisung legt das Format für die Meldungen in den Log-Dateien des Web-Servers fest. Welches LogFormat verwendet wird, hängt von den Einstellungen in der CustomLog-Anweisung ab (siehe Abschnitt 10.5.41).

Die Folgenden sind die Formatierungsoptionen, für den Fall, dass die CustomLog Anweisung auf combined gesetzt ist:

%h (Der Name, oder die IP-Adresse des Remote Hosts)

Listet die Remote-IP-Adresse des anfragenden Clients. Wenn HostnameLookups auf on gesetzt ist, wird der Hostname des Client gespeichert, ausser dieser ist nicht über DNS verfügbar.

%l (rfc931)

Wird nicht verwendet. An dieser Stelle wird in der Protokolldatei – eingetragen.

%u (Authentifizierter Benutzer)

Wenn eine Authentifizierung erforderlich war, hat der Benutzer diesen Namen angegeben. Normalerweise nicht verwendet. An dieser Stelle wird – eingetragen.

%t (Datum)

Listet das Datum und die Uhrzeit der Anforderung.

%r (Request-String)

Listet den Request-String, wie vom Browser oder Client übernommen.

`%s` (Status)

Listet den HTTP Status-Code, welcher vom Client-Host zürückgegeben wurde.

`%b` (Bytes)

Listet die Größe des Dokuments.

`%\"%{Referer}i\"` (Verweisende Webseite)

Listet die URL der Webseite, die den Client Host zum Web-Server verwiesen hat.

`%\"%{User-Agent}i\"` (User-Agent)

Listet den Typ des anfragenden Web-Browsers.

10.5.41. `CustomLog`

`CustomLog` identifiziert die Log-Datei und das Format der Log-Datei. Standardmäßig werden die Log-Meldungen, nach `/var/log/httpd/access_log` geschrieben.

Das Standardformat von `CustomLog` ist `combined`. Folgend ist das `combined`-Format gezeigt:

```
remotehost rfc931 user date "request" status bytes referrer user-agent
```

10.5.42. `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` setzen (so wird keine Signaturzeile eingefügt) oder auf `EMail` ändern . `EMail` fügt ein HTML-Tag `mailto:ServerAdmin` in die Signaturzeile.

10.5.43. `Alias`

Mit der Einstellung `Alias` können Verzeichnisse außerhalb des Verzeichnisses `DocumentRoot` liegen und der Web-Server kann doch darauf zugegreifen. Jede URL, die mit dem Alias endet, verzweigt automatisch zum Aliaspfad. Als Standard-Einstellung ist bereits ein Alias eingerichtet. Auf das Verzeichnis `icons` kann vom Web-Server zugegriffen werden, dieses liegt jedoch nicht im `DocumentRoot`.

10.5.44. `ScriptAlias`

Die Einstellung `ScriptAlias` legt fest, wo CGI-Skripts (oder andere Skriptarten) abgelegt sind. Im Allgemeinen sollten CGI-Skripts nicht in `DocumentRoot` abgelegt werden. In `DocumentRoot` abgelegte CGI-Skripts könnten wie Textdokumente gelesen werden. Deswegen ist das Verzeichnis `cgi-bin` standardmäßig ein `ScriptAlias` von `/cgi-bin/` und in Wirklichkeit das Verzeichnis `/var/www/cgi-bin/`.

Es ist möglich Verzeichnisse mit ausführbaren Dateien ausserhalb von `cgi-bin` zu erstellen. Für Anleitungen dazu, sehen Sie Abschnitt 10.5.59 und Abschnitt 10.5.24.

10.5.45. Redirect

Wenn eine Web-Seite verschoben wird, kann mit Redirect die Zuordnung der alten URL auf eine neue URL erfolgen. Hier das Format:

```
Redirect /<old-path>/<file-name> http://<current-domain>/<current-path>/<file-name>
```

Ersetzen Sie in diesem Beispiel <old-path> mit den alten Pfadinformationen für <file-name> und <current-domain> sowie <current-path> mit der augenblicklichen Domain und den Pfadinformationen für <file-name>.

In diesem Beispiel werden alle Anfragen an <file-name> über die alte URL automatisch zur neuen URL umgeleitet.

Für erweiterte Methoden zur Umleitung, verwenden Sie das Modul mod_rewrite, welche im Apache HTTP-Server enthalten ist. Für weitere Informationen zum Konfigurieren von mod_rewrite, sehen Sie die Dokumentation auf der Webseite der Apache Software Foundation, Online unter http://httpd.apache.org/docs-2.0/mod/mod_rewrite.html.

10.5.46. IndexOptions

IndexOptions bestimmt das Erscheinungsbild der vom Server erstellten Verzeichnislisten durch das Hinzufügen von Symbolen, Dateibeschreibungen usw. Wenn Options Indexes aktiviert ist (siehe Abschnitt 10.5.25), kann Ihr Web-Server eine Verzeichnisliste erstellen, wenn er eine HTTP-Anforderung wie die Folgende empfängt:

Als Erstes sucht Ihr Web-Server in diesem Verzeichnis nach einer Datei aus der Liste, die nach der Anweisung DirectoryIndex angegeben ist (z.B. index.html). Wenn er keine der Dateien finden kann, wird Apache HTTP-Server eine HTML-Verzeichnisliste der in dem Verzeichnis enthaltenen Unterverzeichnisse und Dateien erstellt. Mit bestimmten Anweisungen können Sie in IndexOptions 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 IconsAre-Links,durch die die Symbole zusammen mit dem Dateinamen als Teil des HTML-Ankers für den Link verwendet werden können.

10.5.47. 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.

10.5.48. 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.

10.5.49. 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.

10.5.50. 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 dabei der Default.

10.5.51. AddDescription

Mit `AddDescription` können Sie in vom Server erstellten Listen für bestimmte Dateien von Ihnen eingegebenen Text anzeigen lassen, wozu `FancyIndexing` in `IndexOptions` aktiviert sein muss. Sie können bestimmte Dateien, Platzhalterausdrücke oder Dateiendungen für die Dateien angeben, auf die diese Anweisung angewandt werden soll. `AddDescription` unterstützt das Auflisten von bestimmten Dateien, Wildcard-Ausdrücken oder Dateiendungen.

10.5.52. 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.html` eingestellt.

10.5.53. 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.

10.5.54. 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.

10.5.55. 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.

10.5.56. 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.

10.5.57. LanguagePriority

LanguagePriority ermöglicht die Einstellung, in welchen Sprachen Dateien geliefert werden sollen, falls vom Client im Browser keine Angabe zur Sprache vorliegt.

10.5.58. 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. Mit folgender Anweisung erkennt Apache HTTP-Server die Dateierweiterung .shtml:

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

10.5.59. 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 bearbeiten. Das folgende Beispiel ist eine AddHandler Anweisung für die Dateiendung .cgi.

```
AddHandler cgi-script .cgi
```

Diese Anweisung erlaubt CGIs auch ausserhalb von cgi-bin zu arbeiten, und zwar in jedem Verzeichnis, welches die ExecCGI Option im Verzeichnis-Container gesetzt hat. Sehen Sie Abschnitt 10.5.24 für weitere Informationen zum Einrichten der ExecCGI Option für ein Verzeichnis.

AddHandler wird vom Server neben CGI-Skripts auch für die Verarbeitung der vom Server verarbeiteten HTML- und Image-Map-Dateien verwendet.

10.5.60. 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.

10.5.61. `ErrorDocument`

`ErrorDocument` verknüpft einfach einen HTTP-Antwortcode mit einer Meldung oder einer URL, die zum Client zurückgesendet wird. 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.

Wichtig

Sie *müssen* die Fehlermeldung in doppelte Anführungszeichen ["] setzen, damit diese gültig ist.

10.5.62. `BrowserMatch`

Die Anweisung `BrowserMatch` ermöglicht es Ihrem Server, Umgebungsvariablen zu definieren und 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.

10.5.63. `Location`

Die Tags `<Location>` und `</Location>` ermöglichen die Angabe von Zugangsberechtigungen auf URL-Basis.

Wenn Sie zulassen möchten, dass Benutzer von Ihrer Domain 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 <.example.com>
</Location>
```

Dabei muss *<.example.com>* durch den Namen Ihrer Second Level Domain 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 <.example.com>
</Location>
```

Auch hier muss *<.example.com>* entsprechend ersetzt werden.

10.5.64. ProxyRequests

Um Apache HTTP-Server als einen Proxy-Server konfigurieren, entfernen Sie die Kommentarsymbole aus der <IfModule mod_proxy.c>-Zeile um das mod_proxy Modul zu laden, und setzen Sie die ProxyRequests-Anweisung auf On.

10.5.65. Proxy

Die Tags <Proxy *> und </Proxy> bestimmen einen Container, welcher eine Gruppe von Konfigurationsanweisungen umschließt, die nur auf den Proxy-Server angewandt werden sollen. Viele auf ein Verzeichnis anzuwendende Anweisungen können in <Proxy>-Tags eingeschlossen werden.

10.5.66. ProxyVia

Der Befehl ProxyVia legt für einen HTTP Via: Header fest, ob dieser zusammen mit Anforderungen oder Antworten gesendet wird, die über den Apache Proxy-Server laufen. Wenn der ProxyVia auf On eingestellt ist, enthält der Via: Header den Host-Namen, für Full Host-Namen und die Apache HTTP-Server Version, alle Via: Header werden unverändert weitergegeben wenn auf Off, und die Via: Header werden entfernt bei Einstellung auf Block.

10.5.67. Cache-Anweisungen

Eine Reihe von auskommentierten Cache-Anweisungen sind in der Standardkonfigurationsdatei von Apache HTTP-Server enthalten. Wenn Sie die Proxy-Server Funktion nutzen und auch den Proxy-Cache aktivieren möchten, sollten Sie die Kommentar-Symbole [#] am Anfang der Zeile entfernen. Die folgende Standardeinstellungen für Ihre Cache-Anweisungen sollten für die meisten Konfigurationen ausreichen.

- CacheRoot — Bestimmt den Namen des Verzeichnisses, in dem die zwischengespeicherten Dateien abgelegt werden. Der Standard-CacheRoot ist das Verzeichnis /var/httpd/proxy/.
- 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. Die Standardeinstellung für CacheGcInterval ist 4 Stunden.
- CacheMaxExpire — Im Cache gespeicherte HTML-Dokumente werden für eine maximale Anzahl von Stunden im Cache gehalten (ohne Neuladen vom Ursprungsserver). Der Standardwert ist 24 Stunden.
- 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 — Die Ablaufzeit für ein Dokument in Stunden, das über ein Protokoll empfangen wurde, das keine Ablaufzeiten unterstützt. Die Standardeinstellung ist 1 Stunde.
- NoCache — Gibt Hosts an, deren Inhalt nicht zwischengespeichert werden soll.

10.5.68. `NameVirtualHost`

Wenn Sie namensbasierte virtuelle Hosts einrichten, müssen Sie die Anweisung `NameVirtualHost` für die IP-Adresse verwenden und die Portnummer, falls erforderlich. Die Konfiguration von namensbasierten virtuellen Hosts wird verwendet, wenn Sie verschiedene virtuelle Hosts für verschiedene Domains einrichten möchten ohne mehrere IP-Adressen zu verwenden.

Anmerkung

Alle eingerichteten namensbasierten virtuellen Hosts funktionieren *nur* für unverschlüsselte HTTP-Verbindungen, da Sie keine namensbasierten virtuellen Hosts für einen verschlüsselten Server verwenden können. Müssen Sie virtuelle Hosts mit einem verschlüsselten Server verwenden, benötigen Sie IP-adressbasierte virtuelle Hosts.

Wenn Sie namensbasierte virtuelle Hosts verwenden, sind für die Konfigurationsanweisung `NameVirtualHost` die Kommentare zu entfernen, und nach `NameVirtualHost` ist die richtige IP-Adresse für Ihren Server anzugeben. Anschließend sind mit `VirtualHost`-Tags weitere Informationen zu den verschiedenen Domains hinzuzufügen.

10.5.69. `VirtualHost`

Die Tags `<VirtualHost>` und `</VirtualHost>` umschließen alle Konfigurationsanweisungen, die für einen virtuellen Host gelten. Die meisten Konfigurationsanweisungen können innerhalb von `<VirtualHost>`-Tags verwendet werden und gelten dann für diesen virtuellen Host.

Eine Reihe von auskommentierten `VirtualHost`-Tags umschließen einige Beispielkonfigurationsanweisungen und Platzhalter für die Informationen, die für die Einrichtung eines virtuellen Hosts benötigt würden. Weitere Informationen über virtuelle Hosts finden Sie in Abschnitt 10.8.

Anmerkung

Alle virtuellen Hostumgebungen von SSL wurden in die Datei `/etc/httpd/conf.d/ssl.conf` verschoben.

10.5.70. SSL-Konfigurationsanweisungen

Die SSL-Anweisungen in der Datei `/etc/httpd.conf.d/ssl.conf` können so konfiguriert werden, dass sichere Web-Kommunikationen mit SSL und TLS möglich sind.

10.5.70.1. `SetEnvIf`

Die Apache-Konfigurationsanweisung `SetEnvIf` kann dazu verwendet werden, um Umgebungsvariablen zu setzen, die auf Header-Informationen der Anfrage basieren. In der mitgelieferten Datei `httpd.conf` 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.

Für weitere Informationen zu SSL-Anweisungen, geben Sie die folgende Adresse in einem Web-Browser an:

- http://localhost/manual/mod/mod_ssl.html
- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html

Informationen über das Einrichten eines Apache HTTP Secure Server finden Sie im Kapitel *Apache HTTP Secure Server Configuration* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

Anmerkung

In den meisten Fällen sind die SSL-Anweisungen in der installierten Form völlig ausreichend. Seien Sie Sie sehr vorsichtig wenn Sie Veränderungen an Ihren SSL-Anweisungen vornehmen, da eine Falscheinstellung zu Sicherheitslücken führen kann.

10.6. Standard-Module

Apache HTTP-Server wird mit einer Reihe von Modulen vertrieben. Standardmäßig werden folgende Module mit dem `httpd` Packet auf Red Hat Linux installiert und aktiviert:

```
mod_access
mod_auth
mod_auth_anon
mod_auth_dbm
mod_auth_digest
mod_include
mod_log_config
mod_env
mod_mime_magic
mod_cern_meta
mod_expires
mod_headers
mod_usertrack
mod_unique_id
mod_setenvif
mod_mime
mod_dav
mod_status
mod_autoindex
mod_asis
mod_info
mod_cgi
mod_dav_fs
mod_vhost_alias
mod_negotiation
mod_dir
mod_imap
mod_actions
mod_speling
mod_userdir
mod_alias
mod_rewrite
mod_proxy
mod_proxy_ftp
mod_proxy_http
mod_proxy_connect
```

Folgende Module sind zusätzlich verfügbar, wenn Sie weitere Pakete installieren:

```
mod_auth_mysql
mod_auth_pgsql
mod_perl
mod_python
mod_ssl
php
squirrelmail
```

10.7. Module hinzufügen

Apache HTTP-Server unterstützt *Dynamically Shared Objects* (*DSO*s) oder Module, welche einfach zur Laufzeit, wenn benötigt, geladen werden können.

Das Apache Project stellt eine vollständige DSO-Dokumentation unter http://httpd.apache.org/docs-2.0/dso.html zur Verfügung. Nach der Installation des Pakets `http-manual` steht Ihnen auch weitere Dokumentation zu DSOs unter http://localhost/manual/mod/ bereit.

Damit Apache HTTP-Server DSO verwenden kann, muss dies in einer `LoadModule`-Anweisung in `/etc/httpd/conf/httpd.conf` angegeben werden. Sollte das Modul durch ein eigenes Paket zur Verfügung gestellt werden, muss diese Zeile in der Konfigurationsdatei dieses Moduls enthalten sein. Diese Konfigurationsdatei ist im Verzeichnis `/etc/httpd/conf.d/` zu finden. Sehen Sie Abschnitt 10.5.15 für Weiteres zur `LoadModule`-Anweisung.

Wenn Sie Module aus `http.conf` hinzufügen oder löschen, müssen Sie Apache HTTP-Server neu laden oder starten, wie in Abschnitt 10.4 beschrieben.

Wenn Sie ein neues Modul erzeugen wollen, müssen Sie das Paket `httpd-devel` installieren, weil es die Include-Dateien, die Header-Dateien und die *APache eXtenSion* (`/usr/sbin/apxs`) enthält, welches die Include- und Header-Dateien verwendet, um die DSOs zu kompilieren.

Wenn Sie ein eigenes Modul geschrieben haben, sollten Sie `/usr/sbin/apxs` für das Kompilieren Ihrer sich ausserhalb des Apache Quellbaums befindlichen Modulquellen verwenden. Weitere Informationen zur Verwendung von `/usr/sbin/apxs` finden Sie in der Apache Dokumentation unter http://httpd.apache.org/docs-2.0/dso.html und der man-Seite zu `apxs`.

Speichern Sie Ihr Modul nach dem Kompilieren im Verzeichnis `/usr/lib/httpd`. Fügen Sie dann der Datei `httpd.conf` eine `LoadModule`-Zeile hinzu, welche folgenden Aufbau hat:

```
LoadModule <module-name> <path/to/module.so>
```

Ersetzen Sie <*module-name*> mit dem Namen des Moduls, und <*path/to/module.so*> mit dem Pfad zum DSO.

10.8. Virtual Hosts

Apache HTTP-Server bietet die Möglichkeit zur Verwendung von virtuellen Hosts, um verschiedene Server für verschiedene IP-Adressen, verschiedene Rechnernamen oder verschiedene Ports auf demselben Server zu benutzen. Eine vollständige Anleitung zur Verwendung virtueller Hosts finden Sie unter http://httpd.apache.org/docs-2.0/vhosts/.

10.8.1. Einrichten von virtuellen Hosts

Um einen namensbasierten virtuellen Host einzurichten, ist es am besten, den entsprechenden Container in `httpd.conf` als Grundlage zu nehmen.

Hier die Beispielszeilen für den virtuellen Host:

```
#NameVirtualHost *
#
#<VirtualHost  *>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
```

Um namensbasiertes virtuelles Hosting zu ermöglichen, entfernen Sie das Hash-Symbol (`#`) am Anfang der `NameVirtualHost`-Zeile und ersetzen Sie den Stern (`*`) mit der IP-Adresse des entsprechenden Rechners.

Als nächstes, konfigurieren Sie einen virtuellen Host, indem Sie das Kommentarsymbol aus den `<VirtualHost>`-Zeilen entfernen.

In der öffnenden `<VirtualHost>`-Zeile, ersetzen Sie den Stern (`*`) mit der IP-Adress des entsprechenden Servers. Setzen Sie den `ServerName` auf einen *gültigen* DNS Namen, welcher dem Rechner zugewiesen ist, und stellen Sie die anderen Anweisungen nach Ihren Anforderungen ein.

Der `<VirtualHost>`-Container ist im höchsten Grade Ihren jeweiligen Anforderungen anpassbar und akzeptiert nahezu jede Anweisung verfügbar in der Haupt-Server Konfiguration.

Tipp

Wenn Sie einen virtuellen Host einrichten und dieser an einem Port auf Anforderungen warten soll, der nicht der Standardport ist, müssen Sie für diesen Port einen virtuellen Host einrichten und eine entsprechende `Listen`-Anweisung in der Datei `/etc/httpd/conf/http.conf` einfügen.

Um einen neu erstellten virtuellen Host zu aktivieren, laden oder starten Sie den Apache HTTP-Server neu. Informationen dazu erhalten Sie unter Abschnitt 10.4.

Vollständige Informationen zum Erstellen und Konfigurieren von namensbasierten und IP-Adressenbasierten virtuellen Hosts finden Sie im Web unter http://httpd.apache.org/docs-2.0/vhosts/.

10.8.2. Der virtuelle Host des Secure Web-Servers

Standardmäßig ist Apache HTTP-Server sowohl als normaler Server, als auch als Secure Server konfiguriert. Beide Server verwenden dieselbe IP-Adresse und denselben Host-Namen, warten jedoch an verschiedenen Ports auf Anforderungen: 80 und 443. Mit dieser Konfiguration kann sowohl unverschlüsselte als auch verschlüsselte Kommunikation gleichzeitig ablaufen.

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.

Wichtig

Verwenden Sie keinen namensbasierten virtuellen Host in Verbindung mit einem Secure Web-Server, da der SSL Handshake stattfindet, bevor die HTTP-Anforderung den entsprechenden namensbasierten virtuellen Host identifiziert. Namensbasierte virtuelle Hosts arbeiten nur mit normalen Web-Servern.

Die Konfigurationsanweisungen für Ihren Secure Server sind in der Datei `/etc/httpd/conf.d/ssl.conf` innerhalb von VirtualHost Tags untergebracht.

Standardmäßig verwenden sowohl der sichere als auch der normale Web-Server dieselbe `DocumentRoot`. Es wird empfohlen, dass der Secure Web-Server eine andere `DocumentRoot` verwendet.

Um zu verhindern, dass der normale Web-Server weiterhin Verbindungen akzeptiert, kommentieren Sie die Zeile in `httpd.conf` aus, welche `Listen 80` enthält. Stellen Sie dieser wie folgt ein Hash-Symbol voran:

```
#Listen 80
```

Für weitere Informationen zum Konfigurieren eines SSL Web-Server, sehen Sie das Kapitel *Konfiguration von Apache HTTP Secure Server* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*. Für fortgeschrittene Konfigurationshinweise, sehen Sie die Dokumentation der Apache Software Foundation, welche unter den folgenden URLs verfügbar ist:

- http://httpd.apache.org/docs-2.0/ssl/.
- http://httpd.apache.org/docs-2.0/vhosts/

10.9. Zusätzliche Ressourcen

Weitere Informationen zu Apache HTTP-Server finden Sie in folgenden Ressourcen:

10.9.1. Hilfreiche Webseiten

- http://httpd.apache.org — Die offizielle Website für den Apache HTTP-Server mit Dokumentationen zu allen Anweisungen und Standardmodulen.
- http://www.modssl.org — Die offizielle Website für `mod_ssl`.
- http://www.apacheweek.com — Eine wöchentliche Online-Ausgabe über alles, was Apache betrifft.

10.9.2. Zusätzliche Bücher

- *Apache Desktop Reference* von Ralf S. Engelschall; Addison Wesley — Verfasst von dem ASF-Mitglied und `mod_ssl`-Autor Ralf Engelschall, das *Apache Desktop Reference* ist ein kompaktes jedoch all umfassendes Nachschlagewerk zur Verwendung von Apache HTTP-Server, Kompilierung, Konfiguration, und Laufzeit. Dieses Buch steht online unter http://www.apacheref.com/.
- *Professional Apache* von Peter Wainwright; Wrox Press Ltd — *Professional Apache* stammt von Wrox Press Ltd's "Programmer to Programmer" Reihe und richtet sich sowohl an erfahrene als auch einsteigende Web-Server-Administratoren.
- *Administering Apache* von Mark Allan Arnold; Osborne Media Group — Dieses Buch ist für Internet Service Providers, die sicherere Services zur Verfügung stellen wollen.
- *Apache Server Unleashed* von Richard Bowen, et al; SAMS BOOKS — Eine Enzyklopädie zu Apache HTTP-Server.
- *Apache Pocket Reference* von Andrew Ford, Gigi Estabrook; O'Reilly — Dies ist das letzte Werk der O'Reilly Pocket Reference Reihe.

redhat

Kapitel 11.

E-Mail

Die Geburtsstunde elektronischer Mail (*E-Mail*) liegt in den frühen sechziger Jahren. Die Mailbox war eine Datei im Home-Verzeichnis des Benutzers, das nur vom Benutzer gelesen werden konnte. Anfängliche Mail-Applikationen hängten neue Text-Nachrichten an das Ende dieser Datei an, und der Benutzer musste sich durch diese ständig wachsende Datei wühlen, um die entsprechende Nachricht zu finden. Dieses System war lediglich dazu in der Lage Nachrichten an Benutzer auf dem selben System zu senden.

Das erste Mal, dass eine elektronische Mail über ein Netzwerk gesendet wurde, war in 1971. Der Computer-Engineer Ray Tomlinson sendete eine Test-Nachricht zwischen zwei Rechnern mittles ARPANET — der Vorgänger des Internet. Kommunikation über E-Mail bekam bald darauf sehr populär, und stellte innerhalb von zwei Jahren 75 Prozent des Netzwerkverkehrs auf dem ARPANET dar.

Heutzutage haben sich die auf standardisierten Netzwerkprotokollen basierenden E-Mail-Systeme zu den am meisten verwendeten Services im Internet entwickelt. Red Hat Linux bietet zahlreiche fortgeschrittene E-Mail-Applikationen.

In diesem Kapitel werden bekannte, gegenwärtig verwendete E-Mail-Protokolle und einige Programme, die mit E-Mail im Zusammenhang stehen, beschrieben.

11.1. E-Mail Protokolle

E-Mail wird heutzutage über eine Client/Server Architektur verteilt. Eine elektronische Mail wird mit einem Client-Programm erzeugt. Dieses Programm sendet die E-Mail an einen Server, welcher diese dann an den E-Mail-Server des Empfängers weiterleitet. Dort wird die E-Mail dann vom E-Mail-Server dem E-Mail-Client des Empfängers übergeben.

Um diesen Vorgang zu ermöglichen, erlaubt eine Reihe von Standardnetzwerkprotokollen verschiedenen Rechnern, welche oft verschiedene Betriebssysteme ausführen und verschiedene E-Mail-Programme verwenden, E-Mails zu senden und zu empfangen.

Die folgende Protokolle werden am häufigsten für das Versenden von E-Mails zwischen unterschiedlichen Systemen verwendet.

11.1.1. Mail Transport Protocols

Die Zustellung von E-Mails von einer Client-Applikation zu einem Server, und von einem ausgehenden Server zu einem Ziel-Server wird über das *Simple Mail Transfer Protocol* (*SMTP*) gehandhabt.

11.1.1.1. SMTP

SMTP wird hauptsächlich zum Übertragen von E-Mails zwischen Servern verwendet, ist jedoch auch für E-Mail-Clients wichtig. Um E-Mails senden zu können, muss der Client die Nachricht an einen ausgehenden Mail-Server senden, welcher dann eine Verbindung mit dem Ziel-Server herstellt, um die E-Mail zu übertragen. Aus diesem Grund ist es wichtig, einen SMTP Server beim Konfigurieren des E-Mail-Clients anzugeben.

Unter Red Hat Linux kann ein Benutzer einen SMTP Server auf dem lokalen Rechner konfigurieren, um eingehende E-Mails zu handhaben. Es ist jedoch auch möglich, einen Remote SMTP Server für ausgehende E-Mails zu konfigurieren.

Ein wichtiger Punkt im Bezug zum SMTP Protokoll ist der, dass es keine Authentifizierung benötigt. Dies erlaubt es jedem im Internet, E-Mails zu jedem Anderen und sogar zu größeren Gruppen zu senden. Es ist diese Eigenschaft von SMTP, die Junk-E-Mail, oder *spam*, möglich macht. Moderne

SMTP Server versuchen dies einzuschränken, indem Sie nur bekannten Hosts den Zugriff gewähren. Server, die solche Einschränkungen nicht durchsetzen, werden *Open Relay* Server genannt.

Red Hat Linux benutzt Sendmail (`/usr/sbin/sendmail`) als standardmäßiges SMTP-Programm. Postfix (`/usr/sbin/postfix`), eine einfacher zu verwendende Applikation steht jedoch ebenfalls zur Verfügung.

11.1.2. Mail Access Protocols

Es gibt zwei grundlegende Protokolle, die von E-Mail Client Applikationen verwendet werden, um E-Mails von einem Mail-Server abzurufen: das *Post Office Protocol* (*POP*) und das *Internet Message Access Protocol* (*IMAP*).

Im Unterschied zu SMTP erfordern beide dieser Protokolle, dass die verbindenden Clients sich mit einem Benutzernamen und Passwort authentifizieren müssen. Standardmäßig werden die Passwörter für beide Protokolle unverschlüsselt über das Netzwerk gesandt.

11.1.2.1. POP

Der standardmäßige POP Server in Red Hat Linux ist `/usr/sbin/ipop3d` und wird mit dem `imap`-Paket installiert. Das Verwenden eines POP Servers erlaubt E-Mail-Clients, E-Mails von einem Remote-Server herunterzuladen. Die meisten POP E-Mail-Clients sind automatisch so konfiguriert, dass sie Mitteilungen auf dem E-Mail-Server löschen, wenn sie erfolgreich an das Client-System übermittelt wurden. Dies kann normalerweise jedoch anders eingestellt werden.

POP ist vollständig kompatibel mit wichtigen Internet Messaging Standards, wie *Multipurpose Internet Mail Extensions* (*MIME*), welche es erlauben, Dateien an eine E-Mail anzuhängen.

POP ist am besten geeignet für Benutzer, die nur über ein einziges System verfügen, auf dem sie ihre E-Mails lesen. POP ist ebenfalls eine gute Lösung, wenn Sie keine ständige Verbindung zum Internet oder Ihrem Mail-Server haben. Da POP von Client-Programmen fordert, dass diese nach der Authentifizierung den gesamten Inhalt einer Nachricht herunterladen, kann dies für diejenigen mit einer langsamen Netzwerkverbindung eine lange Zeit in Anspruch nehmen, insbesondere, wenn große Dateien an E-Mails angehängt sind.

Die neueste Variante des Standard POP Protokolls ist POP3.

Es gibt jedoch auch eine Anzahl weniger häufig verwendeter POP Protokoll Varianten:

- *APOP* — POP3 mit MDS-Authentifizierung, wobei ein Hashcode Ihres Passworts, und nicht der unverschlüsselte Passworttext, vom E-Mail-Client zum Server übermittelt wird.
- *KPOP* — POP3 mit Kerberos-Authentifizierung. Weitere Informationen hierzu finden Sie unter Kapitel 17.
- *RPOP* — POP3 mit RPOP-Authentifizierung. Verwendet für jeden Benutzer eine Identifizierung, ähnlich der eines Passworts, um Anfragen von POP zu authentifizieren. Diese ID ist jedoch nicht verschlüsselt, so dass RPOP nicht sicherer als das Standard-POP ist.

Für zusätzliche Sicherheit ist es möglich, *Secure Socket Layer* (*SSL*) Verschlüsselung für die Client-Authentifizierung und den Datentransfer zu verwenden. Dies kann durch den `ipop3s` Service oder das `/usr/sbin/stunnel` Programm aktiviert werden. Sehen Sie Abschnitt 11.5.1 für weitere Informationen.

11.1.2.2. IMAP

Der standardmäßige IMAP Server in Red Hat Linux ist `/usr/sbin/imapd` und wird mit dem `imap`-Paket installiert. Bei der Verwendung von IMAP verbleiben die E-Mail-Nachrichten auf dem Server,

wo der Benutzer diese lesen oder löschen kann. IMAP erlaubt den Client-Applikationen auch Mailboxen zur Speicherung der E-Mails auf dem Server zu erstellen, umzunennen oder zu löschen.

IMAP ist vor allem für Benutzer nützlich, die ihre E-Mails von verschiedenen Rechnern aus abrufen. Auch Benutzer, die nur mit geringer Übertragungsrate Verbindungen zum Internet oder zu einem privaten Netzwerk herstellen können, verwenden oft IMAP, da hier als erstes nur der E-Mail Header angezeigt wird, was Bandbreite spart, bis die eigentlichen E-Mails geöffnet werden. Der Benutzer hat auch die Möglichkeit E-Mails zu löschen, ohne sich deren Inhalt anzusehen oder diese herunterzuladen.

Zur Vereinfachung können IMAP Client-Applikationen Inhalte von E-Mails lokal zwischenspeichern, damit es einem Benutzer möglich ist, E-Mails zu lesen ohne mit dem IMAP Server verbunden sein zu müssen.

IMAP, wie auch POP, ist vollständig kompatibel mit den wichtigen Internet Messaging Standards, wie MIME, was das Anhängen von Dateien an E-Mails erlaubt.

Für zusätzliche Sicherheit ist es möglich SSL für die Client-Authentifizierung und den Datentransfer zu verwenden. Dies kann durch den `imaps` Service oder das `/usr/sbin/stunnel` Programm aktiviert werden. Sehen Sie Abschnitt 11.5.1 für weitere Informationen.

Es gibt andere freie und auch kommerzielle IMAP-Clients und Server, die das IMAP-Protokoll erweitern und über zusätzliche Funktionen verfügen. Eine vollständige Liste finden Sie unter http://www.imap.org/products/longlist.htm.

11.2. E-Mail-Programm-Kategorien

Im allgemeinen können alle E-Mail-Applikationen mindestens einer von drei Kategorien zugeordnet werden. Jede dieser Kategorien hat eine spezielle Funktion beim Senden und Verwalten von E-Mails. Obwohl die meisten Benutzer nur das E-Mail-Programm kennen, das sie zum Senden und Empfangen von Nachrichten benutzen, ist jede dieser Kategorien wichtig, um gewährleisten zu können, dass die E-Mails auch bei der richtigen Adresse ankommen.

11.2.1. Mail Transfer Agent

Ein *Mail Transfer Agent* (*MTA*) überträgt E-Mails zwischen SMTP verwendenden Hosts. Eine E-Mail kann unter Umständen über mehrere MTA's auf dem Weg zu ihrem Bestimmungsort laufen.

Obwohl die Übermittlung von Mitteilungen zwischen Rechnern recht unkompliziert erscheint, ist der gesamte Prozess, in dessen Verlauf ein bestimmter MTA eine Mitteilung akzeptieren kann oder soll, um diese dann an einen Remote-Rechner zu übermitteln, ziemlich kompliziert. Aufgrund der Spams-Problematik ist die Verwendung eines bestimmten MTA's aufgrund dessen Konfiguration ode aufgrund des Netzwerkzgriffs des Systems, auf dem er ausgeführt wird, normalerweise beschränkt.

Viele der moderneren E-Mail Client-Programme können zum Versenden von E-Mails als MTA agieren. Dieser Vorgang sollte aber nicht mit den Prozessen eines reinen MTA's verwechselt werden. Der einzige Grund für E-Mail-Clients die Fähigkeit E-Mails zu versenden (wie ein MTA) zu besitzen, ist der, dass der Host der Applikation keinen eigenen MTA hat. Dies trifft vor allem für E-Mail-Clients auf nicht-Unix-basierten Betriebssystemen zu. Diese Client-Programme senden jedoch lediglich ausgehende E-Mails an einen MTA, für den sie authentifiziert sind, und stellen diese nicht direkt an den E-Mail-Server des Empfängers zu.

Da Red Hat Linux zwei MTAs, Sendmail und Postfix, enthält, wird es von E-Mail Client-Programmen oft nicht erfordert als MTA zu agieren. Red Hat Linux enthält auch einen speziellen MTA, Fetchmail genannt.

Für weitere Informationen zu Sendmail und Fetchmail, sehen Sie Abschnitt 11.3.

11.2.2. Mail Delivery Agent

Ein *Mail Delivery Agent* (*MDA*) wird vom MTA verwendet, um eingehende E-Mails in der richtigen Benutzer-Mailbox abzulegen. In vielen Fällen ist der MDA in Wirklichkeit ein *Local Delivery Agent* (*LDA*), wie `mail` oder Procmail.

Jedes Programm, das in der Lage ist Nachrichten dem Empfänger zuzustellen, sodass diese in einem E-Mail-Client gelesen werden können, kann als MDA bezeichnet werden. Aus diesem Grund können einige MTAs (wie Sendmail und Postfix) die Rolle eines MDA übernehmen, wenn sie neue E-Mails an die lokale Spool-Datei des Benutzers anhängen. Im Allgemeinen übertragen MDAs weder Nachrichten über Systemgrenzen hinweg, noch stellen sie eine Benutzerschnittstelle zur Verfügung; MDAs verteilen und sortieren Nachrichten auf einem lokalen Rechner, so dass eine E-Mail Client-Applikation auf diese Zugreifen kann.

11.2.3. Mail User Agent

Ein *Mail User Agent* (*MUA*) ist synonym zu einer E-Mail Client-Applikation. Ein MUA ist ein Programm, das zumindest das Lesen und Verfassen von E-Mails erlaubt. Viele MUAs können dem Benutzer natürlich auch in anderen Bereichen nützlich sein, unter anderem bei der Abfrage von Nachrichten über die POP- oder IMAP-Protokolle, der Einrichtung von Mailboxen zum Speichern der Nachrichten oder bei der Übergabe neuer Mitteilungen an einen MTA.

MUAs können sowohl grafisch sein, wie **Mozilla Mail**, oder auch eine sehr einfache text-basierte Schnittstelle haben, wie `mutt` oder `pine`.

11.3. Mail Transport Agents

Red Hat Linux enthält zwei primäre MTAs, Sendmail und Postfix. Sendmail ist als Default-MTA konfiguriert. Es ist allerdings recht einfach den Default-MTA auf Postfix umzustellen.

Tipp

Informationen darüber, wie Sie den standardmäßigen MTA von Sendmail auf Postfix umschalten können, finden Sie im Kapitel *Konfiguration des Mail Transport Agent (MTA)* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

Red Hat Linux enthält zusätzlich einen weiteren speziellen MTA, Fetchmail, welcher dazu verwendet wird E-Mails von einem Remote MTA zu einem lokalen MTA zu übermitteln.

Dieser Abschnitt behandelt Sendmail und Fetchmail.

11.3.1. Sendmail

Die Hauptaufgabe von Sendmail, wie anderen MTAs, besteht darin, unter Verwendung des SMTP-Protokolls E-Mails sicher zwischen Rechnern zu übertragen. Sendmail ist sehr gut zu konfigurieren, und Sie können fast jeden Schritt beim Versenden einer E-Mail verfolgen, einschließlich des hierzu verwendeten Protokolls. Viele Systemadministratoren wählen Sendmail als deren MTA, wegen seiner Funktionalität und Skalierbarkeit.

11.3.1.1. Ziele und Einschränkungen

Es ist wichtig zu wissen, was mit Sendmail möglich oder nicht möglich ist. Da die heutigen monolitischen Applikationen vielfältige Aufgaben erfüllen, gehen Sie nämlich vielleicht davon aus, dass Sendmail die einzige Applikation ist, die Sie zum Ausführen eines Mail-Servers auf Ihrem System benötigen. Technisch betrachtet ist dies auch richtig, da die Sendmail E-Mails in Ihr Benutzerverzeichnis speichern kann. Die meisten Benutzer benötigen jedoch mehr als nur eine Applikation, die Mails liefert. Sie möchten doch mit Ihrer E-Mail interagieren und verwenden dazu den E-Mail-Client, der zum Herunterladen von Mitteilungen auf den lokalen Rechner POP oder IMAP verwendet. Oder Sie bevorzugen für den Zugriff auf Ihre Mailbox eine Web-Schnittstelle. Diese anderen Applikationen können in Verbindung mit Sendmail und SMTP arbeiten, wurden aber aus anderen Gründen entwickelt und können unabhängig voneinander angewendet werden.

Es würde den Rahmen dieses Kapitels sprengen, hier im einzelnen auszuführen, wie Sendmail konfiguriert werden sollte oder kann. Hunderte verschiedener Optionen und Vorschriften werden in ganzen Büchern abgehandelt, die ebenfalls alles erklären und dabei helfen, Probleme zu lösen. Sehen Sie die Abschnitt 11.6 für eine List der Ressourcen zu Sendmail.

Sie sollten allerdings wissen, welche Dateien standardmäßig mit Sendmail installiert werden und auch darüber Bescheid wissen, wie Änderungen der Basiskonfiguration vorgenommen werden. Außerdem sollten Sie wissen, wie Sie unerwünschte E-Mails stoppen und wie Sie Sendmail mit dem *Lightweight Directory Access Protocol (LDAP)* erweitern können.

11.3.1.2. Die standardmäßige Installation von Sendmail

Die ausführbare Sendmail-Datei ist `/usr/sbin/sendmail`.

Die lange und detaillierte Konfigurationsdatei von Sendmail ist `/etc/mail/sendmail.cf`. Sie sollten die `sendmail.cf`-Datei nicht direkt bearbeiten. Um Änderungen an der Konfiguration von Sendmail vorzunehmen, bearbeiten Sie stattdessen die `/etc/mail/sendmail.mc`-Datei, sichern Sie das Original `/etc/mail/sendmail.cf.` und benutzen Sie dann den `m4`-Makroprozessor, um eine neue `/etc/sendmail.cf` zu erstellen. Weiter Informationen zur Konfiguration von Sendmail finden Sie im Abschnitt 11.3.1.3.

Im `/etc/mail/`-Verzeichnis sind verschiedene Sendmail-Konfigurationsdateien installiert, unter anderem:

- `access` — Legt fest, welche Systeme Sendmail für die Weitergabe von E-Mails verwenden kann.
- `domaintable` — Erlaubt Ihnen das Mapping von Domain-Names.
- `local-host-names` — Die Datei, die alle Alias-Namen für den Host enthält.
- `mailertable` — Bestimmt die Anweisungen, die das Routing für bestimmte Domain aufheben.
- `virtusertable` — Erlaubt Ihnen die Domain-spezifische Vergabe von Alias-Namen, wodurch mehrere virtuelle Domains auf einem Rechner gehostet werden können.

Einige der Konfigurationsdateien in `/etc/mail/`, wie z.B. `access`, `domaintable`, `mailertable` und `virtusertable`, müssen Ihre Informationen eigentlich in Datenbanken speichern, bevor Sendmail die Änderungen der Konfiguration verwenden kann. Um alle an den Konfigurationen durchgeführten Änderungen in die Datenbankdateien miteinzubeziehen, müssen Sie daher folgenden Befehl ausführen:

```
makemap hash /etc/mail/<name> < /etc/mail/<name>
```

wobei <*name*> der Name der zu konvertierenden Konfigurationsdatei ist.

Wenn Sie z.B. möchten, dass alle E-Mails, die an die `example.com`-Domain adressiert sind, an <`bob@other-example.com`> geschickt werden sollen, müssen Sie der Datei `virtusertable` die folgenden Zeile hinzufügen:

```
@example.com      bob@other-example.com
```

Um die Änderungen abzuschliessen, muss die Datei `virtusertable.db` aktualisiert werden. Führen Sie dazu folgenden Befehl als root aus:

```
makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable
```

Dadurch wird eine neue `virtusertable.db` erstellt, die dann die neue Konfiguration enthält.

11.3.1.3. Typische Änderungen der Sendmail-Konfiguration

Zur Änderung der Konfigurations-Datei von Sendmail erstellen Sie am besten eine völlig neue `/etc/sendmail.cf`-Datei, anstatt die bereits bestehende Datei zu bearbeiten.

Achtung

Bevor Sie die `sendmail.cf`-Datei verändern, sollten Sie eine Sicherungsdatei dieser anlegen.

Um die gewünschten Funktionen Sendmail hinzuzufügen, müssen Sie die `/etc/mail/sendmail.mc`-Datei bearbeiten. Wenn Sie fertig sind, verwenden Sie den `m4`-Makroprozessor, um eine neue `sendmail.cf` mit Hilfe des `m4 /etc/mail/sendmail.mc > /etc/sendmail.cf`-Befehls zu erstellen. Nach der Erstellung einer neuen `/etc/sendmail.cf`, müssen Sie Sendmail neu starten, damit die Änderungen übernommen werden. Geben Sie hierzu einfach als root den Befehl `/sbin/service sendmail restart` ein.

Der `m4`-Makroprozessor wird standardmäßig mit Sendmail installiert ist aber im `m4`-Paket enthalten.

Wichtig

Die Standard-`sendmail.cf`-Datei ermöglicht es Sendmail nicht, Netzwerkverbindungen, die nicht vom eigenen Rechner kommen, zu akzeptieren. Wenn Sie also Sendmail als Server auch für andere Clients konfigurieren möchten, bearbeiten Sie hierzu bitte `/etc/mail/sendmail.mc` und ändern Sie `DAEMON_OPTIONS`, um so auch auf Netzwerkgeräte zu reagieren, oder schreiben Sie diese Option ganz aus. Stellen Sie dann `/etc/sendmail.cf` mit der Ausführung folgenden Befehls wieder her:

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

Diese Konfiguration müsste auf den meisten Seiten, die ausschließlich SMTP verwenden, funktionieren. Sie funktioniert allerdings ganz sicher *nicht* auf UUCP (UNIX auf UNIX Copy)-Seiten. In diesen Fällen müssen Sie eine neue `sendmail.cf` erstellen, wenn Sie UUCP-Mail-Übertragungen verwenden müssen.

Sie sollten sich die Datei `/usr/share/sendmail-cf/README` anschauen, bevor Sie irgendeine Datei der Verzeichnisse unter dem `/usr/share/sendmail-cf`-Verzeichnis bearbeiten, weil diese Auswirkungen darauf haben können, wie die späteren `/etc/mail/sendmail.cf`-Dateien konfiguriert werden.

11.3.1.4. Masquerading

Eine gängige Sendmail-Konfiguration ist, dass ein einzelner Rechner für alle Rechner im Netzwerk als Mail-Gateway eingesetzt wird. Zum Beispiel hat ein Unternehmen einen Rechner mit dem Namen

`mail.bigcorp.com`, der alle Mails abwickelt und aller ausgehenden Post eine einheitliche Rücksendeadresse zuordnet.

In dieser Situation muss der Sendmail-Server die Rechnernamen auf dem Firmennetzwerk verdecken, so dass deren Rücksendeadresse user@bigcorp.com statt user@devel.bigcorp.com lautet.

Fügen Sie hierzu folgende Zeilen zu `/etc/mail/sendmail.mc` hinzu:

```
FEATURE(always_add_domain)dnl
FEATURE('masquerade_entire_domain')
FEATURE('masquerade_envelope')
FEATURE('allmasquerade')
MASQUERADE_AS('bigcorp.com.')
MASQUERADE_DOMAIN('bigcorp.com.')
MASQUERADE_AS(bigcorp.com)
```

Nach Erstellen eines neuen `sendmail.cf` anhand von `m4`, gibt diese Konfiguration vor, dass sämtliche Post innerhalb des Netzwerkes von `bigcorp.com` aus gesandt wurde.

11.3.1.5. Verhindern von Spam

Spam oder Junkmails sind überflüssige und unerwünschte E-Mails, deren Absender der Benutzer nicht kennt und die er auch niemals angefordert hat. Das ist ein störender, kostspieliger, aber weitverbreiteter Missbrauch des Standards zur Internet-Kommunikation.

Mit Sendmail ist es relativ einfach, neue Junkmail-Techniken, die zum Versenden von Junkmails eingesetzt sind, zu blockieren. Die meisten üblichen Junkmail-Methoden werden sogar mit der Standardkonfiguration blockiert.

Das Weiterleiten von SMTP-Nachrichten, auch *SMTP relaying* genannt, wurde standardmäßig mit Version 8.9 deaktiviert. Ohne diese Deaktivierung hätte Sendmail Ihren Mail-Host (`x.org`) angewiesen, Nachrichten von einem Teilnehmer anzunehmen (`y.com`) und sie an einen anderen Teilnehmer (`z.net`) weiterzuleiten. Mittlerweile müssen Sie Sendmail aber ausdrücklich anweisen, einer Domain zu erlauben, Mails über Ihre Domain weiterzuleiten. Um diese Änderung zu aktivieren, müssen Sie die `/etc/mail/relay-domains`-Datei bearbeiten und Sendmail neu zu starten.

Trotzdem kann es häufig vorkommen, dass Ihre Benutzer nach wie vor von Junkmail von anderen Servern über das Internet bombardiert werden, die Sie nicht kontrollieren können. In diesen Fällen können Sie die Zugriffskontrollfeatures, die Ihnen in der `/etc/mail/access`-Datei zur Verfügung stehen, einsetzen. Fügen Sie als root die Domains hinzu, mit denen Sie den Zugriff blockieren oder ausdrücklich zulassen möchten, wie in diesem Beispiel:

```
badspammer.com        ERROR:550 "Go away and do not spam us anymore"
tux.badspammer.com    OK
10.0                  RELAY
```

Dieses Beispiel macht deutlich, dass jede E-Mail, die von `badspammer.com` geschickt wurde, mit einem 550 RFC821-Fehlercode blockiert und zum Absender der Junkmail zurückgeschickt wird, bis auf die E-Mail, die von der Sub-Domain `tux.badspammer.com` kam und akzeptiert wurde. In der letzten Zeile wird angezeigt, dass alle E-Mails, die vom 10.0.*.* Netzwerk geschickt wurden, über Ihren Mail-Server weitergeleitet werden können.

Da `/etc/mail/access.db` eine Datenbank ist, verwenden Sie stets `makemap`, damit die Änderungen in Kraft treten. Geben Sie hierzu den folgenden Befehl als root ein:

```
makemap hash /etc/mail/access < /etc/mail/access
```

Dieses Beispiel geht nicht wirklich tief in die Möglichkeiten von Sendmail ein, was das Blockieren von Zugriff betrifft. Sehen Sie die Datei `/usr/share/doc/sendmail/README.cf` für weitere Informationen und Beispiele.

Da Sendmail den Procmail MDA zur Zustellung von Mails aufruft, ist es auch möglich einen Spam-Filter, wie SpamAssassin, zu verwenden, um Spam für Benutzer zu identifizieren und entsprechend zu handhaben. Sehen Sie Abschnitt 11.4.2.6 für Informationen zu SpamAssassin.

11.3.1.6. Verwenden von Sendmail mit LDAP

Die Verwendung des *Lightweight Directory Access Protocol (LDAP)* ist eine schnelle und wirkungsvolle Möglichkeit, um genauere Informationen über einen bestimmten Benutzer aus einer größeren Gruppe zu erhalten. Sie können z.B. den LDAP-Server benutzen, um eine E-Mail-Adresse aus einem Verzeichnis zu finden, das von einer Firma benutzt wird. In diesem Punkt besteht ein großer Unterschied zu Sendmail: Mit LDAP speichern Sie hierarchische Benutzerinformationen, Sendmail zeigt die Resultate von LDAP bei der Suche nach voradressierten E-Mails.

Sendmail unterstützt jedoch andererseits eine großzügigere Implementation mit LDAP immer dann, wenn es LDAP verwendet, um einzelne Dateien, wie z.B. `aliases` und `virtusertables` auf den verschiedenen Mail-Servern auszutauschen, die zusammenarbeiten, um mittlere bis größere Unternehmensorganisationen zu unterstützen. Kurz gesagt, Sie können LDAP verwenden, um den Mail-Routing-Level von Sendmail und dessen einzelne Konfigurationsdateien in einen leistungsfähigen LDAP-Cluster zu übertragen, der durch viele verschiedene Applikationen verbessert wurde.

Die aktuelle Version von Sendmail enthält Support für LDAP. Um Ihren Sendmail-Server mit LDAP zu erweitern, installieren und konfigurieren Sie zunächst einmal einen LDAP-Server, wie z.B. **OpenLDAP** Dann müssen Sie Ihre `/etc/mail/sendmail.mc` bearbeiten um Folgendes einzufügen:

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

Anmerkung

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

Unter `/usr/share/doc/sendmail/README.cf` erhalten Sie genaue Anweisungen und Beispiele für die RoutingKonfiguration von LDAP.

Erstellen Sie als nächstes `/etc/sendmail.cf` neu, indem Sie `m4` ausführen und Sendmail neu starten. Unter Abschnitt 11.3.1.3 finden Sie hierzu die entsprechenden Anweisungen.

Weitere Informationen zu LDAP finden Sie unter Kapitel 13.

11.3.2. Fetchmail

Fetchmail ist ein MTA, der E-Mails von Remote-Servern holen, und zum lokalen MTA übertragen kann. Viele Benutzer schätzen es, dass das Herunterladen ihrer Mitteilungen von einem Remote-Server und das Lesen und Sortieren ihrer E-Mails in einem E-Mail-Client voneinander getrennt werden kann. Fetchmail wurde für die Bedürfnisse von Dial-up Benutzern entwickelt. Mit Fetchmail

können unter Verwendung aller Protokolle, einschließlich POP3 und IMAP, alle Ihre E-Mails schnell mit Ihrer Mail-Spool-Datei verbunden und heruntergeladen werden. Bei Bedarf können Ihre E-Mail Mitteilungen auch an einen SMTP-Server weitergeleitet werden.

Fetchmail wurde für jeden Benutzer mit einer `.fetchmailrc`-Datei im Home-Verzeichnis des Benutzers konfiguriert.

Mit den Präferenzen der `.fetchmailrc`-Datei überprüft Fetchmail E-Mails auf einem Remote-Rechner, lädt diese herunter und versucht sie an Port 25 des lokalen Rechners zu übertragen. Dabei verwendet es den lokalen MTA, um die E-Mail in die richtige Spool-Datei des Benutzers zu platzieren. Wenn Procmail zur Verfügung steht, können Sie es dazu verwenden, die E-Mail zu filtern und in einer Mailbox zu platzieren, so dass sie dort von einem E-Mail-Client gelesen werden kann.

11.3.2.1. Konfigurationsoptionen bei Fetchmail

Obwohl es möglich ist, alle Optionen für die notwendige Überprüfung von E-Mails auf einem Remote-Server bei der Ausführung von Fetchmail über die Befehlszeile auszuführen, ist die Verwendung der Datei `.fetchmailrc` wesentlich einfacher. All Ihre Konfigurationsdateien werden in der Datei `.fetchmailrc` gespeichert. Sie können diese aber auch während der Ausführung von Fetchmail übergehen, indem Sie die entsprechende Option in der Befehlszeile festlegen.

Die Benutzerdatei `.fetchmailrc` ist in drei bestimmte Arten von Konfigurationsoptionen unterteilt:

- *global options* — Gibt Fetchmail Anweisungen, die die Vorgänge des Programms kontrollieren oder erstellt Einstellungen für jede Verbindung, die E-Mails kontrolliert, zur Verfügung.
- *server options* — Spezifiziert die notwendigen Informationen über den gewählten Server, wie z.B. den Hostnamen oder die Präferenzen, die Sie bei einem bestimmten E-Mail-Server sehen möchten, z.B. der zu prüfende Port oder die Sekunden bis zur Zeitüberschreitung. Diese Optionen wirken sich auf jede Benutzeroption aus, die mit diesem Server verwendet wird.
- *user options* — Enthält Informationen wie z.B. Benutzername und Passwort, die zur Authentifizierung und Überprüfung von E-Mails benötigt werden.

Die allgemeinen Optionen befinden sich am Anfang der `.fetchmailrc`-Datei, gefolgt von einer oder mehreren Server-Optionen, wobei jede dieser Optionen einen anderen, von Fetchmail zu prüfenden E-Mail-Server bezeichnet. Danach folgen die Benutzeroptionen jedem Benutzeraccount, den Sie auf diesem E-Mail-Server prüfen möchten. Genau wie die Serveroptionen können auch mehrere Benutzeroptionen für die Verwendung auf einem bestimmten Server festgelegt werden, so als würden Sie mehrere E-Mail-Accounts auf ein und demselben Server prüfen wollen.

Die Serveroptionen werden mit einem speziellen Optionsverb `poll` oder `skip`, das jeder Serverinformation vorangestellt wird, in der `.fetchmailrc`-Datei eingebunden. Die `poll`-Aktion weist Fetchmail an, diese Serveroption zu verwenden, wenn es ausgeführt wird. Damit werden E-Mails unter Verwendung verschiedener Benutzeroptionen überprüft. Nach der `skip`-Aktion werden die Serveroptionen allerdings so lange nicht überprüft, bis Sie den Hostnamen des Servers eingeben, während Fetchmail abgerufen wird. Die `skip`-Option erlaubt es Ihnen, in `.fetchmailrc` Testkonfigurationen einzustellen und unter Verwendung dieses Services nur dann Überprüfungen vorzunehmen, wenn dies ausdrücklich gewünscht wird. Dies hat keine Auswirkung auf die aktuell ausgeführten Konfigurationen.

Eine Muster-`.fetchmailrc`-Datei sieht wie folgt aus:

```
set postmaster "user1"
set bouncemail

poll pop.domain.com proto pop3
     user 'user1' there with password 'secret' is user1 here

poll mail.domain2.com
```

```
user 'user5' there with password 'secret2' is user1 here
user 'user7' there with password 'secret3' is user1 here
```

In diesem Beispiel sind allgemeine Optionen eingestellt. Der Benutzer verschickt E-Mails als letzten Ausweg (`postmaster`-Option) und alle E-Mail-Fehler werden statt zum Absender zum Postmaster geschickt (`bouncEmail`-Option). Die `set`-Aktion teilt Fetchmail mit, dass diese Zeile eine allgemeine Option enthält. Weiterhin sind zwei E-Mail-Server festgelegt. Einer verwendet zum Überprüfen POP3, der andere sucht ein funktionierendes Protokoll. Zwei Benutzer werden mit der zweiten Serveroption überprüft, es werden jedoch alle gefundenen E-Mails für alle Benutzer an die Mail-Spool des ersten Benutzers geschickt. Daraus ergibt sich die Möglichkeit, mehrere Mailboxen, die in einer einzigen E-Mail-Client-Inbox erscheinen, auf mehreren Servern zu kontrollieren. Jede spezifische Benutzerinformation beginnt mit der `user` Aktion.

Anmerkung

Benutzer müssen ihr Passwort nicht in der Datei `.fetchmailrc` angeben. Ein Auslassen des Abschnitts `with password '`*`password`*`'` hat zur Folge, das Fetchmail beim Starten nach dem Passwort fragt.

Fetchmail enthält viele verschiedene allgemeine, Server- und lokale Optionen. Viele dieser Optionen werden selten oder in ganz bestimmten Situationen verwendet. Die `fetchmail` man-Seite erklärt jede dieser Optionen im Detail. Die häufigsten sind hier aufgeführt.

11.3.2.2. Allgemeine Optionen

Jede allgemeine Option sollte nach einer `set`-Aktion in einer einzelnen Zeile platziert werden.

- `daemon` <*`seconds`*> — Weist Fetchmail an, automatisch den Daemon-Modus zu verwenden, der im Hintergrund in festgelegten Intervallen Mails abruft.
- `postmaster` — Weist Fetchmail einen lokalen Benutzer zu, der bei Problemen mit der Zustellung, benachrichtigt wird.
- `syslog` — Gibt die Log-Datei für Fehler- und Status-Meldungen an. Standardmäßig ist dies `/var/log/maillog`.

11.3.2.3. Serveroptionen

Schreiben Sie die Serveroptionen nach einer `poll` oder `skip`-Aktion in eine eigene Zeile in der Datei `.fetchmailrc`.

- `auth` <*`auth-type`*> — Bezeichnet den Typ der Authentifizierung. Standardmäßig wird die `password`Authentifizierung benutzt, aber einige Protokolle unterstützen andere Authentifizierungstypen, unter anderem `kerberos_v5`, `kerberos_v4` und `ssh`. Bei Verwendung der `any`-Authentifizierung wird Fetchmail zunächst versuchen, ohne Passwort zu arbeiten, danach nach Methoden, die ein Passwort benötigen, suchen und schließlich Ihr volles Passwort zur Authentifizierung an den Server schicken.
- `interval` <*`number`*> — Weist Fetchmail an, mit diesem Server regelmäßig nach einer festgelegten Zeit <*`Nummer`*> auf allen Servern nach Mails zu suchen. Diese Option wird bei Servern verwendet, auf denen Sie selten Mitteilungen erhalten.
- `port` <*`Port-Nummer`*> — Übergeht die Standard-Portnummer für ein bestimmtes Protokoll.

- `proto <protocol>` — Weist Fetchmail an, ein bestimmtes Protokoll zu verwenden, wie z.B. `pop3` oder `imap`, um auf diesem Server nach Mails zu suchen.
- `timeout <seconds>` — Konfiguriert Fetchmail so, dass es nicht weiter ausgeführt wird, wenn der Server für eine bestimmte Zeit inaktiv ist. Wenn dieser Wert nicht eingestellt wird, wird von ein Standard von `300` Sekunden ausgegangen.

11.3.2.4. Benutzeroptionen

Benutzeroptionen können in eine eigenen Zeile unterhalb einer Serveroption geschrieben werden. In beiden Fällen folgt die Benutzeroption der `user`-Option (nachstehend definiert).

- `fetchall` — Weist Fetchmail an, alle Mitteilungen in der Warteschlange herunterzuladen, einschließlich der Mitteilungen, die bereits angezeigt wurden. Standardmäßig ruft Fetchmail nur neue Mitteilungen ab.
- `fetchlimit <Nummer>` — Erlaubt nur das Abrufen einer bestimmten Anzahl von Mitteilungen, bevor es angehalten wird.
- `flush` — Weist Fetchmail an, alle bereits gelesenen Mitteilungen in der Warteschlange zu löschen, bevor neue Mitteilungen abgerufen werden.
- `limit <max-number-bytes>` — Ermöglicht es Ihnen festzulegen, dass nur Mitteilungen bis zu einer bestimmten Größe abgefragt werden. Diese Option ist für langsam arbeitende Netzwerk-Links vorteilhaft, wenn umfangreiche Mitteilungen zu viel Zeit beim Herunterladen in Anspruch nehmen würden.
- `password '<Passwort>'` — Gibt das Passwort an, das vom Benutzer benutzt wird.
- `preconnect "<command>"` — Weist Fetchmail an, den Befehl auszuführen, bevor Mitteilungen für diesen Benutzer abgefragt werden.
- `postconnect "<command>"` — Weist Fetchmail an, den Befehl auszuführen, nachdem Mitteilungen für diesen Benutzer abgefragt wurden.
- `ssl` — Aktiviert SSL-Verschlüsselung.
- `user "<username>"` — Stellt den von Fetchmail verwendeten Benutzernamen ein, um Mitteilungen abzurufen. *Diese Option sollte als erste, vor allen anderen Benutzeroptionen, aufgelistet sein.*

11.3.2.5. Fetchmail Befehls-Optionen

Die meisten Optionen von Fetchmail können in der Befehlszeile verwendet werden, wenn der Befehl `fetchmail` ausgeführt wird. Dabei werden die Konfigurationsoptionen von `.fetchmailrc` wiedergegeben. Dies dient dazu, Fetchmail sowohl mit als auch ohne Konfigurationsdatei zu verwenden. Die meisten Benutzer verwenden diese Optionen nicht in der Befehlszeile, weil es einfacher ist, die Optionen in der Datei `.fetchmailrc` zu belassen, um sie dort immer dann zu verwenden, wenn Fetchmail ausgeführt wird.

Eventuell möchten Sie jedoch gelegentlich den `fetchmail`-Befehl mit anderen Optionen für bestimmte Zwecke benutzen. Da alle Optionen, die in der Befehlszeile festgelegt sind, die Optionen der Konfigurationsdatei übergehen, können Sie auch mit den Befehlsoptionen die `.fetchmailrc`-Einstellungen vorübergehend übergehen, die zu einem Fehler führt.

11.3.2.6. Informations- oder Debugging-Optionen

Bestimmte Optionen, die nach dem `fetchmail`-Befehl verwendet werden, können wichtige Informationen für Sie enthalten.

- `--configdump` — Zeigt jede mögliche Option an, die auf den Informationen von `.fetchmailrc` und Fetchmail-Standards beruhen. Mit dieser Option kann kein Benutzer E-Mails abrufen.
- `-s` — Führt Fetchmail im Silent-Modus aus und verhindert, dass außer Fehlermeldungen sonst keine Mitteilungen angezeigt werden, nachdem der `fetchmail`-Befehl ausgeführt wurde.
- `-v` — Führt Fetchmail im Verbose-Modus aus. die gesamte Kommunikation zwischen Fetchmail und den Remote-E-Mail-Servern wird angezeigt.
- `-V` — Veranlasst Fetchmail, detaillierte Informationen der Version anzuzeigen, listet allgemeine Optionen auf und zeigt Einstellungen an, die von jedem Benutzer verwendet werden, einschließlich des E-Mail-Protokolls und der Authentifizierungsmethode. Bei dieser Option können von keinem Benutzer E-Mails abgerufen werden.

11.3.2.7. Spezielle Optionen

Diese Optionen sind gelegentlich hilfreich, wenn Standards, die in der `.fetchmailrc`-Datei gefunden wurden, aufgehoben wurden.

- `-a` — Weist Fetchmail an, alle neuen oder bereits gesehenen Mitteilungen vom Remote-E-Mail-Server herunterzuladen. Standardmäßig lädt Fetchmail nur neue Nachrichten.
- `-k` — Veranlasst Fetchmail, die Mitteilungen auf dem Remote-E-Mail-Server zu belassen, nachdem sie heruntergeladen worden sind. Diese Option übergeht das Standardverhalten des Löschens von Mitteilungen nach dem Herunterladen.
- `-l` *<max-number-bytes>* — Weist Fetchmail an, keine Mitteilungen herunterzuladen, die eine bestimmte Größe überschreiten, und diese stattdessen auf dem Remote-E-Mail-Server zu belassen.
- `--quit` — Beendet den Fetchmail-Daemon-Prozess.

Weitere Befehle und `.fetchmailrc`-Optionen finden Sie auf der `fetchmail` man-Seite.

11.4. Mail Delivery Agents

Red Hat Linux enthält zwei primäre MDAs, Procmail und `mail`. Beide dieser Applikationen werden als lokale Zustellungsagenten (Delivery Agents) bezeichnet und beide verschieben E-Mails von der Spool-Datei des MTA in die Mailbox des jeweiligen Benutzers. Procmail bietet allerdings ein robustes Filter-System.

Dieser Abschnitt behandelt lediglich Procmail. Für Informationen zu `mail`, sehen Sie dessen man-Seite.

Procmail filtert und stellt E-Mails zu, sobald diese in die Spool-Datei auf dem localhost eingehen. Es ist sehr umfangreich, nimmt nur wenige System-Ressourcen in Anspruch und ist weitverbreitet. Procmail kann eine kritische Rolle in der Zustellung von E-Mails übernehemen, die von E-Mail Client-Applikationen gelesen werden.

Procmail kann auf verschiedene Weise aufgerufen werden. Procmail kann so konfiguriert werden, dass wenn ein MTA eine neue EMail in Ihrer Spool-Datei ablegt, Procmail diese filtert, am für den E-Mail-Client entsprechend konfigurierten Ort ablegt und beendet. Ihr E-Mail-Client kann aber auch so konfiguriert werden, dass Procmail immer dann gestartet wird, wenn Mitteilungen eingegangen sind und diese Mitteilungen jeweils in die korrekte Mailbox geleitet werden. Häufig wird Procmail

durch die `.procmailrc`-Datei im Homeverzeichnis des Benutzers aufgerufen, wenn MTA eine neue E-Mail erhält.

Procmail ist von Anweisungen bestimmter *recipes* oder auch Regeln abhängig, die Mitteilungen mit dem Programm vergleichen. Wenn eine Mitteilung mit den Erfordernissen übereinstimmt, wird die E-Mail in einer bestimmten Datei abgelegt, gelöscht oder anderweitig bearbeitet.

Wenn Procmail startet, liest es die E-Mail und unterteilt sie in Hauptinformationen und Kopfzeilen-Informationen. Danach sucht Procmail standardmäßig im ganzen System nach der `/etc/procmailrc`-Datei und den `rc`-Dateien im `/etc/procmailrcs`-Verzeichnis nach Umgebungsvariablen und Recipes. Anschließend sucht Procmail nach einer `.procmailrc`-Datei im Homeverzeichnis des Benutzers, um Regeln zu finden, die für diesen Benutzer speziell bestimmt sind. Viele Benutzer erstellen auch eigene zusätzliche `rc`-Dateien für Procmail, die sich auf ihre `.procmailrc`-Datei beziehen. Diese können schnell ein- bzw. ausgeschaltet werden, wenn beim Filtern von Mails Probleme auftreten.

Standardmäßig gibt es keine systemweiten `rc`-Dateien im `/etc`-Verzeichnis und auch keine Benutzer-`.procmailrc`-Dateien. Wenn Sie Procmail das erste Mal benutzen, müssen Sie eine `.procmailrc`-Datei mit speziellen Umgebungsvariablen und Recipes erstellen, mit denen Sie festlegen, wie mit bestimmten Mitteilungen zu verfahren ist.

In den meisten Fällen hängt die Konfiguration von Procmail für das Filtern Ihrer E-Mail davon ab, ob eine `.procmailrc`-Benutzerdatei vorhanden ist. Um Procmail zu deaktivieren und Ihre Arbeit in der `.procmailrc`-Datei zu speichern, platzieren Sie Procmail mit dem `mv ~/.procmailrc ~/.procmailrcSAVE`-Befehl in eine Datei mit einem ähnlichen Namen. Wenn Sie Procmail dann erneut testen wollen, ändern Sie den Namen dieser Datei wieder in `.procmailrc`. Procmail steht Ihnen dann sofort wieder zur Verfügung.

11.4.1. Konfiguration von Procmail

Die Konfigurationsdateien von Procmail, insbesondere die Benutzerdatei `.procmailrc`, enthalten wichtige Umgebungsvariablen. Diese Variablen geben Procmail an, welche Mitteilungen sortiert werden sollen und wie mit den Mitteilungen verfahren werden soll, die nicht mit den Recipes übereinstimmen, usw.

Diese Umgebungsvariablen erscheinen normalerweise am Anfang der `.procmailrc`-Datei, und zwar im folgenden Format:

<env-variable>="*<value>*"

In diesem Beispiel ist *<env-variable>* der Name der Variablen, und der *<value>*-Bereich definiert sie.

Viele Umgebungsvariablen werden von den meisten Procmail-Benutzern nicht verwendet, und viele der wichtigsten Umgebungsvariablen sind bereits standardmäßig eingestellt. Sie werden meistens folgende Variablen verwenden:

- `DEFAULT` — Stellt die Standard-Mailbox ein, in der Mitteilungen, die mit keinem einzigen Recipe übereinstimmen, abgelegt werden.

  Der standardmäßige `DEFAULT`-Wert und `$ORGMAIL` stimmen überein.

- `INCLUDERC` — Bestimmt zusätzliche `rc`-Dateien, die weitere Recipes enthalten, die mit Mitteilungen verglichen werden müssen. Dadurch können Sie die Liste der Recipes fpr Procmail in verschiedene Dateien aufteilen, die unterschiedliche Aufgaben übernehmen, wie z.B. das Blockieren von Junkmail und die Verwaltung von E-Mail-Listen, die dann mit kommentierenden Zeilen in der Benutzerdatei `.procmailrc` ein- oder ausgeschaltet werden können.

  Zwei Zeilen in einer `.procmailrc`-Benutzerdatei sehen z.B. wie folgt aus:

  ```
  MAILDIR=$HOME/Msgs
  ```

```
INCLUDERC=$MAILDIR/lists.rc
INCLUDERC=$MAILDIR/spam.rc
```

Wenn der Benutzer das Filtern seiner E-Mails ausschalten will, die Junkmail-Kontrolle aber weiterhin aktiviert bleiben soll, kann er diese Option in der ersten INCLUDERC-Zeile ganz einfach mit dem [#]-Zeichen auskommentieren.

- LOCKSLEEP — Bestimmt die Zeitspanne - in Sekunden - innerhalb derer Procmail versucht, eine bestimmte Sperrdatei zu verwenden. Standardmäßig sind 8 Sekunden eingestellt.
- LOCKTIMEOUT — Stellt die Zeit ein, die nach der letzten Modifizierung einer Sperrdatei vergeht, bis Procmail davon ausgeht, dass sie alt ist und gelöscht werden kann. Standardmäßig sind 1024 Sekunden eingestellt.
- LOGFILE — Der Pfad und die Datei, die alle Informationen über Procmail sowie Fehlermeldungen enthält.
- MAILDIR — Stellt das aktuell ausgeführte Verzeichnis für Procmail ein. Ist es eingestellt, beziehen sich alle anderen Pfade in Procmail auf dieses Verzeichnis.
- ORGMAIL — Legt die ursprüngliche Mailbox oder andere Orte fest, an denen Mitteilungen abgelegt werden können, wenn sie nicht in der standardmäßigen oder recipe-mäßigen Stelle platziert werden können.

  Standardmäßig wird der /var/spool/mail/$LOGNAME Wert verwendet.
- SUSPEND — Legt die Zeit fest - in Sekunden - nach der Procmail stoppt, wenn die benötigten Ressourcen, z.B. ein Swap-Space, nicht zur Verfügung stehen.
- SWITCHRC — Ermöglicht einem Benutzer, eine externe Datei festzulegen, die zusätzliche Recipes enthält. Ähnlich wie die INCLUDERC-Option, aber mit der Ausnahme, dass die Konfigurationsdatei zur Zeit nicht überprüft wird und nur Recipes, die in der SWITCHRC-spezifischen Datei festgelegt sind, angewendet werden.
- VERBOSE — Weist Procmail an, viel mehr Informationen zu protokollieren. Diese Option eignet sich gut für das Debugging.

Weitere wichtige Umgebungsvariablen können Sie Ihrer Shell entnehmen, z.B. LOGNAME, Ihr Login-Name, HOME, die Speicherstelle Ihres Homeverzeichnisses und SHELL, Ihre Standard-Shell.

Eine vollständige Beschreibung aller Umgebungsvariablen sowie deren Werte finden Sie in der procmailrc man-Seite.

11.4.2. Procmail Recipes

Neue Benutzer empfinden den Aufbau der Recipes oft als den schwierigsten Teil im Umgang mit Procmail. Bei einigen Erweiterungen ist das verständlich, wenn die Mitteilungen z.B. anhand von *regulären Ausdrücken* (*regular expressions*) mit den Recipes verglichen werden. Dies ist ein besonderes Format, das die Bedingungen für einen Matching String festlegt. Reguläre Ausdrücke sind jedoch weder schwer zu erstellen noch schwer zu verstehen. Ungeachtet der regulären Ausdrücke ist aufgrund der Art und Weise, wie die Procmail Recipes geschrieben sind, einfach, herauszufinden, wie sie funktionieren.

Eine vollständige Beschreibung des regulären Umfangs würde den Rahmen dieses Kapitels sprengen. Die Struktur der Procmail Recipes ist viel wichtiger. Im Internet finden Sie unter anderem unter http://www.iki.fi/era/procmail/links.html hilfreiche Beispiele für Procmail Recipes. Die korrekte Verwendung und Anpassung der regulären Ausdrücke, die Sie in diesen Beispielen finden, hängt vom Verständnis der Struktur der Procmail Recipes ab. In der grep-man-Seite finden Sie einführende Informationen über die grundlegenden Regeln der regulären Ausdrücke.

Ein Procmail Recipe sieht wie folgt aus:

```
:0<flags>: <lockfile-name>
```

```
* <special-condition-character> <condition-1>
* <special-condition-character> <condition-2>
* <special-condition-character> <condition-N>

<special-action-character><action-to-perform>
```

Die ersten zwei Zeichen in einem Procmail Recipe sind ein Doppelpunkt und eine Null. Nach der Null können wahlweise verschiedene Flags platziert werden, um zu kontrollieren, was Procmail tut, wenn dieses Recipe bearbeitet wird. Ein Doppelpunkt nach dem Abschnitt <*Flags*> bestimmt, dass für diese Mitteilung eine Sperrdatei erstellt wird. Wenn diese Sperrdatei erstellt wird, geben Sie deren Namen in das <*Sperrdatei-Name*>-Feld ein.

Ein Recipe kann verschiedene Bedingungen für die Überprüfung einer Mitteilung enthalten. Sind keine Bedingungen enthalten, wird jede Mitteilung dem Recipe angepasst. Zur Vereinfachung eines Vergleichs mit einer Mitteilung werden in einigen Bedingungen reguläre Ausdrücke platziert. Wenn viele Bedingungen verwendet werden, müssen diese alle verglichen werden, bevor eine Aktion ausgeführt wird. Die Bedingungen werden auf der Grundlage der Flags überprüft, die in der ersten Zeile der Regel eingestellt wurden. Spezielle, wahlweise platzierte Zeichen nach dem `*`-Zeichen können die Bedingungen kontrollieren.

Die Option <*auszuführende Aktion*> legt fest, was mit einer Mitteilung passiert, die einer der Bedingungen entspricht. Pro Recipe wird nur eine Aktion ausgeführt. In vielen Fällen wird der Name der Mailbox verwendet, um die Mitteilungen in die Datei weiterzuleiten, die die E-Mails tatsächlich sortiert. Es können auch spezielle Zeichen für die Aktion verwendet werden, bevor diese festgelegt wird.

11.4.2.1. Delivering und Non-Delivering Recipes

Die Aktion, die ein Recipe beim Vergleichen einer bestimmten Mitteilung durchführt, legt fest, ob das Recipe liefert oder nicht liefert. Ein *Delivering Recipe* enthält eine Aktion, die eine Mitteilung in eine Datei schreibt, die Mitteilung an ein anderes Programm schickt oder an eine andere E-Mail-Adresse weiterleitet. Ein *Non-delivering Recipe* hingegen deckt alle anderen Aktion ab, wie z.B. das Verwenden eines Nesting-Blocks. Ein *Nesting-Block* ist eine Aktion in Klammern `{ }`, die zusätzliche Aktionen für Mitteilungen vorsieht, welche mit den Bedingungen der Recipes verglichen werden. Nesting Blocks können verschachtelt werden und bieten dadurch eine bessere Kontrolle zum Identifizieren und Ausführen von Aktionen in Mitteilungen.

Delivering Recipes, die Mitteilungen vergleichen, weisen Procmail an, eine bestimmte Aktion auszuführen und das Vergleichen der Mitteilungen mit anderen Recipes zu beenden. Mitteilungen, die den Bedingungen in Non-Delivering Recipes entsprechen, werden weiterhin in den aktuellen und folgenden `rc`-Dateien mit anderen Recipes verglichen. Mit anderen Worten: Non-Delivering Recipes bewirken, dass die Mitteilung weiterhin durch die Recipes kontrolliert wird, nachdem eine bestimmte Aktion eingestellt wurde.

11.4.2.2. Flags

Flags sind sehr wichtig, um festzulegen, wie und ob eine Mitteilung mit den Bedingungen des Recipes verglichen wird. Im allgemeinen werden folgende Flags verwendet:

- `A` — Legt fest, dass dieses Recipe nur verwendet wird, wenn das vorherige Recipe ohne ein `A`- oder `a`-Flag diese Mitteilung ebenfalls verglichen hat.

  Um sicherzustellen, dass der letzte Vergleich mit dem Recipe erfolgreich abgeschlossen wurde, verwenden Sie das `a`-Flag.

- `B` — Analysiert den Hauptteil der Mitteilung und sucht nach Matching-Bedingungen.

- b — Verwendet standardmäßig den Hauptteil der Mitteilung und die sich daraus ergebenden Aktionen, wie z.B. das Scheiben der Mitteilung in eine Datei oder das Weiterleiten der Mitteilung. Dies ist standardmäßig.
- c — Erstellt eine Kopie der E-Mail. Dies ist für die Delivering Recipes hilfreich, da die erforderlichen Aktionen in der Mitteilung ausgeführt und die Kopie weiterhin in den rc-Dateien verarbeitet werden kann.
- D — Macht den egrep Vergleich abhängig von Groß- und Kleinschreibung. Standardmäßig wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- E — Ähnelt dem A-Flag, mit dem Unterschied, dass die Bedingungen in diesem Recipe nur mit der Mitteilung verglichen werden und das vorherige Recipe ohne E-Flag die Mitteilung nicht verglichen hat. Dies ist vergleichbar mit der *else*-Aktion.

  Verwenden Sie stattdessen das e-Flag, wenn Sie nur dieses Recipe zum Überprüfen verwenden wollen und die Prüfung des vorherigen Recipes fehlgeschlagen ist.
- f — Verwendet die Pipe als Filter.
- H — Analysiert standardmäßig die Kopfzeile der Mitteilung und sucht nach Matching-Bedingungen.
- h — Verwendet standardmäßig die Kopfzeile bei einer Aktion.
- w — Weist Procmail an, auf einen bestimmten Filter oder Programm zu warten, der/das meldet, ob die vorangegangene Aktion erfolgreich war, bevor die Mitteilung gefiltert wird.

  Wenn Sie "Program failure" (Programmfehler) Meldungen ignorieren möchten, die erscheinen, wenn ein Filter oder eine Aktion nicht erfolgreich war, verwenden Sie stattdessen die W-Option.

Zusätzliche Flags finden Sie in der procmailrc-man-Seite.

11.4.2.3. Festlegen einer lokalen Sperrdatei

Sperrdateien sind für Procmail sehr hilfeich, um sicherzustellen, dass zur gleichen Zeit nicht mehr als ein Prozeß versucht, eine bestimmte Mitteilung zu ändern. Sie können eine lokale Sperrdatei festlegen, indem Sie nach jedem Flag in der ersten Zeile eines Recipes einen Doppelpunkt (:) setzen. Dadurch wird eine Sperrdatei erstellt, die auf dem Namen der Zieldatei und den Einstellungen der allgemeinen LOCKEXT-Umgebungsvariablen basiert.

Alternativ können Sie auch festlegen, dass der Name der lokalen Sperrdatei mit diesem Recipe nach dem Doppelpunkt verwendet wird.

11.4.2.4. Besondere Bedingungen und Aktionen

Bestimmte Zeichen, die vor den Procmail Recipe-Bedingungen und Aktionen verwendet werden, ändern die Art, wie diese interpretiert werden.

Die folgenden Zeichen können nach dem *-Zeichen, am Anfang einer Zeile mit den Recipe-Bedingungen verwendet werden:

- ! — Kehrt die Bedingungen um und verursacht ein Match für den Fall, dass die Bedingungen nicht mit der Mitteilung übereinstimmen.
- < — Prüft, ob die Mitteilung eine bestimmte Byte-Zahl unterschreitet.
- > — Prüft, ob die Mitteilung eine bestimmte Byte-Zahl überschreitet.

Folgende Zeichen werden verwendet, um spezielle Aktionen durchzuführen:

- ! — Weist Procmail an, die Mitteilung an die gegebenen E-Mail-Adressen weiterzuleiten.

- `$` — Verweist auf eine vorher in der Refers to `rc`-Datei eingestellte Variable. Dieses Zeichen wird üblicherweise verwendet, um eine allgemeine Mailbox einzustellen, die sich auf verschiedene Recipes bezieht.
- `|` — Das Pipe-Zeichen weist Procmail an, ein bestimmtes Programm zu starten, das diese Mitteilung verarbeitet.
- `{` and `}` — Erstellt einen Nesting-Block, der weitere Recipes zum Vergleichen mit der Mitteilung enthält.

Wenn am Beginn einer Zeile für eine Aktion kein spezielles Zeichen verwendet wird, geht Procmail davon aus, dass die Aktionszeile in der Mailbox festgelegt ist, in die die Mitteilung geschrieben sein sollte.

11.4.2.5. Recipe Beispiele

Procmail ist ein äußerst flexibles Programm, das es Ihnen erlaubt, Mitteilungen mit sehr spezifischen Bedingungen zu vergleichen und danach detaillierte Aktionen in diesen Mitteilungen ausführt. Aufgrund dieser Flexibilität kann das Erstellen eines Procmail Recipes zu einem bestimmten Zweck für neue Benutzer schwierig sein.

Der beste Weg, um bei der Erstellung von Procmail Recipe-Bedingungen Erfahrungen zu sammeln, ist das Verständnis für reguläre Ausdrücke sowie das Anschauen der Beispiele, die von anderen erstellt wurden. Die folgenden sehr einfachen Beispiele demonstrieren dei Struktur der Procmail Recipes und bilden die Grundlage für kompliziertere Konstruktionen.

Wie im folgenden Beispiel gezeigt, enthalten die meisten einfachen Recipes keine Bedingungen:

```
:0:
new-mail.spool
```

Die erste Zeile startet das Recipe und legt fest, dass eine lokale Sperrdatei erstellt werden muss, ohne den Namen dabei festzulegen. Procmail verwendet den Namen der Zieldatei und die `LOCKEXT`-Option zur Benennung der Datei. Es sind keine Bedingungen festgelegt, so dass jede Mitteilung mit diesem Recipe übereinstimmt und in der Spooldatei `new-mail.spool` abgelegt wird, die sich in dem Verzeichnis befindet, das von der Umgebungsvariablen `MAILDIR` festgelegt wird. Ein E-Mail-Client kann die Nachrichten in dieser Datei dann ansehen.

Dieses einfache Recipe kann bis zum Ende aller `rc`-Dateien gehen, um Mitteilungen zu einer standardmäßigen Location zu leiten. Bei einem komplizierteren Beispiel können Mitteilungen von einer bestimmten Adresse entnommen und entfernt werden, wie aus folgendem Beispiel hervorgeht.

```
:0
* ^From: spammer@domain.com
/dev/null
```

In diesem Beispiel werden alle von `spammer@domain.com` verschickten Mitteilungen an `/dev/null` weitergeleitet und dort gelöscht.

Achtung

Vergewissern Sie sich bei jeder Regel, dass sie richtig funktioniert, bevor Mitteilungen an `/dev/null` weitergeleitet werden, wo sie definitiv und endgültig gelöscht werden. Wenn Ihre Recipe-Bedingungen versehentlich eine korrekte Mitteilung empfangen, werden Sie nicht wissen, dass Sie diese Mitteilung erhalten haben, es sei denn, der Absender benachrichtigt Sie.

Es ist besser, wenn sich die Aktionen des Recipes auf eine spezielle Mailbox richten, die Sie von Zeit zu Zeit überprüfen können und nach *false positives* oder Mitteilungen suchen, die versehentlich

mit den Bedingungen verglichen wurden. Wenn Sie feststellen, dass versehentlich keine Mitteilungen überprüft wurden, können Sie die Mailbox löschen und die Aktion, Mitteilungen an `/dev/null` weiterzuleiten, wieder aktivieren.

Procmail wird primär als Filter von E-Mails benutzt, der als solcher diese automatisch an die richtige Stelle leitet und Sie die E-Mails nicht manuell sortieren müssen. Das folgende Recipe greift sich die E-Mails heraus, die von einer bestimmten Mailing-Liste gesendet wurden, und legt sie im richtigen Ordner ab.

```
:0:
* ^(From|CC|To).*tux-lug
tuxlug
```

Jede Mitteilung, die von der `tux-lug@domain.com`-Mailing-List verschickt wurde, wird automatisch für Ihren E-Mail-Client in der Mailbox `tuxlug` abgelegt. Bitte beachten Sie, dass die Bedingung in diesem Beispiel die Mitteilung danach überprüft, ob sich die E-Mail-Adresse der Mailing-Liste in den Zeilen `From`, `CC` oder `To` befindet.

Sehen Sie die zahlreichen Procmail Online-Ressourcen, Abschnitt 11.6, für genauere Beschreibungen und kompliziertere Recipes.

11.4.2.6. Spam Filters

Da es von Sendmail, Postfix oder Fetchmail aufgerufen wird, wenn eine neue E-Mail eintrifft, kann Procmail als mächtiges Tool gegen Spam verwendet werden.

Dies trifft vor allem zu, wenn Procmail zusammen mit SpamAssassin verwendet wird. Zusammen, können diese beiden Applikationen Spam E-Mails schnell erkennen, und diese Aussortieren oder Vernichten.

SpamAssassin verwendet Header-Analysis, Text-Analysis, Blacklists, und eine Spam-Tracking Datenbank um Spam richtig zu identifizieren und entsprechend zu markieren.

Der einfachste Weg für einen lokalen Benutzer SpamAssassin zu verwenden, ist die folgende Zeile im oberen Bereich der Datei `~/.procmailrc` einzufügen:

```
INCLUDERC=/etc/mail/spamassassin/spamassassin-default.rc
```

Die Datei `/etc/mail/spamassassin/spamassassin-default.rc` enthält eine einfache Procmail-Regel, die SpamAssassin für alle eingehenden E-Mails aktiviert. Wird eine E-Mail als Spam erkannt, wird diese im Header entsprechend markiert, und dem Titel der E-Mail wird Folgendes vorangestellt:

```
*****SPAM*****
```

Dem Body der Nachricht wird dies in den Abschnitten vorangestellt, die dazu geführt haben, dass diese E-Mail als Spam klassifiziert wurde.

Um als Spam markierte E-Mails abzulegen, kann eine Regel ähnlich der Folgenden verwendet werden:

```
:0 Hw
* ^X-Spam-Status: Yes
spam
```

Diese Regel legt alle als Spam markierten E-Mails in eine Mailbox mit dem Namen `spam`.

Da SpamAssassin ein Perl-Skript ist, kann es auf überfüllten Servern notwending werden den binären SpamAssassin Daemon (`spamd`) und die Client-Applikation (`spamc`) zu verwenden. Ein solches Konfigurieren von SpamAssassin, erfordert allerdings Root-Zugriff zum Host.

Um den `spamd` Daemon zu starten, geben Sie folgenden Befehl als root ein:

```
/sbin/service spamassassin start
```

Damit der SpamAssassin Daemon zur Bootzeit gestarten wird, müssen Sie mit einem Initscript-Utility, wie **Services-Konfigurationstool** (`redhat-config-services`), den Service `spamassassin` entsprechend einrichten. Sehen Sie Abschnitt 1.4.2 für weitere Informationen zu Initscript-Utilities.

Um Procmail für die Verwendung der SpamAssassin Client-Applikation anstelle des Perl-Skripts einzurichten, fügen Sie die folgende Zeile im oberen Bereich der Datei `~/.procmailrc` hinzu, oder, für eine System-weite Konfiguration, in die Datei `/etc/procmailrc`:

```
INCLUDERC=/etc/mail/spamassassin/spamassassin-spamc.rc
```

11.5. Mail User Agents

Unter Red Hat Linux gibt es eine vielzahl von Mail-Programmen. Es gibt graphische E-Mail-Clients, mit Unmengen an Funktionalität, wie **Mozilla Mail** oder **Ximian Evolution**, als auch Text-basierte E-Mail-Programme, wie **mutt** und **pine**.

Für Anleitungen zur Verwendung dieser Applikationen, sehen Sie das Kapitel *E-Mail-Applikationen* im *Red Hat Linux Handbuch Erster Schritte*.

Der Rest dieses Abschnitts geht auf die Sicherheit bei der Kommunikation zwichen Client und Server ein.

11.5.1. Sicherheit bei der Kommunikation

Bekannte MUAs, die Teil von Red Hat Linux sind, wie z.B. **Mozilla Mail**, `mutt`, und `pine`, gewährleisten SSL-verschlüsselte E-Mail-Sitzungen.

Wie alle anderen Dienste, die unverschlüsselte und wichige E-Mail-Informationen wie z.B. Benutzernamen, Passwörter und vollständige Mitteilungen über das Netzwerk verschicken, können diese Informationen auch ohne besondere Kenntnisse über Server oder Clients abgefangen und eingesehen werden. Bei der Verwendung der Standardprotokolle POP und IMAP werden alle Informationen über die Authentifizierung im "Klartext" übermittelt. Angreifer, die diese Informationen abfangen, können sich dadurch Zugriff zu diesen Accounts verschaffen.

11.5.1.1. Sichere E-Mail-Clients

Die meisten E-Mail-Clients in Linux kontrollieren E-Mails auf Remote-Servern und unterstützen SSL zum Verschlüsseln von Mitteilungen, wenn sie über ein Netzwerk verschickt werden. Um SSL beim Abfragen von E-Mails verwenden zu können, muss es auf dem E-Mail-Client und dem Server allerdings aktiviert sein.

SSL ist auf einem Client einfach zu aktivieren. Oft klickt man dazu lediglich auf einen Button im Konfigurationsbereich der E-Mail-Clients. Sichere IMAP und POP haben bekannte Portnummern (993 bzw. 995), die der E-Mail-Client verwendet, um Mitteilungen zu authentifizieren und herunterzuladen.

11.5.1.2. Sicherheit in E-Mail-Client Kommunikationen

Die Bereitstellung einer SSL-Verschlüsselung für IMAP und POP-Benutzer auf dem E-Mail-Servers ist recht einfach.

Zuerst müssen Sie ein SSL-Zertifikat erzeugen. Dies kann auf zwei verschiedene Weisen geschehen: Durch Anfordern eines SSL-Zertifikats bei der *Certificate Authority* (*CA*) oder durch Erzeugen eines eigensignierten Zertifikats.

Achtung

Eigensignierte Zertifikate sollten lediglich für Testzwecke verwendet werden. Jeder in einem Produktionsablauf verwendete Server sollte ein SSL-Zertifikat verwenden, das von der CA ausgestellt wurde.

Um ein eigensigniertes Zertifikat für IMAP zu erstellen, wechseln Sie in das `/usr/share/ssl/certs/`-Verzeichnis, und geben den folgenden Befehl als root ein:

```
make imapd.pem
```

Beantworten Sie alle Fragen um diesen Vorgang abzuschliessen.

Um ein eigensigniertes Zertifikat für POP zu erstellen, wechseln Sie in das `/usr/share/ssl/certs/`-Verzeichnis, und geben den folgenden Befehl als root ein:

```
make ipop3d.pem
```

Auch hier beantworten Sie alle Fragen um diesen Vorgang abzuschliessen.

Nach Abschluss verwenden Sie den Befehl `/sbin/service`, um den entsprechenden Daemon (`imaps` oder `pop3s`) zu starten. Richten Sie als nächstes den `imaps` oder `pop3s` Service so ein, dass dieser in den richtigen Runlevels startet, wozu Sie ein Initscript-Utility, wie **Services-Konfigurationstool** (`redhat-config-services`) verwenden können. Sehen Sie Abschnitt 1.4.2 für weitere Information zu Initscript-Utilities.

Alternativ, können Sie auch den Befehl `stunnel` als SSL-Verschlüsselungs-Wrapper auf die `imapd` und `pop3d` Daemons anwenden.

Das `stunnel`-Programm verwendet externe OpenSSL-Biblitotheken, die in Red Hat Linux enthalten sind, für eine leistungsfähige Verschlüsselung und zum Schutz Ihrer Verbindungen. Sie können ein SSL-Zertifikat bei der CA beantragen oder ein eigensigniertes erstellen.

Um ein eigensigniertes Zertifikat zu erstellen, wechseln Sie in das Verzeichnis `/usr/share/ssl/certs/` und geben den folgenden Befehl als root ein:

```
make stunnel.pem
```

Auch hier beantworten Sie alle Fragen, um diesen Vorgang abzuschliessen.

Nachdem das Zertifikat generiert wurde, ist es möglich, den Befehl `stunnel` zu verwenden, um den `imapd` Mail-Daemon zu starten. Benutzen Sie dazu folgenden Befehl:

```
/usr/sbin/stunnel -d 993 -l /usr/sbin/imapd imapd
```

Nach Ausführen dieses Befehls können Sie einen IMAP E-Mail-Client öffnen und mit Ihrem E-Mail-Server, der die SSL-Verschlüsselung verwendet, verbinden.

Um `pop3d` mit dem Befehl `stunnel` zu starten, geben Sie folgenden Befehl ein:

```
/usr/sbin/stunnel -d 993 -l /usr/sbin/pop3d pop3d
```

Weitere Informationen zur Verwendung von `stunnel` können Sie in der `stunnel` man-Seite oder in den Dokumenten des `/usr/share/doc/stunnel-<version-number>`-Verzeichnisses nachlesen.

11.6. Zusätzliche Informationsquellen

Die Folgende ist eine Liste zusätzlicher Dokumentation zu E-Mail-Applikationen.

11.6.1. Installierte Dokumentation

- Informationen über das Konfigurieren von Sendmail sind in den Paketen `sendmail` und `sendmail-cf` enthalten.
  - `/usr/share/doc/sendmail/README.cf` — Enthält Informationen über `m4`, die Dateispeicherstellen von Sendmail, unterstützte Mailer und den Zugang zu erweiterten Features, uvm.
  - `/usr/share/doc/sendmail/README` — Enthält Informationen über die Verzeichnisstruktur von Sendmail, den IDENT Protokoll-Support sowie Einzelheiten zu den Zugriffsrechten für die Verzeichnisse und die Probleme im Zusammenhang der falschen Konfiguration dieser Zugriffsrechte.

  Zusätzlich enthalten die `sendmail` und `aliases`-man-Seiten nützliche Informationen zu den verschiedenen Sendmail-Optionen und zur richtigen Konfiguration der Sendmail `/etc/mail/aliases`-Datei.
- `/usr/share/doc/fetchmail-<Versionsnummer>` — Enthält in der `FEATURES`-Datei eine komplette Liste der Features von Fetchmail sowie ein einführendes `FAQ`-Dokument.
- `/usr/share/doc/procmail-<Versionsnummer>` — Enthält eine `README`-Datei, die einen Überblick über Procmail gibt, eine `FEATURES`-Datei, die alle Programmfeatures erklärt, und eine `FAQ`-Datei mit Antworten zu den gängigen Fragen zur Konfiguration.

  Um zu verstehen, wie Procmail funktioniert und wie neue Recipes erstellt werden, sind die man-Seiten äußerst hilfreich:
  - `procmail` — Überblick über die Arbeitsweise von Procmail und die Schritte, die zum Filtern von E-Mails notwendig sind.
  - `procmailrc` — Erklärt das Format der `rc`-Datei, mit der Recipes erstellt werden.
  - `procmailex` — Bietet viele nützliche Beispiele aus der Praxis der Procmail-Recipes.
  - `procmailsc` — Erklärt die Weight-Scoring-Technik, die von Procmail verwendet wird, um festzustellen, ob ein bestimmtes Recipe mit einer bestimmten Nachricht übereinstimmt.
  - `/usr/share/doc/spamassassin-<version-number>/` — Dieses Verzeichnis enthält eine große Anzahl an Informationen im Bezug zu SpamAssassin. Ersetzen Sie `<version-number>` mit der Versionsnummer des `spamassassin`-Pakets.

11.6.2. Hilfreiche Webseiten

- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-Administrator-HOWTO.html — Bietet einen Überblick zur Funktionsweise von E-Mails und prüft mögliche E-Mail-Lösungen und E-Mail-Konfigurationen der Clients und Server.

- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-User-HOWTO/ — Betrachtet E-Mails aus der Perspektive des Benutzers, untersucht verschiedene bekannte E-Mail-Client-Applikationen und bietet eine Einführung für verschiedene Themen, wie Alias-Namen, Weiterleiten, Auto-Reply, Mailing-Listen, Mail-Filter und Junkmail.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Secure-POP+SSH.html — Zeigt, wie eine POP-E-Mail mit Hilfe von SSH und Port-Forwarding empfangen wird, so dass Ihre E-Mail-Passwörter und die Mitteilungen sicher übermittelt werden.
- http://www.sendmail.net/ — Neuigkeiten, Interviews und Artikel zu Sendmail, unter anderem auch ein detaillierterer Überblick über die vielen möglichen Optionen.
- http://www.sendmail.org/ — Vollständige technische Analyse der Sendmail-Features und Konguationsbeispiele.
- http://tuxedo.org/~esr/fetchmail — Die Homepage für Fetchmail, mit einem Online-Handbuch und gründliche Behandlung häufig gestellter Fragen (FAQ).
- http://www.procmail.org/ — Die Homepage für Procmail, mit Links zu ausgesuchten Mailing-Listen für Procmail sowie verschiedene FAQ-Dokumente.
- http://www.ling.helsinki.fi/users/reriksso/procmail/mini-faq.html — Ausgezeichnete Procmail-FAQ, mit Tips für Problemlösungen und Details zum Sperren von Dateien und zur Verwendung von Wildcard-Zeichen.
- http://www.uwasa.fi/~ts/info/proctips.html — Dutzende von Tipps, die die Verwendung von Procmail unter verschiedenen Umständen erheblich vereinfachen, wie man die `.procmailrc`-Dateien testet und wie das Scoring bei Procmail funktioniert, mit dem festgelegt wird, ob eine bestimmte Maßnahme ergriffen werden soll.
- http://www.spamassassin.org/ — Die offizielle Seite des SpamAssassin Projekts.

11.6.3. Literatur zum Thema

- *Sendmail* von Bryan Costales in Zusammenarbeit mit Eric Allman et al; O'Reilly & Associates — Eine gute Beschreibung von Sendmail. Geschrieben mit der Unterstützung des Entwicklers von Delivermail und Sendmail.
- *Removing the Spam: Email Processing and Filtering* von Geoff Mulligan; Addison-Wesley Publishing Company — Ein Buch, das die verschiedenen Methoden betrachtet, mit denen Email-Administratorren unter Anwendung bekannter Tools wie z.B. Sendmail oder Procmail, Probleme mit Junkmails handhaben.
- *Internet Email Protocols: A Developer's Guide* von Kevin Johnson; Addison-Wesley Publishing Company — Vollständiger Überblick über die wichtigsten E-Mail-Protokolle und deren Sicherheit.
- *Managing IMAP* von Dianna Mullet und Kevin Mullet; O'Reilly & Associates — Beschreibt die einzelnen Schritte zur Konfiguration eines IMAP-Servers.

Kapitel 12.
Berkeley Internet Name Domain (BIND)

Die meisten modernen Netzwerke, einschliesslich dem Internet, erlauben dem Benutzer andere Computer über deren Namen zu bestimmen. Dies befreit den Benutzer davon, die numerische Netzwerk-Adresse behalten zu müssen. Der effektivste Weg ein Netzwerk zu konfigurieren, sodass es namensbasierte Verbindungen zulässt, ist durch das Einrichten eines *Domain Name Service* (*DNS*) oder *Nameserver*, welcher Rechnernamen in IP-Adressen auflöst und umgekehrt.

Dieses Kapitel stellt den in Red Hat Linux enthaltenen Nameserver, *Berkeley Internet Name Domain* (*BIND*) DNS Server, vor, mit dem Fokus auf die Struktur dessen Konfigurationsdateien und der Art und Weise, wie dieser lokal und auch remote verwaltet werden kann.

Anweisungen für die Konfiguration von BIND unter Verwendung des graphischen **Bind Konfigurationstool** finden Sie im Kapitel *BIND-Konfiguration* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

Warnung

Wenn Sie das **Bind Konfigurationstool** verwenden, sollten Sie die BIND- Konfigurationsdateien nicht manuell bearbeiten, da alle manuell vorgenommenen Änderungen vom **Bind Konfigurationstool** überschrieben werden.

12.1. Einführung in den DNS

Wenn Hosts auf einem Netzwerk zu einem anderen über deren Hostnamen, auch *fully qualified domain name (FQDN)* genannt, verbinden, wird DNS verwendet, um die IP-Adressen der Rechner über deren Hostnamen zu bestimmen.

Die Verwendung von DNS und FQDN sind auch für Systemadministratoren vorteilhaft. Dank dieser Namen verfügen Administratoren über die Flexibilität, IP-Adressen für einzelne Rechner zu ändern, ohne namenbasierte Abfragen der Rechner ausführen zu müssen. Umgekehrt können die Administratoren festlegen, welche Rechner eine namenbasierte Abfrage in einer für die Benutzer transparenten Weise handhaben.

DNS wird im Allgemeinen mit Hilfe zentralisierter Server implementiert, die für einige Domains authorisiert sind und sich auf andere DNS-Server für andere Domains beziehen.

Eine Client-Applikation verbindet üblicherweise über den Port 53 mit dem Nameserver und fragt Informationen über diesen ab. Der Nameserver wird versuchen, mit Hilfe einer Resolver-Bibliothek den FQDN zu lösen. Diese Bibliothek kann die vom Host angeforderten Informationen oder Daten über den Namen aus einer früheren Abfrage enthalten. Wenn der Nameserver die Antwort nicht in seiner Resolver-Bibliothek findet, wird er andere Nameserver, die sogenannten *Root- Nameserver* verwenden, um festzulegen, welche Nameserver für diesen FQDN autorisiert sind. Mit dieser Information wird anschließend bei den autorisierten Nameservern dieser Name abgefragt, um die IP-Adresse festzustellen. Bei einem Reverse-Lookup wird die gleiche Prozedur durchgeführt, allerdings mit dem Unterschied, dass hier eine unbekannte IP-Adresse und nicht ein Name abgefragt wird.

12.1.1. Nameserver Zonen

Im Internet kann ein FQDN eines Hosts in verschiedene Bereiche eingeteilt werden. Diese Bereiche werden in einer Hierarchie, ähnlich wie bei einem Baum mit Hauptstamm, primären Abzweigungen, sekundären Abzweigungen usw. angeordnet. Betrachten Sie den folgenden FQDN:

```
bob.sales.example.com
```

Wenn Sie sehen möchten, wie ein FQDN aufgelöst wurde, um eine IP-Adresse für ein bestimmtes System zu finden, müssen Sie den Namen von rechts nach links lesen. Jede Ebene der Hierarchie ist durch Punkte (`.`) voneinander getrennt. In diesem Beispiel bestimmt `com` die *Top-Level-Domain* für diesen FQDN. Der `domain`-Name ist eine Subdomain von `com` mit `sales` als Subdomain von `example`. Ganz links im FQDN befindet sich der Hostname, `bob`, der einen bestimmten Computer identifiziert.

Mit Ausnahme des Hostnamens wird jeder Bereich als *Zone* bezeichnet, die einen bestimmten *Namespace* (Namensbereich) festlegt. Ein Namespace kontrolliert die Bezeichnung der Subdomains auf der linken Seite. In diesem Beispiel sind zwar nur zwei Subdomains angegeben, ein FQDN muss aber mindestens eine und kann viel mehr Subdomains enthalten, je nach der Organisation des Namespace.

Die Zonen werden mit Hilfe von *Zone-Dateien* in authorisierten Nameservern festgelegt. Die Zone-Dateien beschreiben den Namenspace der Zone, den für eine bestimmte Domain oder Subdomain zu verwendenden Mail-Server, uvm. Die Zone-Dateien sind auf *primären Nameservern* (auch *Master-Nameserver* genannt) gespeichert, die für Änderungen an Dateien maßgeblich sind, sowie auf *sekundären Nameservern* (auch *Slave-Nameserver* genannt), die ihre Zone-Dateien von den primären Nameservern erhalten. Jeder Nameserver kann gleichzeitig für unterschiedliche Zonen sowohl primärer als auch sekundärer Nameserver sein. Zugleich können sie auch für mehrere Zonen maßgeblich sein. Dies hängt alles von der Konfiguration des Nameservers ab.

12.1.2. Nameserver Types

Primäre Nameserver können auf vier verschiedene Arten konfiguriert sein:

- *Master* — Speichert die ursprünglichen und maßgeblichen Zonen für einen bestimmten Namespace, beantwortet Fragen von anderen Nameservern, die nach Antworten für diesen Namespace suchen.
- *Slave* — Beantwortet ebenfalls die Anfragen anderer Nameserver bezüglich des Namespace, für den dieser die Autorität darstellt. Die Slave-Nameserver erhalten ihre Informationen über ein Namespace jedoch von Master-Nameservern.
- *Caching-Only* — Bietet Services für IP-Auflösungen, hat aber nicht für alle Zonen eine Berechtigung. Antworten für alle Auflösungen werden üblicherweise in einer Datenbank bearbeitet, die für eine bestimmte Zeit im Hauptspeicher verbleibt. Sie werden von dem Zone-Record, das die Antworten erhält, nach der ersten Auflösung für andere DNS-Clients festgelegt.
- *Forwarding* — Leitet Anfragen zum Auflösen an eine spezielle Liste von Nameservern weiter. Wenn keiner der angegebenen Nameserver den Auflösungsprozess durchführen kann, wird der Vorgang abgebrochen und die Auflösung schlägt fehl.

Ein Nameserver kann einem oder mehreren dieser Typen zugehören. Zum Beispiel kann ein Nameserver für einige Zonen der Master und für andere Zonen der Slave sein und für andere ausschließlich Auflösungen weiterleiten.

12.1.3. BIND als Nameserver

BIND führt Namensauflösungsdienste mittles des `/usr/sbin/named` Daemon durch. BIND enthält auch ein administratives Utility, `/usr/sbin/rndc` genannt. Mehr Information zu `rndc` kann unter Abschnitt 12.4 gefunden werden.

BIND speichert seine Konfigurationsdateien in den folgenden zwei Orten:

- `/etc/named.conf` — Die Konfigurationsdatei für den `named` Daemon.

- `/var/named/` directory — Das `named` Arbeitsverzeichnis, welches Zone, Statistiken, und Cache-Dateien enthält.

Die nächsten zwei Abschnitte behandeln die BIND Konfigurationsdateien in mehr Detail.

12.2. `/etc/named.conf`

Die `/etc/named.conf`-Datei ist eine Ansammlung von Direktiven, die in verschachtelte, geschweifte Klammern platzierte `{ }`-Optionen verwenden. Administratoren müssen vorsichtig beim Bearbeiten der Datei `named.conf` sein und jegliche syntaktische Fehler veremeiden, da auch die kleinsten Fehler den Service `named` vom Starten abhalten können.

Warnung

Bearbeiten Sie die Datei `/etc/named.conf` oder andere Dateien aus dem `/var/named/`-Verzeichnis *nicht* manuell, wenn Sie mit dem **Bind Konfigurationstool** arbeiten. Alle manuell vorgenommenen Änderungen an diese Dateien werden überschrieben, wenn **Bind Konfigurationstool** das nächste Mal verwendet wird.

Eine typische `named.conf`-Datei ist ähnlich wie folgt gegliedert:

```
<statement-1> ["<statement-1-name>"] [<statement-1-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};

<statement-2> ["<statement-2-name>"] [<statement-2-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};

<statement-N> ["<statement-N-name>"] [<statement-N-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};
```

12.2.1. Häufig verwendete Typen von Statements

Die folgenden Typen von Statements werden häufig in `/etc/named.conf` verwendet:

12.2.1.1. `acl` Statement

Das `acl` Statement (Access Control Statement) definiert eine Gruppe von Hosts, welchen Zugriff zum Nameserver erlaubt oder verboten werden kann.

Ein `acl` Statement hat folgende Form:

```
acl <acl-name> {
    <match-element>;
    [<match-element>; ...]
};
```

In diesem Statement ersetzen Sie *<acl-name>* mit dem Namen der Access-Control-List (Liste der Zugriffskontrolle) und ersetzen Sie *<match-element>* mit einer List von IP-Adressen, wobei Adressen durch ein Semikolon getrennt werden. Meistens wird eine individuelle IP-Adresse oder IP-Netzwerk-Notation (wie `10.0.1.0/24`) benutzt, um die IP Adresse im `acl` Statement zu identifizieren.

Die folgenden Access-Control-Lists sind bereits als Schlüsselwörter definiert, um die Konfiguration zu vereinfachen:

- `any` — Vergleicht jede IP-Adresse.
- `localhost` — Vergleicht jede IP-Adresse, die auf dem lokalen System verwendet wird.
- `localnets` — Vergleicht jede IP-Adresse auf allen Netzwerken, mit denen das lokale System verbunden ist.
- `none` — Vergleicht keine IP-Adressen.

Wenn mit anderen Statements (wie dem `options` Statement) verwendet, können `acl` Statements sehr hilfreich dabei sein, BIND Nameserver vor unbefugtem Zugriff zu schützen.

Das folgende Beispiel gibt zwei Access-Control-Lists und benutzt ein `options` Statement, um anzugeben, wie diese vom Nameserver behandelt werden sollen:

```
 acl black-hats {
   10.0.2.0/24;
   192.168.0.0/24;
};

acl red-hats {
   10.0.1.0/24;
};

options {
   blackhole { black-hats; };
   allow-query { red-hats; };
   allow-recursion { red-hats; };
}
```

Dieses Beispiel enthält zwei Access-Control-Lists, `black-hats` und `red-hats`. Hosts in der `black-hats` Liste ist der Zugriff zum Nameserver verboten, während Hosts in der `red-hats` Liste normaler Zugriff gewährt ist.

12.2.1.2. `include` Statement

Das `include` Statement erlaubt Dateien in `named.conf` einzuschliessen. In dieser Weise können sensitive Konfigurationsdaten (wie `keys`) in einer separaten Datei mit eingeschränkten Rechten gehalten werden.

Ein `include` Statement hat die folgende Form:

```
include  "<file-name>"
```

In diesem Statement, ersetzen Sie *<file-name>* mit dem absoluten Pfad zu einer Datei.

12.2.1.3. `options` Statement

Das `options` Statement legt Konfigurationsoptionen des globalen Servers fest und setzt Defaults für andere Statements. Es kann verwendet werden, um den Ort des `named` Arbeitsverzeichnisses anzugeben, den Typ der erlaubten Queries, uvm.

Das `options` Statement hat die folgende Form:

```
options {
        <option>;
 [<option>; ...]
};
```

In diesem Statement, ersetzen Sie die *<option>* Direktiven mit einer gültigen Option.

Die folgenden sind häufig benutzte Optionen:

- `allow-query` — Legt fest, welche Hosts diesen Nameserver abfragen dürfen. Standardmäßig sind alle Hosts dazu berechtigt. Mit Hilfe einer Access-Controll-List, einer Sammlung von IP-Adressen oder Netzwerken kann festgelegt werden, dass nur bestimmte Hosts den Nameserver abfragen dürfen.
- `allow-recursion` — Ähnelt der Option `allow-query`, mit der Ausnahme, dass sie sich auf rekursive Abfragen bezieht. Standardmäßig können alle Hosts rekursive Abfragen auf dem Nameserver durchführen.
- `blackhole` — Gibt an, welchen Hosts es nicht erlaubt is Anfragen an den Server zu stellen.
- `directory` — Ändert das `named`-Arbeitsverzeichnis, so dass es sich von dem Default, `/var/named/`, unterscheidet.
- `forward` — Kontrolliert das Verhalten beim Weiterleiten einer `forwarders` Direktive.

  Die folgenden Optionen werden angenommen:

  - `first` — Gibt an, dass Nameserver, die in der `forwarders`-Option festgelegt sind, zuerst nach Informationen abgefragt werden, sollten anschließend keine Informationen vorhanden sein, versucht `named` die Auflösung selbst durchzuführen.
  - `only` — Gibt an, dass `named` nicht versucht die Auflösung selbst durchzuführen, wenn die `forwarders` Direktive nicht erfolgreich war.

- `forwarders` — Legt eine Liste von Nameservern fest, bei denen Abfragen für Auflösungen weitergeleitet werden.
- `listen-on` — Legt die Netzwerk-Schnittstelle fest, die `named` verwendet, um Anfragen zu prüfen. Standardmäßig werden alle Schnittstellen verwendet.

  Auf diese Weise, sollte der DNS Server auch der Gateway sein, kann BIND dazu konfiguriert werden nur Anfragen, welche von einem dieser Netzwerke gestellt wurden, zu beantworten.

  Eine `listen-on` Direktive kann folgendermaßen aussehen:

  ```
  options {
     listen-on { 10.0.1.1; };
  };
  ```

  Auf diese Art und Weise werden nur Anfragen von der Netzwerk-Schnittstelle akzeptiert, die das private Netzwerk (`10.0.1.1`) verwendet.
- `notify` — Kontrolliert, ob `named` die Slave-Server informiert, wenn eine Zone aktualisiert wird. Nimmt die folgenden Optionen an:

  - `yes` — Informiert Slave-Server.
  - `no` — Informiert Slave-Server nicht.

  - `explicit` — Informiert Slave-Server nur dann, wenn diese in einer `also-notify` List innerhalb des Zonen Statement angegeben sind.

- `pid-file` — Erlaubt das Festlegen eines alternativen Ortes für die Prozess-ID-Datei, die `named` erstellt.
- `statistics-file` — Erlaubt das Festlegen eines alternativen Ortes in welcher die Statistik-Dateien abgelegt werden. Standardmäßig werden `named`-Statistiken in `/var/named/named.stats` gespeichert.

Es gibt noch zahlreiche andere Optionen, bei denen einige voneinander abhängig sind, um fehlerfrei zu funktionieren. Weitere Informationen hierzu finden Sie im *BIND 9 Administrator Reference Manual*, in Abschnitt 12.7.1, und in den man-Seiten zu `bind.conf`.

12.2.1.4. `zone` Statement

Ein `zone` Statement legt die Eigenschaften einer Zone, wie den Ort der Konfigurationsdatei und Zonen-spezifische Optionen fest. Diese Statement kann benutzt werden um globale `options` Statements zu überschreiben.

Ein `zone` Statement hat die folgende Form:

```
zone <zone-name> <zone-class> {
     <zone-options>;
     [<zone-options>; ...]
};
```

In diesem Statement *<zone-name>* ist der Name der Zone, *<zone-class>* ist die optionale Klasse der Zone, und *<zone-options>* ist eine List von Optionen, welche die Eigenschaften der Zone bestimmen.

Das *<zone-name>*-Attribut für die Zone ist besonders wichtig, da es den Standardwert für die `$ORIGIN` Direktive festlegt, welche den Zonen-Dateien im Verzeichnis `/var/named/` entspricht. Der `named` Daemon hängt den Namen der Zone an jeden nicht-FQDN an, welcher in der Zonen-Datei aufgelistet ist.

Wenn, zum Beispiel, ein `zone` Statement den Namespace für `example.com` angibt, verwende `example.com` als *<zone-name>*, damit es an Hostnamen in der `example.com` Zonen-Datei angehängt wird.

Für mehr Information zu Zonen-Dateien, siehe Abschnitt 12.3.

Die am häufigsten verwendeten Optionen von `zone` Statement sind die Folgenden:

- `allow-query` — Legt fest, welche Clients Informationen über diese Zone anfordern dürfen. Standardmäßig sind alle Anfragen zulässig.
- `allow-transfer` — Bestimmt die Slave-Server, die den Transfer der Informationen über die Zonen anfordern dürfen. Standardmäßig sind alle Transfer-Anfragen zulässig.
- `allow-update` — Bestimmt die Hosts, die Informationen in ihrer Zone dynamisch aktualisieren dürfen. Standardmäßig sind Anfragen für dynamische Updates nicht zulässig.

  Wenn Sie zulassen, dass Hosts Informationen über ihre Zonen aktualisieren, sollten Sie unbedingt sicherstellen, dass Sie diese Option nur aktivieren, wenn der Host absolut sicher ist. Es ist besser, die Updates der Zonen-Records manuell von einem Administrator durchführen zu lassen und den `named`-Service, soweit möglich, neu zu laden.
- `file` — Bestimmt den Namen der Datei im `named`-Arbeitsverzeichnis, die die Zone-Konfigurationsdateien enthält. Standardmäßig ist dies `/var/named/`.

- `masters` — The `masters` option lists the IP addresses from which to request authoritative zone information. Used only if the zone is defined as `type slave`.
- `notify` — Wird verwendet, wenn die Zone als Slave `type` festgelegt ist. Die `masters`- Option teilt dem `named` eines Slaves die IP-Adressen mit, von denen maßgebliche Informationen über die Zone angefragt werden:
  - `yes` — Informiert Slave Server.
  - `no` — Informiert Slave Server nicht.
  - `explicit` — Informiert Slave-Server nur dann, wenn diese in einer `also-notify` List innerhalb des Zonen Statement angegeben sind.

- `type` — Gibt den Typ der Zone an.

  Folgend ist eine Liste der gültigen Optionen:
  - `forward` — Weist den Nameserver an, alle Anfragen zu Informationen über die Zone an andere Nameserver weiterzuleiten.
  - `hint` — Ein spezieller Zonen-Typ, mit dem auf die Root-Nameserver verwiesen wird, die verwendet werden, um Abfragen zu lösen, wenn eine Zone ansonsten unbekannt ist. Sie brauchen neben der Standarddatei `/etc/named.conf` keine zusätzliche Hinweisdatei konfigurieren.
  - `master` — Bezeichnet den Nameserver, der für diese Zone maßgeblich ist. Wenn die Konfigurationsdateien für diese Zone auf Ihrem System sind, sollte der `master`-Typ eingestellt werden.
  - `slave` — Bezeichnet den Nameserver, der für diese Zone der Slave-Server ist und der `named` mitteilt, die Zonen-Konfigurationsdateien für diese Zone von der IP-Adresse des Master-Nameservers abzufragen.

- `zone-statistics` — Weist `named` an, die Statistiken über diese Zone aufzubewahren und diese entweder in der Standard-Datei (`/var/named/named.stats`) oder an einer Stelle abzulegen, die mit der `statistics-file`-Option in der `server`-Anweisung, sofern vorhanden, dafür eingerichtet wurde. Sehen Sie Abschnitt 12.2.2 für mehr Information über das `server` Statement.

12.2.1.5. Beispiele von `zone`-Statements

Die meisten Änderungen in der `/etc/named.conf`-Datei eines Master- oder Slave-Nameservers betreffen das Hinzufügen, Modifizieren oder Löschen von `zone`-Direktiven. Obwohl diese `zone`-Anweisungen mehrere Optionen enthalten können, werden von den meisten Nameservern nur wenige verwendet. Die folgenden `zone`-Direktiven sind sehr allgemeine Beispiele, die auf Master-Slave-Nameservern verwendet werden können.

Nachfolgend finden Sie ein Beispiel für eine `zone`- Anweisung für den primären Nameserver, der `example.com` (`192.168.0.1`) hostet:

```
zone "example.com" IN {
  type master;
  file "example.com.zone";
  allow-update { none; };
};
```

Diese `zone`-Direktive benennt die Zone `example.com`, stellt als `type master` ein und weist den `named`-Service an, die Datei `/var/named/example.com.zone` zu lesen und weist `named` an, Aktualisierungen durch andere Hosts nicht zuzulassen.

Eine zone-Anweisung eines Slave-Servers für example.com unterscheidet sich etwas vom vorherigen Beispiel. Für einen Slave-Server wird der Typ auf slave festgelegt. An die Stelle der Zeile allow-update tritt eine Anweisung, die named die IP-Adresse des Master-Servers mitteilt.

Die zone-Anweisung eines Slave-Servers für example.com könnte folgendermaßen aussehen:

```
zone "example.com" {
  type slave;
  file "example.com.zone";
  masters { 192.168.0.1; };
};
```

Diese zone-Anweisung weist named auf dem Slave-Server an, bei dem Master-Server mit der IP 192.168.0.1 nach Informationen für die Zone example.com zu suchen. Die Informationen, die der Slave-Server vom Master-Server erhält, werden in der Datei /var/named/example.com.zone gespeichert.

12.2.2. Andere Statement-Typen

Die Folgende ist eine Liste von weniger verwendeten Statement-Typen welche in named.conf verfügbar sind:

- controls — Konfiguriert verschiedene Sicherheitsbedingungen, die für den Befehl rndc zum Verwalten des named-Services nötig sind.

  Unter Abschnitt 12.4.1 sehen Sie, wie die controls-Anweisung aussehen sollte, einschließlich mehrerer Optionen, die nur mit ihr verwendet werden.

- key "<*key-name*>" — Legt für einen bestimmten Schlüssel einen Namen fest. Schlüssel werden verwendet, um verschiedene Aktionen zu authentifizieren, wie z.B. sichere Updates oder die Verwendung des rndc-Befehls. Mit key werden zwei Optionen verwendet:

  - algorithm <*algorithm-name*> — Der verwendete Algorithmus-Typ, z.B. dsa oder hmac-md5.
  - secret "<*key-value*>" — Der verschlüsselte Schlüssel.

  Unter Abschnitt 12.4.2 finden Sie die Anweisungen zum Schreiben einer key-Direktive.

- logging — Erlaubt die Verwendung mehrerer Arten von Protokollen mit der Bezeichnung *channels*. Wird die Option channel in der logging-Anweisung verwendet, wird ein benutzerdefiniertes Protokoll mit eigenem Dateinamen (file), Größenbeschränkung (size), Version (version), und dessen Wichtigkeit (severity) erstellt. Nachdem ein benutzerdefinierter Channel festgelegt wurde, wird dieser mit der Option category klassifiziert und beginnt mit dem Protokollieren, wenn named neu gestartet wird.

  Standardmäßig protokolliert named normale Mitteilungen im syslog-Daemon, der diese in /var/log/messages platziert. Dies geschieht, weil sich verschiedene standardmäßige Channel mit unterschiedlicher Wichtigkeit im BIND befinden. Zum Beispiel verarbeitet ein Channel die Protokoll-Mitteilungen (default_syslog) und ein anderer speziell Debugging-Mitteilungen (default_debug). Die standardmäßige Kategorie default, verwendet zum normalen Protokollieren, ohne spezielle Konfigurationen, integrierte Channel.

  Den Protokollierungsprozess individuell anzupassen kann sehr aufwendig sein und übersteigt den Umfang dieses Kapitels. Informationen über die Erstellung von benutzerdefinierten BIND-Protokollen finden Sie im *BIND 9 Administrator Reference Manual* in Abschnitt 12.7.1.

- server — Definiert bestimmte Optionen, die Auswirkungen darauf haben, wie named sich gegenüber Remote-Name-Servern verhalten soll, insbesondere im Hinblick auf Benachrichtigungen und Zone-Übertragungen.

Die Option `transfer-format` kontrolliert, ob mit jeder Mitteilung ein Resource-Record (`one-answer`) oder mehrere Ressource-Records mit jeder Meldung gesendet werden (`many-answers`). Da `many-answers` leistungsfähiger ist, wird es nur von neueren Name-Servern angenommen.

- `trusted-keys` — Enthält verschiedene öffentliche Schlüssel für die Verwendung mit Secure DNS (DNSSEC). Unter Abschnitt 12.5.3 finden Sie eine Einführung in die BIND-Sicherheit.
- `view "<view-name>"` — Erstellt spezielle Ansichten, die bestimmten Informationen entsprechen, die von dem Host abhängig sind, der den Name-Server kontaktiert. Dadurch erhalten einige Hosts Informationen, die sich vollkommen von denen unterscheiden, die andere Hosts erhalten. Eine andere Möglichkeit ist, nur bestimmte Zonen für bestimmte sichere Hosts zugänglich zu machen, während nicht sichere Hosts nur Abfragen für andere Zonen erstellen können.

  Es können auch mehrere Ansichten verwendet werden, solange ihre Namen eindeutig sind. Die `match-clients`-Option legt die IP-Adressen fest, die für eine bestimmte Ansicht verwendet werden. Alle `option`-Direktiven können in einer Ansicht verwendet werden. Sie überschreiben dabei die allgemeinen, bereits für `named` konfigurierten Optionen. Die meisten `view`-Direktiven enthalten mehrere `zone`-Anweisungen, die für die `match-clients`-Liste gelten. Es ist wichtig, in welcher Reihenfolge die `view`-Anweisungen aufgelistet sind, da die erste `view`-Direktive, die mit einer bestimmten IP-Adresse des Client übereinstimmt, verwendet wird.

  Unter Abschnitt 12.5.2 finden Sie weitere Informationen zur `view`-Anweisung.

12.2.3. Kommentar-Tags

Die Folgende ist eine Liste gültiger, in `named.conf` verwendeter, Kommentar-Tags:

- `//` — Wenn an den Anfang der Zeile gestellt, wird diese Zeile von `named` ignoriert.
- `#` — Wenn an den Anfang der Zeile gestellt, wird diese Zeile von `named` ignoriert.
- `/*` und `*/` — Hierin eingeschlossener Text wird von `named` ignoriert.

12.3. Zone-Dateien

Zone-Dateien sind im `named`-Arbeitsverzeichnis gespeichert und enthalten Informationen über einen bestimmten Namespace. Die Standarddatei ist `/var/named`. Jede Zone-Datei ist gemäß der Daten der `file`-Option in der `zone`- Direktive benannt. Normalerweise bezieht sich der Name auf die entsprechende Domain und identifiziert die Datei als Datei, die Zone-Daten enthält, wie z.B. `example.com.zone`.

Jede Zone-Datei kann Direktiven und Resource-Records enthalten. *Direktiven* weisen den Name-Server an, bestimmte Aktionen auszuführen oder spezielle Einstellungen für die Zone zu verwenden. *Resource-Records* legen die Parameter der Zone fest. Diese ordnen bestimmten Systemen innerhalb des Namespaces der Zone eine Identität zu. Anweisungen sind optional, aber Resource-Records sind notwendig, um dieser Zone den Name-Service zur Verfügung zu stellen.

Alle Direktiven und Resource-Records sollten in einer eigenen Zeile stehen.

Kommentare können in Zone-Dateien nach dem Semikolon (`;`) platziert werden.

12.3.1. Zone-Dateien-Direktiven

Anweisungen werden durch das vorangestellte Dollarzeichen `$` identifiziert, das vor dem Namen der Anweisung üblicherweise im oberen Teil der Zone-Datei steht.

Folgende Anweisungen werden am häufigsten verwendet:

- `$INCLUDE` — Weist `named` an, in diese Zone-Datei an Stelle der Anweisung eine andere Zone-Datei einzufügen. Dadurch können zusätzliche Einstellungen der Zone getrennt von der Haupt-Zone-Datei gespeichert werden.
- `$ORIGIN` — Stellt den Domain-Name so ein, dass er an alle ungeeigneten Records angefügt wird. Wie z.B. die, die ausschließlich den Host festlegen.

  Eine Zone-Datei kann z.B. folgende Zeile enthalten:
  ```
  $ORIGIN example.com
  ```
  Jetzt würde an alle Namen, die in Resource-Records verwendet werden und nicht mit einem Punkt (`.`) enden, `example.com` angehängt.

  

  Anmerkung

  Die Verwendung der `$ORIGIN`-Direktive ist nicht erforderlich, wenn der Name der Zone in `/etc/named.conf` mit dem Wert übereinstimmt, den Sie `$ORIGIN` zuweisen würden. Standardmäßig wird der Name der Zone als Wert der `$ORIGIN`-Anweisung verwendet.

- `$TTL` — Legt den Standard-*Time to Live (TTL)*-Wert für die Zone fest. Dieser Wert legt für die Name-Server in Sekunden fest, wie lange das Resource-Record für die Zone gültig ist. Ein Resource- Record kann einen eigenen TTL-Wert besitzen, der den Wert dieser Anweisung für die Zone überschreibt.

  Wird dieser Wert erhöht, können die Remote-Name-Server die Zone-Informationen länger verarbeiten. Dadurch werden zwar die Abfragen für diese Zone reduziert, es vergrößert sich jedoch der Zeitraum, bis man von den Änderungen der Resource-Records profitieren kann.

12.3.2. Resource-Records der Zone-Datei

Die Hauptkomponente einer Zone-Datei ist deren Resource-Records.

Es gibt viele Typen von Resource-Records, Folgende werden am häufigsten verwendet:

- `A` — Adressen-Record, das einem Namen eine IP-Adresse zuweist. Beispiel:
  ```
  <host>      IN      A      <IP-address>
  ```
  Wenn der `<host>`-Wert nicht angegeben wird, verweist ein `A`-Record auf eine standardmäßige IP-Adresse für den oberen Teil des Namespaces. Dieses System gilt für alle nicht-FQDN-Anfragen.

  Beachten Sie das folgende `A`-Record-Beispiel für die `example.com` Zone-Datei:
  ```
                IN      A       10.0.1.3
  server1       IN      A       10.0.1.5
  ```
  Anfragen für `example.com` richten sich an 10.0.1.3, während Anfragen für `server1.example.com` sich an 10.0.1.5 richten.
- `CNAME` — Name-Record, welcher Namen untereinander zuordnet. Dieser Typ ist auch als Alias bekannt.

  Im nächsten Beispiel wird `named` angewiesen, dass alle Anfragen, die an den `<alias-name>` gesendet werden, auf den Host `<real-name>` zeigen. `CNAME`-Records werden am häufigsten verwendet, um auf Dienste zu verweisen, die ein allgemeines Namensschema für den korrekten Host, wie `www` für Web-Server, verwenden.
  ```
  <alias-name>      IN      CNAME       <real-name>
  ```
  Betrachten Sie das folgende Beispiel. In dieser Einrichtung bindet der `A`-Record einen Hostnamen an eine IP-Adresse, während ein `CNAME`-Record den allgemein verwendeten Hostnamen `www` zuweist.
  ```
  server1       IN      A       10.0.1.5
  ```

```
www             IN      CNAME   server1
```

- MX — Mail eXchange- Record, das angibt, welchen Weg eine Mail nimmt, die an ein bestimmtes Namespace gesendet und von dieser Zone kontrolliert wurde.

  ```
        IN      MX      <preference-value>   <email-server-name>
  ```

  In diesem Beispiel ermöglicht *<preference-value>*, die E-Mail-Server der Reihenfolge nach zu nummerieren, auf denen Sie für dieses Namespace bestimmte E-Mails empfangen möchten, indem Sie einigen E-Mail-Systemen den Vorrang vor anderen geben. Der MX-Resource-Record mit dem niedrigsten *<preference-value>* wird den anderen vorgezogen. Sie können mehreren E-Mail-Servern denselben Wert zuweisen, um den E-Mail-Verkehr zwischen den Servern zu verteilen.

  Der *<email-server-name>* kann ein Hostname oder ein FQDN sein.

  ```
        IN      MX      10      mail.example.com.
        IN      MX      20      mail2.example.com.
  ```

  In diesem Beispiel wird der erste `mail.example.com`-E-Mail-Server vor dem `mail2.example.com`-E-Mail-Server bevorzugt, wenn eine E-Mail für die Domain `example.com` ankommt.

- NS — Name-Server-Record, der die maßgeblichen Name-Server für eine bestimmte Zone anzeigt.

  Beispiel für einen NS-Record:

  ```
        IN      NS      <nameserver-name>
  ```

  Der *<nameserver-name>* sollte ein FQDN sein.

  Anschließend werden zwei Nameserver als maßgeblich für die Domain aufgelistet. Es ist nicht so wichtig, ob diese Namenserver Slave- oder Master-Nameserver sind, da beide bereits maßgebend sind.

  ```
        IN      NS      dns1.example.com.
        IN      NS      dns2.example.com.
  ```

- PTR — PoinTeR-Record verweist auf einen anderen Teil des Namespace.

  PTR-Records werden primär für eine umgekehrte Namensauflösung verwendet, da sie IP-Adressen zu einem bestimmten Namen verweisen. Unter Abschnitt 12.3.4 finden Sie weitere Beispiele zur Verwendung von PTR-Records.

- SOA — Start Of Authority-Record, gibt wichtige maßgebliche Informationen über den Namespace an den Name-Server.

  Nach den Direktiven festgelegt ist ein SOA-Resource-Record, der erste Resource-Record in einer Zone-Datei.

  Das folgende Beispiel zeigt die Basisstruktur eines SOA-Record:

  ```
  @     IN      SOA     <primary-name-server>      <hostmaster-email> (
                        <serial-number>
                        <time-to-refresh>
                        <time-to-retry>
                        <time-to-expire>
                        <minimum-TTL> )
  ```

  Das @-Symbol richtet die $ORIGIN-Anweisung (oder den Namen der Zone, falls die $ORIGIN-Direktive nicht eingestellt ist) als Namespace ein, das von diesem SOA-Resource-Record eingestellt wurde. Als *<primary-Nameserver>* wird der erste, für diese Domain maßgebliche Name-Server verwendet und die E-Mail der über diesen Namespace zu kontaktierenden Person wird durch die *<hostmaster-email>* ersetzt.

  Die *<serial-number>* wird bei jeder Änderung der Zone-Datei erhöht, so dass `named` erkennt, dass diese Zone neu geladen werden kann. Die *<time-to-refresh>* teilt den Slave-Servern mit, wie lange sie warten müssen, bevor sie beim Master-Nameserver anfragen, ob alle Änderungen für die Zone durchgeführt wurden. Der Wert der *<serial-number>* wird vom

Slave-Server verwendet, um festzustellen, ob veraltete Daten der Zone verwendet werden, die aktualisiert werden sollten.

Die *<time-to-retry>* gibt den Zeitraum an, nach dem eine neue Anfrage bezüglich der Aktualisierung durchgeführt werden soll, wenn der Master-Nameserver auf die letzte Anfrage nicht reagiert hat. Wenn der Master-Nameserver nicht geantwortet hat, bevor die *<time-to-expire>* abläuft, reagiert der Slave-Nameserver nicht mehr auf Anfragen bezüglich des Namespaces.

<minimum-TTL> ist die Zeit, die anderen Nameservern zum Verarbeiten der Zonen-Informationen mindestens zur Verfügung steht (in Sekunden).

In BIND werden alle Zeiten in Sekunden angegeben. Sie können jedoch auch Abkürzungen für andere Zeiteinheiten verwenden, wie z.B. Minuten (M), Stunden (H), Tage (D) und Wochen (W). In der Tabelle unter Tabelle 12-1 finden Sie Zeiträume in Sekunden und die entsprechende Zeit in anderen Formaten.

Sekunden	Andere Zeiteinheiten
60	1M
1800	30M
3600	1H
10800	3H
21600	6H
43200	12H
86400	1D
259200	3D
604800	1W
31536000	365D

Tabelle 12-1. Sekunden im Vergleich zu anderen Zeiteinheiten

Das folgende Beispiel zeigt Ihnen, wie ein SOA-Resource-Record aussehen könnte, wenn es mit echten Werten konfiguriert ist.

```
@      IN      SOA     dns1.example.com.     hostmaster.example.com. (
                       2001062501 ; serial
                       21600      ; refresh after 6 hours
                       3600       ; retry after 1 hour
                       604800     ; expire after 1 week
                       86400 )    ; minimum TTL of 1 day
```

12.3.3. Beispiele für Zone-Dateien

Einzeln betrachtet könnten die Anweisungen und Resource-Records schwer zu verstehen sein. Sind beide in einer gemeinsamen Datei plaziert, wird es einfacher.

Im nächsten Beispiel ist eine sehr einfache Zone-Datei abgebildet.

```
$ORIGIN example.com
$TTL 86400
@      IN      SOA     dns1.example.com.     hostmaster.example.com. (
                       2001062501 ; serial
                       21600      ; refresh after 6 hours
                       3600       ; retry after 1 hour
```

```
                        604800     ; expire after 1 week
                        86400 )    ; minimum TTL of 1 day

        IN      NS      dns1.example.com.
        IN      NS      dns2.example.com.

        IN      MX      10      mail.example.com.
        IN      MX      20      mail2.example.com.

                IN      A        10.0.1.5

server1         IN      A        10.0.1.5
server2         IN      A        10.0.1.7
dns1            IN      A        10.0.1.2
dns2            IN      A        10.0.1.3

ftp             IN      CNAME    server1
mail            IN      CNAME    server1
mail2           IN      CNAME    server2
www             IN      CNAME    server2
```

In diesem Beispiel werden Standard-Anweisungen und `SOA`-Werte verwendet. Die maßgeblichen Name-Server sind dabei als `dns1.example.com` und `dns2.example.com` eingestellt, die über `A`-Records verfügen, wodurch sie mit `10.0.1.2` bzw. `10.0.1.3` verbunden sind.

Die mit `MX`-Records konfigurierten E-Mail-Server verweisen auf `server1` und `server2` über `CNAME`-Records. Da die `server1`- und `server2`-Namen nicht mit einem Punkt enden (`.`), wird die `$ORIGIN`-Domain nach ihnen abgelegt, wobei sie zu `server1.domain.com` und `server2.domain.com` erweitert werden. Mit den dazugehörigen `A`-Resource-Records können dann ihre IP-Adressen bestimmt werden.

Die beliebten FTP- und Web-Dienste, die unter den standardmäßigen Namen `ftp.domain.com` und `www.domain.com` zur Verfügung stehen, verweisen auf Rechner, die entsprechende Dienste für die Namen bieten, die `CNAME`-Records verwenden.

12.3.4. Zone-Dateien für die umgekehrte Auflösung von Namen

Eine Zone-Datei für die umgekehrte Auflösung von Namen wird verwendet, um eine IP-Adresse in ein bestimmtes Namespace in einem FQDN umzusetzen. Sie ähnelt einer standardmäßigen Zone-Datei, mit dem Unterschied, dass die `PTR`-Resource-Records zur Verknüpfung der IP-Adressen mit bestimmten Systemnamen verwendet werden.

Ein `PTR`-Record sieht Folgendem ähnlich:

```
<last-IP-digit>       IN      PTR     <FQDN-of-system>
```

Die *<last-IP-digit>* bezieht sich auf die letzte Ziffer in einer IP-Adresse, mit der auf einen bestimmten FQDN im System hingewiesen wird.

Im folgenden Beispiel werden die IP-Adressen `10.0.1.20` durch `10.0.1.25` den korrespondierenden FQDN zugewiesen.

```
$ORIGIN 1.0.10.in-addr.arpa
$TTL 86400
@       IN      SOA     dns1.example.com.      hostmaster.example.com. (
                        2001062501 ; serial
                        21600      ; refresh after 6 hours
                        3600       ; retry after 1 hour
                        604800     ; expire after 1 week
                        86400 )    ; minimum TTL of 1 day
```

```
      IN     NS     dns1.example.com.
      IN     NS     dns2.example.com.

20    IN     PTR    alice.example.com.
21    IN     PTR    betty.example.com.
22    IN     PTR    charlie.example.com.
23    IN     PTR    doug.example.com.
24    IN     PTR    ernest.example.com.
25    IN     PTR    fanny.example.com.
```

Diese Zone-Datei würde mit einer `zone`-Anweisung in der `named.conf`-Datei in den Dienst übernommen, was dann so ähnlich aussieht wie:

```
zone "1.0.10.in-addr.arpa" IN {
  type master;
  file "example.com.rr.zone";
  allow-update { none; };
};
```

Es gibt nur einen kleinen Unterschied zwischen diesem Beispiel und einer standardmäßigen `zone`-Direktive: der Name wird anders angegeben. Bitte beachten Sie, dass bei einer Zone für eine umgekehrte Auflösung die ersten drei Blöcke der IP-Adresse zum Umkehren benötigt werden und `.in-addr.arpa` danach angegeben ist. Dadurch kann ein einzelner Block von IP-Ziffern, der in der Zone-Datei zum umgekehrten Auflösen von Namen verwendet wird, richtig an diese Zone angefügt werden.

12.4. Die Verwendung von `rndc`

BIND enthält das Utility `rndc`, mit dem Sie den `named`-Daemon über die Befehlszeile vom lokalen und von einem Remote Host verwalten können.

Um zu verhindern, dass nicht authorisierte Benutzer auf deren System BIND auf Ihrem Server kontrollieren, wird durch einen gemeinsam verwendeten Schlüssel gewährleistet, dass ausdrücklich nur bestimmte Hosts ein entsprechendes Zugriffsrecht haben. Damit `rndc` in allen `named`-Dateien auf einem lokalen Rechner Befehle ausführen kann, müssen die Schlüssel, die in `/etc/named.conf` und `/etc/rndc.conf` verwendet werden, übereinstimmen.

12.4.1. Configuring `/etc/named.conf`

Um die Verbindung von `rndc`zu Ihrem `named`-Dienst zu ermöglichen, muss beim Start von `named` die `controls`-Anweisung in Ihrer `/etc/named.conf`-Datei vorhanden sein.

Das folgende Beispiel einer `controls`-Anweisung ermöglicht es Ihnen, `rndc`-Befehle vom lokalen Host auszuführen.

```
controls {
  inet 127.0.0.1 allow { localhost; } keys { <key-name>; };
};
```

Diese Anweisung weist `named` an, am standardmäßigen TCP-Port 953 nach Loopback-Adressen zu suchen und lässt `rndc`-Befehle zu, die vom lokalen Host ausgeführt werden, wenn der richtige Schlüssel angegeben wird. Der *<key-name>* bezieht sich auf die `key`-Direktive, die sich auch in der `/etc/named.conf`-Datei befindet. Im nächsten Beispiel wird eine `key`-Anweisung veranschaulicht.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
```

```
};
```

In diesem Beispiel ist *<key-value>* ein HMAC-MD5-Schlüssel. Mit dem nachfolgenden Befehl können Sie Ihre eigenen HMAC-MD5-Schlüssel erstellen:

```
dnssec-keygen -a hmac-md5 -b <bit-length> -n HOST <key-file-name>
```

Es empfiehlt sich, einen Schlüssel mit einer Größe von mindestens 256 Bit zu erstellen. Der aktuelle Schlüssel sollte im *<key-value>*-Bereich unter *<key-file-name>* gespeichert sein.

Achtung

Da `/etc/named.conf` von jedem gelesen werden kann, ist es angeraten, die `key`-Anweisung in eine separate Datei auszulagern, welche nur von root gelesen werden kann, und eine `include`-Anweisung zu verwenden, um diese Datei einzubinden, wie im folgenden Beispiel:

```
include "/etc/rndc.key";
```

12.4.2. Konfigurieren von `/etc/rndc.conf`

Die `key`-Anweisung ist die wichtigste in der Datei `/etc/rndc.conf`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

<key-name> und *<key-value>* sollten exakt mit den Einstellungen in `/etc/named.conf` übereinstimmen.

Um den Schlüsseln, welche in `/etc/named.conf` auf dem Ziel-Server angegeben sind, zu entsprechen, fügen Sie folgende Zeilen zu `/etc/rndc.conf` hinzu.

```
options {
  default-server  localhost;
  default-key     "<key-name>";
};
```

Dieser Befehl setzt den globalen Default-Schlüssel. Der Befehl `rndc` kann allerdings auch verschiedene Schlüssel für verschiedene Server verwenden, wie im folgenden Beispiel gezeigt:

```
server localhost {
  key  "<key-name>";
};
```

Achtung

Stellen Sie sicher, dass jeweils nur ein root-Benutzer auf die Datei `/etc/rndc.conf` zugreifen kann.

12.4.3. Befehlszeilenoptionen

Ein `rndc`-Befehl sieht wie folgt aus:

`rndc <options> <command> <command-options>`

Wenn `rndc` auf einem korrekt konfigurierten lokalen Host ausgeführt wird, stehen Ihnen folgende Befehle zur Verfügung:

- `halt` — Hält den `named`-Service sofort an.
- `querylog` — Protokolliert alle Abfragen, die von Clients auf diesem Name-Server durchgeführt wurden.
- `refresh` — Aktualisiert die Datenbank des Nameservers.
- `reload` — Weist den Name-Server an, die Zone-Dateien neu zu laden, aber alle vorher verarbeiteten Antworten zu behalten. Dadurch können Sie Änderungen in den Zone-Dateien durchführen, ohne dass die gespeicherten Auflösungen von Namen verloren gehen.

  Wenn sich Ihre Änderungen nur auf eine bestimmte Zone auswirken, können Sie nur diese Zone zu laden. Geben Sie hierzu nach dem `reload`-Befehl den Namen der Zone ein.
- `stats` — Schreibt die aktuellen `named`-Statistiken in die Datei `/var/named/named.stats`.
- `stop` — Stoppt den Server vorsichtig, und speichert dabei alle dynamischen Updates und die vorhandenen *Incremental Zone Transfers* (*IXFR*) Daten, vor dem Beenden.

Gelegentlich werden Sie bestimmt auch die Standardeinstellungen in der `/etc/rndc.conf`-Datei übergehen wollen. Hierzu stehen Ihnen folgende Optionen zur Verfügung:

- `-c <configuration-file>` — Weist `rndc` an, nicht die standardmäßige `/etc/rndc.conf`-Datei, sondern eine andere Konfigurationsdatei zu benutzen.
- `-p <port-number>` — Legt für die `rndc`-Verbindung eine andere als die standardmäßige Portnummer 953 fest.
- `-s <server>` — Weist `rndc` an, Befehle an einen anderen Server zu schicken und nicht an den `default-server` in der `/etc/rndc.conf`-Datei.
- `-y <key-name>` — Ermöglicht es Ihnen, einen anderen als den `default-key` in der `/etc/rndc.conf`-Datei einzustellen.

Zusätzliche Informationen zu diesen Optionen finden Sie auf der `rndc`-man-Seite

12.5. Erweiterte Funktionen von BIND

Die meisten BIND-Implementierungen verwenden für die Dienste zur Auflösung von Namen oder als Autorität für bestimmte Domains oder Sub-Domains nur `named`. Die Version 9 von BIND verfügt jedoch auch über eine Reihe weiterer Features, die - korrekte Konfigurierung und Verwendung vorausgesetzt - einen sichereren und effizienteren DNS-Dienst gewährleisten.

Achtung

Einige dieser Features, wie z.B. DNSSEC, TSIG und IXFR, sollten nur in Netzwerkumgebungen mit Nameservern verwendet werden, die diese Features unterstützen. Wenn Ihre Netzwerkumgebung nicht-BIND- oder ältere BIND-Nameserver enthält, prüfen Sie bitte, ob es dafür verbesserte Features gibt, bevor Sie sie verwenden.

Alle hier vorgestellten Features werden im *BIND 9 Administrator Reference Manual* detaillierter beschrieben. Unter Abschnitt 12.7.1 finden Sie mehr Informationen.

12.5.1. DNS-Protokoll-Erweiterungen

BIND unterstützt Incremental Zone Transfers (IXFR), bei denen Slave-Server nur die aktualisierten Teile einer Zone, die auf einem Master-Name-Server modifiziert wurden, heruntergeladen werden. Der standardmäßige Transfer AXFR Process erfordert, dass auch bei der kleinsten Änderung die gesamte Zone an alle Slave-Name-Server übermittelt wird. Für sehr populäre Domainn mit sehr großzügigen Zone-Dateien und vielen Slave-Name-Servern macht IXFR den Benachrichtigungs- und Update-Prozess weniger ressourcenintensiv.

Beachten Sie bitte, dass IXFR nur zur Verfügung steht, wenn Sie für Änderungen der Master-Zonen-Records *dynamisch updaten*. Wenn Sie Zone-Dateien manuell bearbeiten, um Änderungen durchzuführen, verwenden Sie AXFR. Weitere Informationen über das dynamische Updaten finden Sie im *BIND 9 Administrator Reference Manual*. Unter Abschnitt 12.7.1 finden Sie mehr Informationen.

12.5.2. Mehrere Ansichten

Mit der `view`-Anweisung in `named.conf` ermöglicht Ihnen BIND, die Antworten eines Name-Servers auf Abfragen benutzerspezifisch zu konfigurieren.

Dies ist vor allem dann nützlich, wenn Sie nicht möchten, dass externe Clients einen bestimmten DNS-Dienst ausführen oder bestimmte Informationen sehen können, während Sie dies auf dem lokalen Netzwerk internen Clients ermöglichen.

Die `view`-Anweisung verwendet die `match-clients`-Option, um IP-Adressen oder ganze Netzwerke zu vergleichen und diesen spezielle Optionen und Zone-Daten zu geben.

12.5.3. Sicherheit

BIND unterstützt eine Reihe verschiedener Methoden, um das Updaten von Zonen auf Master- oder Slave-Nameservern zu schützen:

- *DNSSEC* — Abkürzung für *DNS SECurity*. Dieses Feature ist für Zonen, die mit einem *Zonenschlüssel* kryptographisch signiert werden, bestimmt.

  Auf diese Weise kann sichergestellt werden, dass die Informationen über eine spezielle Zone von einem Nameserver stammen, der mit einem bestimmten privaten Schlüssel signiert wurde, und der Empfänger über den öffentlichen Schlüssel dieses Nameservers verfügt.

  Version 9 von BIND unterstützt auch die SIG(0) öffentlicher/privater Schlüssel Methode für die Authentifizierung von Nachrichten.

- *TSIG* — Abkürzung für *Transaction SIGnatures*, ein gemeinsam verwendeter geheimer Schlüssel auf dem Master- und Slave-Name-Server, der sicherstellt, dass die Übertragungen zwischen dem Master- und dem Slave-Name-Server authorisiert sind.

  Dieses Feature unterstützt die auf der IP-Adresse basierende Methode der Transfer-Authorisierung. Somit muss ein unerwünschter Benutzer nicht nur Zugriff auf die IP-Adresse haben, um die Zone zu übertragen, sondern auch den geheimen Schlüssel kennen.

  Version 9 von BIND unterstützt auch *TKEY*, eine weitere Methode der Autorisierung von Zone-Übertragungen auf der Basis eines gemeinsam verwendeten geheimen Schlüssels.

12.5.4. IP-Version 6

Die Version 9 von BIND kann mit den `A6` Zone-Records Name-Service für die IP-Version 6 (IPv6)-Umgebungen zur Verfügung stellen.

Wenn Ihre Netzwerkumgebung sowohl über Ipv4- als auch IPv6-Hosts verfügt, können Sie den `lwresd` Lightweight Resolver Daemon in Ihren Netzwerk-Clients verwenden. Dieser Daemon ist ein sehr effektiver Caching-Only-Name-Server, der die neuesten `A6`- und `DNAME`-Records versteht, die mit Ipv6 verwendet werden. Auf der `lwresd`-man-Seite finden Sie weitere Informationen hierzu.

12.6. Allgemein zu vermeidende Fehler

Es kommt häufig vor, dass Anfänger bei der Bearbeitung der Konfigurationsdateien von BIND Fehler machen oder bei der Verwendung von `named` zunächst Schwierigkeiten haben. Viele der nachfolgend beschriebenen Probleme können Sie aber vermeiden, wenn Sie Folgendes beachten:

- *Erhöhen Sie die Seriennummer, wenn Sie eine Zone-Datei bearbeiten.*

  Wenn die Seriennummer nicht erhöht wird, hat Ihr Master-Name-Server zwar die korrekten neuen Informationen, Ihr Slave-Name-Server wird jedoch nie über diese Änderungen oder den Versuch informiert, die Daten in der Zone zu aktualisieren. Die Seriennummer stimmt mit der des Master-Servers überein, auch wenn sich die Daten für die Zone von denen des Master-Name-Servers vollkommen unterscheiden.
- *Achten Sie darauf, dass Sie geschweifte Klammern und Strichpunkte in der `/etc/named.conf`-Datei richtig verwenden.*

  Ein ausgelassener Strichpunkt oder eine nicht geschlossene geschweifte Klammer kann dazu führen, dass `named` nicht startet.
- *Denken Sie daran, in den Zone-Dateien nach jedem FQDN Punkte (`.`) zu setzen und sie beim Hostnamen wegzulassen.*

  Der Punkt bedeutet, dass der angegebene Name komplett ist. Wird er weggelassen, platziert `named` den Namen der Zone oder des `$ORIGIN`-Werts hinter den Namen, um ihn zu vervollständigen.
- *Wenn Ihre Firewall Verbindungen von Ihrem `named` zu anderen Nameservern blockiert, müssen Sie möglicherweise die Konfigurationsdatei bearbeiten.*

  Standardmäßig verwendet die Version 9 von BIND willkürliche Ports oberhalb von 1024, um andere Name-Server abzufragen. Einige Firewalls gehen jedoch von Name-Servern aus, die für die Kommunikation nur den Port 53 verwenden. Sie können dieses Verhalten erzwingen, indem Sie in `/etc/named.conf` folgende Zeile zur `options`-Direktive hinzufügen:

  ```
  query-source address * port 53;
  ```

12.7. Zusätzliche Ressourcen

Folgende Quellen enthalten zusätzliche Hintergrundinformationen zu BIND.

12.7.1. Installierte Dokumentation

- BIND verfügt über installierte Dokumentationen, die verschiedene Themen behandeln und jeweils in einem eigenen Verzeichnis abgelegt sind:
  - `/usr/share/doc/bind-<version-number>/` — Enthält eine `README`-Datei mit einer Liste der neuesten Features.

- `/usr/share/doc/bind-<version-number>/arm/` — Enthält das *BIND 9 Administrator Reference Manual* im HTML- und SGML-Format, mit Details über die für BIND erforderlichen Ressourcen, zur Konfigurationsweise der verschiedenen Name-Server-Typen, zur Durchführung des Load-Balancing und anderen spezielleren Themen. Die meisten neuen Benutzer werden sich mit dieser Informationsquelle am besten mit BIND vertraut machen können.
- `/usr/share/doc/bind-<version-number>/draft/` — Enthält ausgewählte technische Dokumente, die sich mit den Problemen beschäftigen und einige Methoden zur Lösung dieser Probleme vorschlagen.
- `/usr/share/doc/bind-<version-number>/misc/` — Enthält Dokumente über spezielle verbesserte Merkmale. Benutzer der Version 8 von BIND sollten sich das Dokument `migration` anschauen, das sich mit bestimmten Änderungen befasst, die für eine Verwendung der Version 9 von BIND vorzunehmen sind. In der `options`-Datei sind alle in BIND 9 implementierten Optionen aufgelistet, die in `/etc/named.conf` verwendet werden.
- `/usr/share/doc/bind-<version-number>/rfc/` — In diesem Verzeichnis finden Sie jedes RFC-Dokument, das mit BIND zusammenhängt.

- `man named` — Untersucht ausgewählte Argumente, die zur Steuerung des BIND-Name-Server-Daemon verwendet werden können.
- `man named.conf` — Eine vollständige Liste von Optionen, welche in der `named`-Konfigurationsdatei zur Verfügung stehen.
- `man rndc` — Erklärt die verschiedenen Optionen, die bei der Verwendung von `rndc` zur Kontrolle eines BIND Name-Servers zur Verfügung stehen.
- `man rndc.conf` — A Eine vollständige Liste von Optionen, welche in der `rndc`-Konfigurationsdatei zur Verfügung stehen.

12.7.2. Hilfreiche Webseiten

- http://www.isc.org/products/BIND — Die Homepage des BIND-Projekts. Hier finden Sie Informationen aktuellen Releases und können das *BIND 9 Administrator Reference Manual* in der PDF-Version herunterladen.
- http://www.redhat.com/mirrors/LDP/HOWTO/DNS-HOWTO.html — Befasst sich mit BIND als Caching-Nameserver und der Konfiguration der einzelnen Zone-Dateien sowie der Konfiguration verschiedener Zone-Dateien, die als primärer Name-Server für eine Domain benötigt werden.

12.7.3. Bücher zum Thema

- *DNS and BIND* von Paul Albitz und Cricket Liu; O'Reilly & Associates — Ein bekanntes Buch, das allgemeine und weiterführende Optionen der Konfiguration von BIND erklärt und Strategien zum Schutz Ihres DNS-Servers vorstellt.
- *The Concise Guide to DNS and BIND* von Nicolai Langfeldt; Que — Beschreibt die Verbindungen zwischen mehreren Netzwerkdiensten und BIND mit Schwerpunkt auf aufgabenorientierten technischen Themen.

redhat

Kapitel 13.

Lightweight Directory Access Protocol (LDAP)

LDAP (*Lightweight Directory Access Protocol*) ist ein Satz von offenen Protokollen, die zum Zugreifen auf zentral gespeicherte Informationen über ein Netzwerk verwendet werden. Es basiert auf dem *X.500*-Standard für das gemeinsame Nutzen von Verzeichnissen, ist jedoch weniger komplex und ressourcenintensiv. Aus diesem Grund wird LDAP bisweilen auch *X.500 Lite* genannt.

Ebenso wie X.500 organisiert LDAP die Informationen mit Hilfe von Verzeichnissen hierarchisch. In den Verzeichnissen kann eine Vielfalt an Informationen gespeichert werden. Zudem können sie auf ähnliche Weise wie der Network Information Service (NIS) verwendet werden, so dass alle Benutzer von jedem beliebigen Rechner in einem LDAP-unterstützten Netzwerk auf ihre Accounts zugreifen können.

In den meisten Fällen wird LDAP jedoch einfach als virtuelles Telefonbuch verwendet, mit dem Benutzer auf auf Kontaktinformationen für andere Benutzer zugreifen können. LDAP geht allerdings über ein herkömmliches Telefonbuch hinaus, da es seine Verzeichnisse auf andere LDAP-Server weltweit übertragen und somit globalen Zugriff auf Informationen zur Verfügung stellen kann. Momentan wird LDAP allerdings in der Regel eher in Einzelorganisationen wie Universitäten, Regierungsabteilungen und Privatunternehmen verwendet.

LDAP ist ein Client-Server-System. Der Server kann eine Vielfalt an Datenbanken zum Speichern eines Verzeichnisses verwenden, wobei jede für schnelle und umfangreiche Lesevorgänge optimiert ist. Wenn eine LDAP-Clientanwendung eine Verbindung mit einem LDAP-Server herstellt, kann sie entweder ein Verzeichnis abfragen oder Informationen hochladen. Im Fall einer Abfrage antwortet der Server entweder auf die Abfrage oder, wenn er nicht lokal antworten kann, verweist er den Anfrage-Upstream an einen übergeordneten LDAP-Server weiter, der die Antwort übernimmt. Versucht die Clientanwendung, Informationen in ein LDAP-Verzeichnis zu laden, prüft der Server, ob der Benutzer zum Ausführen der Änderung berechtigt ist und fügt dann die Informationen hinzu bzw. aktualisiert sie.

In diesem Kapitel wird die Konfiguration und Verwendung von OpenLDAP 2.0, einer Open-Source-Implementierung des LDAPv2- und LDAPv3-Protokolls behandelt.

13.1. Warum LDAP?

Der Hauptvorteil von LDAP ist die Verdichtung von bestimmten Informationen für eine gesamte Organisation in ein zentrales Repository. So kann LDAP zum Beispiel für das Verwalten von Benutzerlisten für alle Gruppen einer Organisation als ein zentrales Verzeichnis verwendet werden, auf das vom gesamten Netzwerk aus zugegriffen werden kann. Und da LDAP SSL (Secure Sockets Layer) und TLS (Transport Layer Security) unterstützt, können sensible Daten vor neugierigen Augen geschützt werden.

LDAP unterstützt auch viele Backend-Datenbanken, in denen die Verzeichnisse gespeichert werden. Die Administratoren verfügen hierdurch über die notwendige Flexibilität, eine Datenbank bereitzustellen, die für die Informationsarten, die der Server verbreiten soll, optimal angepasst ist. Des Weiteren verfügt LDAP über eine gut durchdachte API (Application Programming Interface), und es sind auch zahlreiche LDAP-fähige Applikationen vorhanden, deren Anzahl und Qualität zunimmt.

Der Nachteil von LDAP ist die Konfiguration, die nicht unbedingt leicht ist.

13.1.1. Funktionserweiterungen von OpenLDAP 2.0

OpenLDAP 2.0 umfasst zahlreiche wichtige Funktionen.

- *LDAPv3 Support — LDAPv3-Support* — OpenLDAP 2.0 unterstützt SASL (Simple Authentication and Security Layer), TLS (Transport Layer Security) und SSL (Secure Sockets Layer) neben weiteren Verbesserungen. Viele Änderungen, die seit LDAPv2 am Protokoll vorgenommen wurden, sollen zur Sicherheit von LDAP beitragen.
- *IPv6 Support* — OpenLDAP unterstützt die nächste Generation des Internetprotokolls, Version 6.
- *LDAP Over IPC* — OpenLDAP kann innerhalb eines bestimmten Systems mit Hilfe von IPC (Interprocess Communication) kommunizieren. Das Umgehen der Kommunikation über ein Netzwerk erhöht die Sicherheit.
- *Aktualisierte C API* — Verbessert die Art und Weise, in welcher Programmierer zu LDAP Verzeichnis-Servern verbinden und mit diesen arbeiten.
- *LDIFv1 Support* — OpenLDAP 2.0 ist mit LDAP Data Interchange Format (LDIF) Version 1 voll kompatibel.
- *Verbesserter Stand-Alone LDAP Server* — OpenLDAP enthält jetzt ein aktualisiertes Zugriffssteuerungssystem, Thread-Pooling, bessere Tools und vieles mehr.

13.2. LDAP Terminologie

Jede Diskussion des LDAP erfordert ein grundlegendes Verständnis einiger LDAP-spezifischen Begriffe:

- *Eintrag* — Ein Eintrag (Entry) stellt in einem LDAP-Verzeichnis eine Einheit dar. Ein Eintrag wird durch seinen eindeutigen Namen (Distinguished Name, DN) identifiziert.
- *Attribute* — Attribute sind direkt mit dem Eintrag zusammenhängende Informationen. 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 u.a. Telefonnummern und E-Mail-Adressen.

  Bestimmte Attribute sind obligatorisch, während andere Attribute optional sind. In einer *Objektklasse* (Objectclass) ist festgelegt, welche Attribute pro Eintrag obligatorisch und welche optional sind. Die Objektklassendefinitionen sind in verschiedenen Schemadateien im Verzeichnis `/etc/openldap/schema` abgelegt. Für mehr Information zu LDAP Schemata, siehe Abschnitt 13.5.
- *LDIF* — Das *LDAP-Datenaustauschformat* (LDAP Data Interchange Format, LDIF) ist ein ASCII-Textformat für LDAP-Einträge. Dateien, die Daten von einem LDAP-Server importieren oder auf einen LDAP-Server exportieren, müssen im LDIF-Format vorliegen. Ein LDIF-Eintrag sieht zum Beispiel folgendermaßen aus:

  ```
  [<id>]
  dn: <distinguished name>
  <attrtype>: <attrvalue>
  <attrtype>: <attrvalue>
  <attrtype>: <attrvalue>
  ```

  Ein Eintrag kann so viele der `<attrtype>: <attrvalue>` Paare haben, wie erforderlich. Eine leere Zeile markiert das Ende eines Eintrags.

Achtung

Alle der `<attrtype>` und `<attrvalue>` Paare *müssen* in einer entsprechenden Schemadatei definiert sein, um diese Informationen verwenden zu können.

Alle Angaben innerhalb der spitzen Klammern "<" und ">" sind Variablen und können mit Ausnahme von *<ID>* beim Erstellen eines neuen LDAP-Eintrags festgelegt werden. Die *<ID>* ist eine Zahl, die von der Anwendung festgelegt wird, wenn der Eintrag bearbeitet wird.

Anmerkung

YSie sollten LDIF-Einträge nie manuell bearbeiten. Verwenden Sie stattdessen eine LDAP-Clientanwendung, wie eine der in Abschnitt 13.3 aufgezählten.

13.3. OpenLDAP Daemons and Utilities

Die Suite der OpenLDAP Bibliotheken ist über folgende Pakete verteilt:

- `openldap` — Enthält die Bibliotheken welche zum Ausführen der OpenLDAP Server- und Client-Applikationen benötigt werden.
- `openldap-clients` — Enthält die Befehlszeilentools zur Ansicht und zum Verändern der Verzeichnisse auf einem LDAP-Server.
- `openldap-server` — Enthält die Server und andere Tools, welche zum Konfigurieren und für den Betrieb eines LDAP Servers benötigt werden.

Das `openldap-servers`-Paket enthält zwei Server: den *Standalone LDAP Daemon* (`/usr/sbin/slapd`) und den *Standalone LDAP Update Replication Daemon* (`/usr/sbin/slurpd`).

Der `slapd`-Daemon ist der eigenständige LDAP-Server, während der `slurpd`-Daemon zum Synchronisieren der Änderungen von einem LDAP-Server auf andere LDAP-Server im Netzwerk verwendet wird. Der `slurpd`-Daemon ist nur erforderlich, wenn mehrere LDAP-Server verwendet werden.

Das `openldap-server`-Paket installiert zum Durchführen von Verwaltungsaufgaben folgende Utilities in `/usr/sbin`:

- `slapadd` — Fügt Einträge aus einer LDIF-Datei in ein LDAP-Verzeichnis ein. `/usr/sbin/slapadd -l` *`ldif-Eingabe`* liest die LDIF-Datei, *`ldif-Eingabe`*, welche die neuen Einträge enthält.
- `slapcat` — Entnimmt Einträge aus einem LDAP-Verzeichnis im Standardformat — Berkeley DB — und speichert diese in einer LDIF-Datei. Der Befehl `/usr/sbin/slapcat -l` *`ldif-Ausgabe`* gibt zum Beispiel eine LDIF-Datei *`ldif-Ausgabe`* aus, welche die Einträge aus dem LDAP-Verzeichnis enthält.
- `slapindex` — Indiziert das `slapd`-Verzeichnis auf Grundlage des aktuellen Inhalts neu.
- `slappasswd` — Generiert einen verschlüsselten Wert eines Benutzerpasswortes zur Verwendung mit dem `ldapmodify`- oder `rootpw`-Wert in der slapd-Konfigurationsdatei `/etc/openldap/slapd.conf`. Führen Sie `/usr/sbin/slappasswd` aus, um das Passwort zu erstellen.

Warnung

Stellen Sie sicher, dass `slapd` mit Hilfe von `/usr/sbin/service slapd stop` angehalten wird, bevor Sie `slapadd`, `slapcat` oder `slapindex` verwenden. Andernfalls riskieren Sie die Integrität des LDAP-Verzeichnis.

Weitere Informationen zur Verwendung dieser Utilities finden Sie auf den jeweiligen man-Seiten.

Das `openldap-clients`-Paket installiert Tools zum Hinzufügen, Ändern und Löschen von Einträgen eines LDAP-Verzeichnisses in `/usr/bin/`. Diese Tools beinhalten Folgendes:

- `ldapmodify` — Ändert Einträge in einem LDAP-Verzeichnis durch Eingaben aus einer Datei oder von der Standardeingabe.
- `ldapadd` — Fügt durch Annehmen von Eingaben über eine Datei oder der Standardeingabe Einträge zum Verzeichnis hinzu. `ldapadd` ist nichts anderes als ein harter Link zu `ldapmodify -a`.
- `ldapsearch` — Sucht mit Hilfe eines Shell-Prompts im LDAP-Verzeichnis nach Einträgen.
- `ldapdelete` — Löscht Einträge aus einem LDAP-Verzeichnis durch Annehmen von Eingaben des Benutzers am Terminal oder über eine Datei.

Alle Utilities, `ldapsearch` ausgenommen, sind einfacher durch Verweisen auf eine Datei mit den vorzunehmenden Änderungen zu verwenden, als durch Eingabe eines Befehls für jeden Eintrag, der in einem LDAP-Verzeichnis geändert werden soll. Das Format solcher Dateien wird auf der man-Seite der jeweiligen Applikation skizziert.

13.3.1. NSS, PAM, and LDAP

Neben den OpenLDAP-Paketen enthält Red Hat Linux das Paket `nss_ldap`, welches die Möglichkeit LDAP in Linux- und andere UNIX-Umgebungen zu integrieren optimiert.

Das Paket `nss_ldap` stellt folgende Module zur Verfügung:

- `/lib/libnss_ldap-<glibc-version>.so`
- `/lib/security/pam_ldap.so`

Die `libnss_ldap-<glibc-version>.so` Module ermöglichen Applikationen, Benutzer, Gruppen, Hosts und sonstige Informationen mit Hilfe eines LDAP-Verzeichnisses über die Schnittstelle *Nameservice Switch* (NSS) zu suchen. NSS erlaubt Applikationen eine Authetifizierung unter Verwendung von LDAP in Verbindung mit dem Name-Service *Network Information Service* (NIS) und Klartext-Authentifizierungsdateien.

Das Modul `pam_ldap` ermöglicht PAM-fähigen Applikationen, Benutzer mit Hilfe von in einem LDAP-Verzeichnis gespeicherten Informationen zu authentifizieren. PAM-fähige Applikationen umfassen Konsolenanmeldung, POP- und IMAP-Mail-Server und Samba. Wenn ein LDAP-Server im Netzwerk bereitgestellt wird, können alle Anmeldesituationen gegen eine Benutzer-ID und Passwortkombination authentifizieren und so die Verwaltung spürbar vereinfachen.

13.3.2. PHP4, Apache HTTP-Server, und LDAP

Red Hat Linux enthält auch Pakete mit LDAP-Modulen für Apache HTTP-Server und PHP-serverseitige Skriptsprache.

Das Paket `php-ldap` fügt LDAP-Unterstützung zur PHP4 HTML-eingebetteten Skriptsprache über das Modul `/usr/lib/php4/ldap.so` hinzu. Dieses Modul ermöglicht PHP4-Skripten, auf Informationen zuzugreifen, die in einem LDAP-Verzeichnis gespeichert sind.

Wichtig

Red Hat Linux wird nicht länger mit dem Paket `auth_ldap` ausgeliefert. Dieses Paket stellte LDAP-Support für Versionen 1.3 und früher von Apache HTTP-Server bereit. Sehen Sie die Webseiten der Apache Software Foundation unter http://www.apache.org/ für detaillierte Informationen zum Status dieses Moduls.

13.3.3. LDAP Client-Applikationen

Es stehen grafische LDAP-Clients zur Verfügung, die das Erstellen und Ändern von Verzeichnissen unterstützen. Diese sind allerdings nicht im Lieferumfang von Red Hat Linux enthalten. Eine solche Anwendung ist **LDAP Browser/Editor** — Ein Java-basiertes Tool, das unter http://www.iit.edu/~gawojar/ldap zur Verfügung steht.

Die meisten anderen LDAP-Clients greifen auf die Verzeichnisse im Lesemodus zu und verwenden sie zum Verweisen (und nicht Ändern) auf unternehmensweite Informationen. Beispiele für diese Anwendungen sind Mozilla-basierte Web-Browser, Sendmail **Balsa**, **Pine**, **Evolution**, **Gnome Meeting**.

13.4. OpenLDAP Konfigurationsdateien

Die Konfigurationsdateien von OpenLDAP werden im Verzeichnis `/etc/openldap/` installiert. Im Folgenden werden die wichtigsten Verzeichnisse und Dateien kurz vorgestellt:

- `/etc/openldap/ldap.conf` — Dies ist die Konfigurationsdatei für alle *Client*-anwendungen, die die OpenLDAP-Bibliotheken verwenden. Darunter befinden sich unter anderem Sendmail, **Pine**, **Balsa**, **Evolution** und **Gnome Meeting**.
- `/etc/openldap/schema/`-Verzeichnis — Dieses Unterverzeichnis enthält das vom `slapd`-Daemon verwendete Schema. Weitere Informationen zu diesem Verzeichnis finden Sie unter Abschnitt 13.5.
- `/etc/openldap/slapd.conf` — Dies ist die Konfigurationsdatei für den `slapd`-Daemon. Weitere Informationen zu dieser Datei finden Sie unter Abschnitt 13.6.1.

Anmerkung

Wenn das `nss_ldap`-Paket installiert ist, erstellt es die Datei `/etc/ldap.conf`. Diese Datei wird von den PAM- und NSS-Modulen verwendet, die vom `nss_ldap`-Paket bereitgestellt werden. Weitere Informationen zu dieser Konfigurationsdatei finden Sie unter Abschnitt 13.7.

13.5. Das Verzeichnis `/etc/openldap/schema/`

Das `/etc/openldap/schema/`-Verzeichnis beinhaltet die LDAP-Definition, 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. Auf die verschiedenen Schemadateien wird in `/etc/openldap/slapd.conf` mit Hilfe der `include`-Zeilen verwiesen, wie im folgenden Beispiel zu sehen ist:

```
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
```

Achtung

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

Sie können das von OpenLDAP verwendete Schema erweitern, um zusätzliche Attributtypen und Objektklassen mit Hilfe der Standardschemadateien zu unterstützen. Erstellen Sie dafür eine `local.schema`-Datei im Verzeichnis `/etc/openldap/schema`. Referenzieren Sie dieses neue Schema in `slapd.conf`, indem Sie die folgende Zeile unter die standardmäßigen `include`-Schemazeilen hinzufügen:

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

Definieren Sie anschließend Ihre neuen Attributtyen und Objektklassen der `local.schema`-Datei. Viele Organisationen verwenden die standardmäßig installierten Attributtypen und Objektklassen der Schemadateien und modifizieren diese für die Verwendung in der `local.schema`-Datei.

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

13.6. Überblick über die OpenLDAP-Einrichtung

In diesem Abschnitt wird ein kurzer Überblick über das Installieren und Konfigurieren eines OpenLDAP-Verzeichnisses gegeben. Weitere Details finden Sie unter folgenden URLs:

- http://www.openldap.org/doc/admin/quickstart.html — Der *Quick-Start Guide* auf der OpenLDAP-Website.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — *LDAP Linux HOWTO* vom Linux Documentation Project, das auf der Website von Red Hat gespiegelt ist.

Die Grundschritte zum Erstellen eines LDAP-Servers sind folgende:

1. Installieren Sie die RPMs `openldap`, `openldap-servers` und `openldap-clients`.
2. Bearbeiten Sie die Datei `/etc/openldap/slapd.conf`, um auf die LDAP-Domain und den LDAP-Server zu verweisen. Weitere Informationen finden Sie unter Abschnitt 13.6.1.
3. Starten Sie `slapd` mit folgendem Befehl:
   ```
   /sbin/service/ldap start
   ```
   Nachdem Sie LDAP korrekt konfiguriert haben, können Sie `chkconfig`, `ntsysv` oder **redhat-config-services** verwenden, um LDAP so zu konfigurieren, dass es zur Bootzeit gestartet wird. Weitere Informationen zum Konfigurieren von Diensten finden Sie im Kapitel *Kontrolle des Zugriffs auf die Dienste* im *Official Red Hat Linux Customization Guide*.
4. Fügen Sie Einträge zum LDAP-Verzeichnis mit Hilfe von `ldapadd` hinzu.
5. Verwenden Sie `ldapsearch`, um zu prüfen, ob `slapd` korrekt auf die Informationen zugreift.
6. Wenn Sie an diesem Punkt angelangt sind, sollte Ihr LDAP-Verzeichnis ordnungsgemäß funktionieren, und Sie können alle LDAP-fähigen Anwendungen für die Verwendung des LDAP-Verzeichnisses konfigurieren.

13.6.1. Bearbeiten des Verzeichnisses `/etc/openldap/slapd.conf`

Sie müssen die Konfigurationsdatei `/etc/openldap/slapd.conf` des `slapd`-LDAP-Servers ändern, um ihn verwenden zu können. Sie müssen diese Datei bearbeiten, um sie an Ihre Domain und Server anzupassen.

Die `Suffix`-Zeile nennt die Domain, für die der LDAP-Server Informationen bereitstellt und sollte wie folgt geändert werden:

```
suffix          "dc=your-domain,dc=com"
```

Hier muss ein gültiger Domainname eingetragen werden. Zum Beispiel:

```
suffix          "dc=example,dc=com"
```

Der Eintrag `rootdn` ist der *eindeutige Name* (*DN*) für einen Benutzer, der keinen Einschränkungen durch Parameter der Zugriffssteuerung oder Benutzerverwaltung unterliegt, die im LDAP-Verzeichnis für Vorgänge festgelegt sind. Der Benutzer `rootdn` ist sozusagen Root für das LDAP-Verzeichnis. Die `rootdn`-Zeile ist zu ändern in:

```
rootdn          "cn=root,dc=example,dc=com"
```

Wenn Sie vorhaben, dass LDAP-Verzeichnis übers Netzwerk zu verwalten, ändern Sie die `rootpw`-Zeile — indem Sie den Standardwert mit einem verschlüsselten Passwort ersetzen. Um ein verschlüsseltes Passwort zu erzeugen, geben Sie den folgenden Befehl ein:

```
slappasswd
```

Sie werden dazu aufgefordert, ein Passwort einzugeben, und durch eine zweite Eingabe zu bestätigen. Danach gibt das Programm das verschlüsselte Passwort am Terminal aus.

Als nächstes, kopieren Sie das neu erzeugte verschlüsselte Passwort in die Datei `/etc/openldap/slapd.conf` in eine der `rootpw`-Zeilen, und entfernen Sie das Hash-Symbol (`#`).

Nach Abschluss, sollte die `rootpw`-Zeile etwa wie folgt aussehen:

```
rootpw {SSHA}vv2y+i6V6esazrIv70xSSnNAJE18bb2u
```

Warnung

LDAP-Passwörter einschließlich der in `/etc/openldap/slapd.conf` angegebenen `rootpw`-Direktive werden als Klartext über das Netzwerk gesendet, es sei denn, Sie aktivieren die TLS-Verschlüsselung.

Für zusätzliche Sicherheit sollte die `rootpw`-Direktive nur verwendet werden, wenn die Anfangskonfiguration und Auffüllung des LDAP-Verzeichnisses über ein Netzwerk erfolgt. Nach Vervollständigen der Aufgabe ist es das Beste, die `rootpw`-Direktive auszukommentieren, indem ihr ein Gatterzeichen (#) vorangestellt wird.

Wenn Sie das Befehlszeilentool `/usr/bin/slapadd` verwenden, um das LDAP-Verzeichnis lokal aufzufüllen, müssen Sie die `rootpw`-Direktive nicht verwenden.


Wichtig

Sie müssen root sein um `/usr/sbin/slapadd` zu verwenden. Der Verzeichnis-Server wird jedoch als Benutzer `ldap` ausgeführt. Der Verzeichnis-Server ist deshalb nicht in der Lage, Dateien, welche von `slapadd` erzeugt wurden, zu ändern. Um dieses Problem zu beheben, geben Sie den folgenden Befehl ein, nachdem Sie `slapadd` beendet haben:

```
chown -R ldap /var/lib/ldap
```

13.7. 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 13.9 angegebenen Literaturhinweisen.

Installieren der notwendigen LDAP-Pakete

Zuerst sollten Sie sicherstellen, dass die erforderlichen Pakete auf beiden, dem LDAP-Server und dem LDAP-Client installiert sind. Der LDAP-Server benötigt das `openldap-server` Paket.

Die Pakete `openldap`, `openldap-clients`, und `nss_ldap` müssen auf allen LDAP Client-Maschinen installiert sein.

Bearbeiten der Konfigurationsdateien

- Bearbeiten Sie die Datei `/etc/openldap/slapd.conf` auf dem LDAP-Server, um sicherzustellen, dass diese mit den Gegebenheiten Ihrer Organisation übereinstimmt. Bitte sehen Sie Abschnitt 13.6.1 für Anleitungen zum Bearbeiten der Datei `slapd.conf`.
- Auf allen Client-Rechnern müssen sowohl `/etc/ldap.conf` als auch `/etc/openldap/ldap.conf` den jeweiligen Server und grundlegende Informationen für Ihre Organisation enthalten.

  Die einfachste Weise hierzu ist das Ausführen von **Authentifizierungs-Konfigurations-Tool** (`authconfig-gtk`) und das Auswählen von **LDAP verwenden** in der Tab **Benutzerinformationen**.

  Diese Dateien können auch manuell bearbeitet werden.
- Auf allen Client-Maschinen, muss die Datei `/etc/nsswitch.conf` bearbeitet werden um LDAP zu verwenden.

  Die einfachste Weise hierzu ist das Ausführen von **Authentifizierungs-Konfigurations-Tool** (`authconfig-gtk`) und das Auswählen von **LDAP verwenden** in der Tab **Benutzerinformationen**.

  Wenn Sie `/etc/nsswitch.conf` manuell bearbeiten, fügen Sie `ldap` in den entsprechenden Zeilen hinzu.

  Zum Beispiel:

  ```
  passwd: files ldap
  shadow: files ldap
  group: files ldap
  ```

13.7.1. PAM and LDAP

Führen Sie `authconfig` aus, und wählen Sie die Option **LDAP verwenden** im Tab **Authentifizierung** aus, damit Sie standardmäßige PAM-fähige Anwendungen für die Authentifizierung mit LDAP verwenden können. Weitere Informationen zum Konfigurieren von PAM finden Sie unter Kapitel 14 sowie auf den man-Seiten von PAM.

13.7.2. Umwandeln Ihrer alten Authentifizierungsinformationen in das LDAP-Format

Das Verzeichnis `/usr/share/openldap/migration/` enthält mehrere Shell- und Perl-Skripte zur Umwandlung Ihrer alten Authentifizierungsinformationen in das LDAP-Format.

Zuerst müssen Sie die Datei `migrate_common.ph` an Ihre Domain anpassen. Die Standardwerte der Standard-DNS-Domain müssen ähnlich wie folgt geändert werden:

```
$DEFAULT_MAIL_DOMAIN = "your_company";
```

Die Standardannahme muss ebenfalls geändert werden von:

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

Das Umwandeln einer Benutzerdatenbank in ein LDAP-Format kann in eine Gruppe von Umwandlungsskripten unterteilt werden, die mit dem Paket `nss_ldap` installiert wurden. Entscheiden Sie mit Hilfe von Tabelle 13-1, welches Skript zur Umwandlung der Benutzerdatenbank ausgeführt werden soll.

Vorhandener Namensdienst	Wird LDAP ausgeführt?	Zu verwendendes Skript
`/etc` Klartext-Dateien	Ja	`migrate_all_online.sh`
`/etc` Klartext-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`

Tabelle 13-1. LDAP Umwandlungsskripte

Führen Sie das Ihrem vorhandenen Name-Service entsprechende Skript aus.

Anmerkung

Um einige dieser Skripte ausführen zu können, müssen Sie Perl auf Ihrem System installiert haben.

Die Dateien `README` und `migration-tools.txt` im Verzeichnis `/usr/share/openldap/migration/` enthalten weitere Detailinformationen zum Umwandeln der Informationen.

13.8. Aktualisieren auf OpenLDAP Version 2.0

In OpenLDAP Version 2.0 wurde das Speicherformat vom `slapd` LDAP Server geändert. Wenn Sie LDAP von Red Hat Linux 7.0 oder früher aktualisieren, müssen Sie die existierenden LDAP Verzeichnisse mithilfe des folgenden Befehls in eine LDIF-Datei exportieren:

```
ldbmcat -n > <ldif_file>
```

Geben Sie im obigen Befehl als *<ldif_file>* den Namen der Ausgabedatei ein. Geben Sie anschließend den folgenden Befehl ein, um die Datei in OpenLDAP zu importieren: 2.0:

```
slapadd -l <ldif_file>
```

Wichtig

Sie müssen root sein um `/usr/sbin/slapadd` zu verwenden. Der Verzeichnis-Server wird jedoch als Benutzer `ldap` ausgeführt. Der Verzeichnis-Server ist deshalb nicht in der Lage, Dateien, welche von `slapadd` erzeugt wurden, zu ändern. Um dieses Problem zu beheben, geben Sie den folgenden Befehl ein, nachdem Sie `slapadd` beendet haben:

```
chown -R ldap /var/lib/ldap
```

13.9. Zusätzliche Ressourcen

Es sind weitere, LDAP betreffende Informationen erhältlich. Konsultieren Sie bitte diese Quellen, insbesondere die OpenLDAP-Website und das LDAP- HOWTO, ehe Sie LDAP auf Ihrem System konfigurieren.

13.9.1. Installierte Dokumentationen

- LDAP-man-Seiten — Die `ldap`-man-Seite ist sehr gut geeignet, um eine Einführung in LDAP zu erhalten. Man- Seiten gibt es auch für die verschiedenen LDAP-Daemonen und -Dienstprogramme.
- `/usr/share/docs/openldap-`*<Versionsnummer>* — Enthält allgemeine `README`-Dokument- und sonstige Informationen.

13.9.2. Hilfreiche Websites

- http://www.openldap.org — Homepage des OpenLDAP-Projekts. Auf dieser Website finden Sie äußerst viele Informationen zum Konfigurieren von OpenLDAP.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — Ein älteres, aber immer noch relevantes LDAP-HOWTO.
- http://www.padl.com — Entwickler von `nss_ldap` und `pam_ldap`, neben vielen anderen hilfreichen LDAP-Tools.
- http://www.innosoft.com/ldapworld — Enthält Informationen zu LDAP-RFCs und LDAP Version 3-Spezifikationen.
- http://www.kingsmountain.com/ldapRoadmap.shtml — Jeff Hodges' LDAP Road Map enthält Links für verschiedene hilfreiche FAQs und aktuelle Neuigkeiten über das LDAP-Protokoll.

- http://www.rudedog.org/auth_ldap — Homepage des `auth_ldap`-Authentifizierungsmoduls für Apache HTTP-Server.
- 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 Verzeichnis- strukturen.

13.9.3. Bücher zum Thema

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

III. Sicherheit

Die Verwendung von sicheren Protokollen ist ein kritischer Punkt in der Gewährleistung der Integrität des Systems. Dieser Teil beschreibt entscheidende Tools zur Authentifizerung von Benutzern, Kontrolle des Netzwerkszugriffs, sicheren Kommunikataion über das Netzwerk und Erkennung von Angreifern. Weitere Informationen zur Sicherung eines Red Hat Linux Systems finden Sie im *Red Hat Linux Security Guide*.

Inhaltsverzeichnis

Kapitel 14.

Pluggable Authentication Modules (PAM)

Programme, die Benutzern Zugriff zu einem System gewähren, überprüfen die Identität der Benutzer durch einen Prozess, der *Authentifizierung* genannt wird. Historisch haben alle diese Programme ihren eigenen Weg, die Authentifizierung durchzuführen. Unter Red Hat Linux sind viele dieser Programme dafür konfiguriert, einen zentralisierten Authentifizierungsprozess zu benutzen, der *Pluggable Authentication Modules* (*PAM*) genannt wird.

PAM benutzt eine auswechselbare, modulare Architektur, welche dem System-Administrator einen hohen Grad an Flexibilität beim Einstellen der Authentifizierungsregeln des Systems bereit stellt.

Es ist kaum notwendig, die Standard PAM Konfigurationsdateien für eine Applikation, welche PAM verwendet, zu ändern. Hin und wieder kann es allerdings notwendig werden, eine PAM Konfigurationsdatei zu ändern. Da eine falsche Einstellung in der PAM Konfigurationsdatei die Systemsicherheit kompromitieren kann, sollten Sie mit der Struktur der Konfigurationsdateien von PAM vertraut sein, bevor Sie eventuelle Änderungen vornehmen (weitere Informationen finden Sie unter Abschnitt 14.3).

14.1. Vorteile von PAM

PAM bietet die folgenden Vorteile:

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

14.2. PAM-Konfigurationsdateien

Die PAM-Konfigurationsdateien sind im Verzeichnis `/etc/pam.d/` enthalten. In früheren Versionen von PAM wurde die Datei `/etc/pam.conf` verwendet, die aber künftig nicht mehr verwendet wird. Die Datei `pam.conf` wird nur eingelesen, wenn das Verzeichnis `/etc/pam.d/` nicht existiert.

14.2.1. PAM Servicedateien

Für Applikationen oder *Services*, welche PAM verwenden, besteht eine Datei im Verzeichnis `/etc/pam.d/`. Jede dieser Dateien ist nach dem Service benannt, für welchen diese den Zugriff kontrolliert.

Es ist dem PAM verwendenden Programm überlassen seinen Servicenamen zu bestimmen und die entsprechende PAM Konfigurationsdatei im Verzeichnis `/etc/pam.d/` abzulegen. Das `login` Program, zum Beispiel, bestimmt seinen Servicenamen als `/etc/pam.d/login`.

14.3. Format der PAM Konfigurationsdatei

Jede PAM Konfigurationsdatei enthält eine Gruppe von Anweisungen, welche wie folgt formattiert sind:

```
<module interface>  <control flag>  <module path>  <module arguments>
```

Jedes dieser Elemente ist in den folgenden Abschnitten erklärt.

14.3.1. Modul-Schnittstellen

Es gibt vier Typen von Modul-Schnittstellen, welche den unterschiedlichen Aspekten des Authentifizierungsprozesses entsprechen:

- `auth` — Diese Module werden zur Authentifizierung des Benutzers benutzt, zum Beispiel durch Erfragen und Überprüfen des Passworts und dem Einstellen von Berechtigungsmerkmalen, wie z.B. Mitgliedschaft in einer Gruppe oder Kerberos-Tickets.
- `account` — Diese Module stellen sicher, dass der Zugriff erlaubt ist. Zum Beispiel können sie prüfen, ob der Account abgelaufen ist, oder ob der Benutzer zur Anmeldung um diese Uhrzeit zugelassen ist.
- `password` — Diese Module werden zur Einstellung des Passworts verwendet.
- `session` — Diese Module werden, nachdem der Benutzer authentifiziert wurde, dazu verwendet, seine Session zu verwalten. Das Modul kann auch zusätzliche, für den Zugriff benötigte Tasks durchführen, wie beispielsweise das Mounten des Home-Verzeichnisses des Benutzers oder die Aktivierung seiner Mailbox.

Anmerkung

Ein einzelnes Modul kann jeglichen, oder alle der o.g. Modul-Schnittstellen ansprechen. Zum Beispiel `pam_unix.so` besitzt Komponenten, die alle vier Modularten ansprechen.

In einer PAM Konfigurationsdatei wird als Erstes die Modul-Schnittstelle bestimmt. Eine solche typische Zeile in einer Konfiguration könnte wie folgt aussehen:

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

Dies weist PAM an, die `auth`-Schnittstelle des `pam_unix.so` Moduls zu verwenden.

14.3.1.1. Module stapeln

Anweisungen der Modul-Schnittstellen können *gestapelt* werden, so dass mehrere Module zu einem Zweck verwendet werden können. Deshalb ist die Reihenfolge in der die Module aufgelistet werden für den Authentifikationsprozess sehr wichtig.

Das Stapeln macht es dem Administrator einfacher, zu erkennen, dass bereits einige Voraussetzungen erfüllt sind, bevor die Benutzerauthentifizierung stattgefunden hat. Zum Beispiel verwendet `rlogin` in der Regel fünf gestapelte `auth` Module, 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
```

Bevor `rlogin` ausgeführt wird, stellt PAM fest, dass die `/etc/nologin` Dateien nicht existieren, dass sie auch nicht versuchen, sich aus der Ferne über eine unverschlüsselte Netzwerkverbindung als Root anzumelden und dass alle Umgebungsvariablen geladen werden können.Wenn die `rhosts` -Authentifizierung erfolgreich, kann die Verbindung zugelassen werden. Ist die Authentifizierung nicht erfolgreich ist, wird zur Standardauthentifizierung mit Passwort übergegangen.

14.3.2. 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 einstellen, wie wichtig der Erfolg oder das Fehlschlagen des entsprechenden Moduls für die Authentifizierung des gesamten Service ist.

Es gibt vier vordefinierte Steuer-Flags:

- `required` — Solche Module müssen erfolgreich überprüft werden, bevor die Authentifizierung erfolgen kann. Wenn bei einem `required` Modul Fehler auftreten, wird der Benutzer darüber informiert, sobald auch alle anderen Module, welche die gleiche Schnittstelle referenzieren überprüft wurden.
- `requisite` — Solche Module müssen ebenfalls überprüft werden, bevor die Authentifizierung erfolgreich sein kann. Wenn bei einem `requisite` Modul Fehler auftreten, wird der Benutzer hierüber sofort informiert. Diese Mitteilung zeigt das erste fehlerhafte `required` *oder* `requisite` Modul an.
- `sufficient` — Bei solchen Modulen werden Fehler ignoriert. Wenn ein `sufficient` Modul jedoch erfolgreich überprüft wurde, und kein `required` Modul fehlschlägt, werden keine weiteren Überprüfungen dieser Modul-Schnittstelle benötigt und diese wird erfolgreich authentifiziert.
- `optional` — Solche Module sind für die erfolgreiche oder fehlgeschlagene Authentifizierung dieser Modul-Schnittstelle nicht von Bedeutung. Diese werden nur dann wichtig, wenn kein anderes Modul dieser Modul-Schnittstelle erfolgreich war oder fehlgeschlagen ist. In diesem Fall bestimmt der Erfolg oder Misserfolg eines `optional` Moduls die gesamte PAM-Authentifikation für diese Modul-Schnittstelle.


Wichtig

Die Reihenfolge in welcher `required` Module aufgerufen werden spielt keine Rolle. Bei den Steuer-Flags `sufficient` und `requisite` ist die Reihenfolge allerdings wichtig.

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 im Verzeichnis `/usr/share/doc/pam-`*`version-number`*`/` (wobei <*`version-number`*> die Versionsnummer von PAM ist).

14.3.3. PAM Modul-Pfade

Modulpfade geben PAM an, wo die "Pluggable Modules" zu finden sind, die von der ausgewählten Modul-Schnittstelle 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, wird angenommen, dass sich das angegebene Modul in `/lib/security/` , dem Default-Verzeichnis für PAM-Module, befindet.

14.3.4. Modul-Argumente

PAM verwendet Argumente, um während der Authentifizierung Informationen über eine bestimmte Modul-Schnittstelle einem "Pluggable Module" zu übermitteln.

Zum Beispiel verwendet das Modul `pam_userdb.so` versteckte Dateien aus der Berkeley DB-Datei, um den Benutzer zu authentifizieren. Berkeley DB ist eine in vielen Anwendungen eingebundenes Open-Source Datenbank-System. Das Modul verwendet ein `db` Argument, welches die von Berkeley DB für den angeforderten Service zu verwendende Datenbank angibt.

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

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

Im vorangegangenen Beispiel ersetzen Sie *<path-to-file>* mit dem vollständigen Pfad der Berkeley DB Datenbank-Datei.

Ungültige Argumente werden ignoriert und wirken sich auch nicht auf den Erfolg oder Misserfolg eines PAM-Moduls aus. Wenn ein ungültiges Argument auftaucht, erscheint jedoch normalerweise eine Fehlermeldung in `/var/log/messages`.

14.4. Beispiele für PAM-Konfigurationsdateien

Eine Konfigurationsdatei einer PAM-Anwendung sieht z.B. 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 retry=3
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
session   required  /lib/security/pam_unix.so
```

Die erste Zeile ist ein Kommentar, was durch das Hash-Zeichen (`#`) am Anfang der Zeile erkenntlich ist.

Die Zeilen zwei bis vier stellen drei Module in den Stack für die Authentifizierung bei der Anmeldung.

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

Wenn der Benutzer sich als Root anzumelden versucht, stellt dieses Modul 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
```

Dieses Modul fragt den Benutzer nach einem Passwort und überprüft dieses Passwort anhand der in `/etc/passwd` und, falls vorhanden, in `/etc/shadow` gespeicherten Informationen. Das Modul `pam_unix.so` erkennt die in `/etc/shadow` gespeicherten Shadow-Passwörter und verwendet sie zu Authentifizierung von Benutzern. Im Abschnitt 6.5 finden Sie weitere Informationen über Shadow-Passwörter.

Das Argument `nullok` weist das Modul `pam_unix.so` an, ein leeres Passwort zuzulassen.

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

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

Anmerkung

In diesem Beispiel werden alle drei `auth` Module überprüft, auch wenn schon beim ersten `auth` Modul Fehler auftreten. Der Grund dafür ist: wenn ein Benutzer weiß, weshalb seine Authentifizierung abgelehnt wurde, ist es für ihn einfacher, diese zu umgehen.

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

Dieses Modul übernimmt jegliche 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 retry=3
```

Ist ein Passwort abgelaufen, fordert die Passwort-Komponente des `pam_cracklib.so` Moduls zur Eingabe eines neuen Passworts auf. Zusätzlich wird das neue Passwort getestet, um festzustellen, ob es einfach durch ein Wörterbuch-basiertes Programm zum Erkennen von Passwörtern erkannt werden kann. Schlägt der Test einmal fehl, hat der Benutzer aufgrund des Arguments `retry=3` zwei weitere Möglichkeiten, ein besseres Passwort zu erstellen.

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

Diese Zeile legt fest, dass bei einer Änderung des Benutzer-Passworts durch das Programm die `password` Komponente des `pam_unix.so` Moduls verwendet wird. Das passiert nur, wenn der Teil `auth` des `pam_unix.so` Moduls bestimmt, dass das Passwort geändert werden muss.

Das Argument `shadow` teilt dem Modul mit, beim Updaten eines Benutzer-Passworts ein Shadow-Passwort zu erstellen.

Das Argument `nullok` weist das Modul an, dem Benutzer zu erlauben sein Passwort *von* einem leeren Passwort zu ändern. Andernfalls wird ein Null-Passwort als Account-Sperre betrachtet.

Das letzte Argument dieser Zeile ist `use_authtok` und ein gutes Beispiel für die Wichtigkeit der Reihenfolge beim Stapeln von PAM-Modulen. Dieses Argument weist das Modul an, den Benutzer nicht zur Eingabe eines neuen Passworts aufzufordern. Stattdessen wird jedes Passwort akzeptiert, das von vorherigen Passwort-Modulen verwendet wurde. Auf diese Weise müssen allen neuen Passwörter den `pam_cracklib.so` Test für sichere Passwörter durchlaufen, bevor sie akzepiert werden.

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

Die letzte Zeile gibt an, dass das Modul `pam_unix.so` für die Verwaltung der Sitzung verwendet werden soll. Dieses Modul protokolliert bei jedem Start und Ende einer Sitzung den Benutzernamen und den Service-Typ in die Datei `/var/log/messages`. Wenn Sie weitere Funktionen benötigen, kann es durch das Stapeln mit anderen Sitzungsmodulen ergänzt werden.

Die nächste Beispielkonfigurationsdatei erläutert das `auth` Modulstapeln für den `rlogin` Dienst.

```
#%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
```

Zunächst 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
```

Anschließend verhindert `pam_securetty.so`, dass Root-Anmeldungen auf unsicheren Terminals vorgenommen werden können. Damit werden praktisch alle Root-Anmeldungen über `rlogin` aus Sicherheitsgründen verhindert.

Tipp

Um sich als Root von einem Remote-Rechner aus anzumelden, benutzen Sie OpenSSH. Für mehr Informationen zum SSH Protokoll sehen Sie Kapitel 18.

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

Diese Zeile lädt das Modul `pam_env.so`, das die in `/etc/security/pam_env.conf` angegebenen Umgebungsvariablen festlegt.

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

Das `pam_rhosts_auth.so` Modul authentifiziert den Benutzer unter Verwendung von `.rhosts` im Hauptverzeichnis des Benutzers. Sollte dies erfolgreich sein, wird PAM die Authentifizierung als erfolgreich ansehen. Sollte `pam_rhosts_auth.so` fehlschlagen, wird dieser Versuch der Authentifizierung ignoriert.

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

Wenn die Authentifizierung des Benutzers durch `pam_rhosts_auth.so` gescheitert ist, führt das `pam_stack.so` Modul eine normale Passwort-Authentifizierung durch.

Das Argument `service=system-auth` bedeutet, dass der Benutzer die PAM-Konfiguration zur System- Authentifizierung in `/etc/pam.d/system-auth` durchlaufen muss.

Tipp

Wenn Sie den Prompt beim Eingeben des Passworts nicht anzeigen möchten, nachdem die `securetty` Prüfung fehlgeschlagen ist, können Sie das `pam_securetty.so` Modul von `required` in `requisite` ändern.

14.5. Module erstellen

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 neu zu kompilieren.

Dokumentationen über das Schreiben von Modulen finden Sie im Verzeichnis `/usr/share/doc/pam-<version-number>/` (wobei *<version-number>* die Versionsnummer von PAM ist).

14.6. PAM und Besitzrechte von Geräten

Red Hat Linux erlaubt es dem ersten Benutzer mithilfe des PAM-Moduls `pam_console.so` , sich in der Konsole des Computers anzumelden, das Bearbeiten von Geräten und das Ausführen von Tasks, die normalerweise für Root-Benutzer reserviert sind.

14.6.1. Besitzrechte von Geräten

Wenn sich ein Benutzer unter Red Hat Linux in einem Computer anmeldet, wird das `pam_console.so` Modul durch `login` oder die grafischen Anmeldeprogramme **gdm** und **kdm** aufgerufen. Ist dieser Benutzer der erste Benutzer, der sich in der physischen Konsole anmeldet — *Konsolen-Benutzer* genannt — bewilligt das Modul dem Benutzer das Besitzrecht einer ganzen Reihe von Geräten, die normalerweise im Besitz von Root sind. Der Konsolen-Benutzer besitzt diese Geräte solange, bis die letzte lokale Sitzung für diesen Benutzer beendet ist. Sobald sich der Benutzer abgemeldet hat, kehrt das Besitzrecht auf seinen Standardwert zurück.

Es sind alle Geräte betroffen, nicht nur Soundkarten, Disketten-Laufwerke und CD-ROM Laufwerke.

Dadurch hat der lokale Benutzer die Möglichkeit, diese Geräte zu bearbeiten, ohne als Root angemeldet zu sein, was allgemeine Tasks für den Konsolen-Benutzer vereinfacht.

Die Liste von Geräten, die von `pam_console.so` kontrolliert werden können vom Administrator in der Datei `/etc/security/console.perms` bearbeitet werden.

14.6.2. Zugriff zu Applikationen

Der Konsolen-Benutzer hat die Möglichkeit, mithilfe einer Datei, die den Befehlsnamen im Verzeichnis `/etc/security/console.apps/` enthält, zu bestimmten Programm Zugriff zu erhalten.

Eine wichtige Gruppe von Applikationen, zu denen der Konsolen-Benutzer Zugriff hat, sind folgende drei Programme zum Abschalten und Neubooten des Systems:

- `/sbin/halt`
- `/sbin/reboot`
- `/sbin/poweroff`

Da diese Programme PAM-kompatible Applikationen sind, benötigen sie das `pam_console.so` Modul.

Weitere Informationen finden Sie in den man-Seiten zu `pam_console`, `console.perms`, `console.apps` und `userhelper`.

14.7. Zusätzliche Ressourcen

Folgend finden Sie eine Aufstellung von Informationsquellen zur Verwendung und Konfiguration von PAM. Zusätzlich zu diesen Quellen sollten Sie sich mit den PAM-Konfigurationsdateien in Ihrem System vertraut machen, um deren Aufbau besser zu verstehen.

14.7.1. Installierte Dokumentationen

- `man pam` — Gute Information zur Einführung von PAM, einschließlich Aufbau und Zweck der PAM-Konfigurationsdateien.

- `/usr/share/doc/pam-<version-number>` — Enthält einen *System Administrators' Guide*, ein *Module Writers' Manual* und ein *Application Developers' Manual* sowie eine Kopie des PAM Standards, DCE-RFC 86.0.

14.7.2. Hilfreiche Websites

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

Kapitel 15.

TCP Wrappers und `xinetd`

Die Kontrolle des Zugriffs zu Netzwerk-Services ist eine der wichtigsten Sicherheitsaufgaben, denen sich der Administrator stellen muss. Glücklicherweise gibt es unter Red Hat Linux eine Reihe von Tools, welche genau dies tun. Eine `iptables`-basierte Firewall, zum Beispiel, filtert alle unerwünschten Netzwerk-Pakete im Netzwerk-Stack des Kernel heraus. Für Netzwerk-Services, welche davon Verwendung machen, fügt *TCP Wrapper* eine zusätzliche Schutzschicht hinzu, indem dieser definiert, welchen Hosts es erlaubt ist zu "*wrapped*" Netzwerk-Services zu verbinden, und welchen nicht. Einer dieser "wrapped" Netzwerk-Services ist `xinetd` *super server*. Dieser Service wird Super-Server genannt, da dieser Verbindungen zu einem Subnet von Netzwerk-Services kontrolliert und Zugriffskontrolle weiter feinabstimmt.

Abbildung 15-1 ist eine grundlegende Illustration welche zeigt, wie diese Tools zusammen arbeiten um Netzwerk-Services zu schützen.

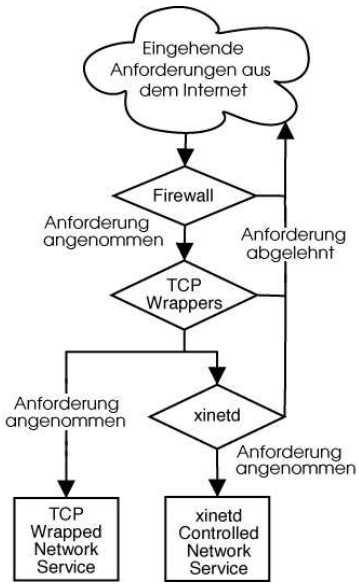

Abbildung 15-1. Zugriffskontrolle zu Netzwerk-Services

Dieses Kapitel beschäftigt sich mit der Rolle von TCP Wrapper und `xinetd` in der Zugriffskontrolle zu Netzwerk-Services und in wie diese Tools verwendet werden können um das Management von sowohl Logging, als auch Verwendbarkeit zu verbessern. Für eine Diskussion der Verbindung von Firewall und `iptables`, siehe Kapitel 16.

15.1. TCP Wrappers

Das TCP Wrappers Paket (`tcp_wrappers`) ist unter Red Hat Linux per Default installiert und stellt Host-basierte Zugriffskontrolle zu Netzwerk-Services bereit. Die wichtigste Komponente in diesem

Paket ist die /usr/lib/libwrap.a-Bibliothek. In allgemeinen Begriffen, ist ein "TCP wrapped" Service einer, der gegen die libwrap.a-Bibliothek kompiliert wurde.

Wenn ein Verbindungsversuch zu einem "TCP wrapped" Service eingeleitet wird, wird der Service zuerst die *Hosts-Zugriffs*-Dateien (/etc/hosts.allow und /etc/hosts.deny) untersuchen, um festzustellen, ob der Client-Host erlaubt ist zu verbinden. Dieser wird dann den syslog-Daemon (syslogd) verwenden, um den Namen des anfordernden Hosts und Service entweder zu /var/log/secure oder zu /var/log/messages zu schreiben.

Wenn es einem Client-Host erlaubt ist zu verbinden, gibt TCP Wrapper die Kontrolle über die Verbindung zum angeforderten Service und wird nicht mehr in die Kommunikation zwischen Client-Host und Server eingreifen.

Zusätzlich zu Zugriffskontrolle und Logging, TCP Wrapper kann Befehle aktivieren um mit dem Client zu interagieren, bevor er die Kontrolle der Verbindung zum angeforderten Netzwerk-Service übergibt oder diesen ablehnt.

Da TCP Wrapper ein wertvoller Zusatz zum Arsenal jeden Administrators Sicherheits-Tools sind, sind die meisten Netzwerk-Services unter Red Hat Linux gegen die libwrap.a gebunden. Einige dieser Anwendungen sind /usr/sbin/sshd, /usr/sbin/sendmail und /usr/sbin/xinetd.

Anmerkung

Um festzustellen, ob die Binärdatei eines Netzwerk-Service gegen libwrap.a gebunden ist, geben Sie den folgenden Befehl als root ein:

```
strings -f <binary-name> | grep hosts_access
```

Ersetzen Sie <*binary-name*> mit dem Namen der Binärdatei des Netzwerk-Service.

15.1.1. Vorteile eines TCP Wrappers

TCP Wrappers bietet zwei grundlegende Vorteile im Vergleich zu anderen Kontrollmethoden für Netzwerkdienste:

- *Der sich verbindende Client bemerkt den Einsatz von TCP Wrappers nicht* — Zugelassene Benutzer bemerken keinen Unterschied und Angreifer erhalten niemals zusätzliche Informationen über den Grund dafür, warum ihr Verbindungsversuch fehlgeschlagen ist.
- *Zentralisiertes Management von mehreren Protokollen* — TCP Wrappers arbeiten unabhängig vom Netzwerkdienst, den sie schützen. Dies erlaubt es mehreren Server-Applikationen sich eine gemeinsame Gruppe von Konfigurationsdateien zu teilen, was ein vereinfachtes Management zur Folge hat.

15.2. TCP Wrappers Konfigurationsdateien

Um zu bestimmen, ob es einer Client-Maschine erlaubt ist, zu einem gewissen Service zu verbinden, verwenden TCP Wrappers die folgenden zwei Dateien, die auch Hosts-Zugriffsdateien gennant werden:

- /etc/hosts.allow
- /etc/hosts.deny

Wenn ein Verbindungsversuch zu einem "TCP wrapped" Service eingeleitet wird, wird der Service folgende Schritte durchführen:

1. *Der Service wird zuerst `/etc/hosts.allow` untersuchen.* — Der "TCP wrapped" Service arbeitet die Datei `/etc/hosts.allow` sequentiell ab, und wendet die erste für diesen Service angegebene Regel an. Sollte dieser eine solche Regel finden, erlaubt dieser die Verbindung. Wenn nicht, wird dieser zum Schritt 2 übergehen.
2. *Der Service untersucht `/etc/hosts.deny`.* — Der "TCP wrapped" Service arbeitet die Datei `/etc/hosts.deny` sequentiell ab. Sollte es eine entsprechende Regel finden, wird die Verbindung abgelehnt. Wenn nicht, wird die Verbindung erlaubt.

Die folgenden Punkte sind wichtig, wenn TCP Wrappers verwendet werden um Netzwerk-Services zu schützen:

- Da Zugriffsregeln in `hosts.allow` zuerst angewendet werden, haben diese Vorrang vor den Regeln in `hosts.deny`. Sollte der Zugriff zu einem Service in `hosts.allow` erlaubt sein, wird jegliche Regel in `hosts.deny`, welche den Zugriff verbietet, ignoriert.
- Da alle Regeln von oben nach unten abgearbeitet werden, wird lediglich die erste Regel für einen gegebenen Service angewendet, weswegen die Reihenfolge der Regeln sehr wichtig ist.
- Sollte keine Regel für einen gegebenen Service gefunden werden, in keiner der beiden Dateien, so wird der Zugriff zu diesem Service gewährt.
- "TCP wrapped" Services speichern Regeln für die Hosts-Zugriffsdateien nicht zwischen, jegliche Änderungen zu `hosts.allow` oder `hosts.deny` treten deswegen sofort in Kraft.

15.2.1. Formatieren von Zugriffsregeln

Das Format der beiden Dateien `/etc/hosts.allow` und `/etc/hosts.deny` ist gleich. Leere Zeilen oder Zeilen, die mit dem Zeichen (`#`) beginnen, werden nicht berücksichtigt. Jede Regel muss auf einer neuen Zeile beginnen.

Jede Regel verwendet folgendes grundlegende Format, um den Zugriff zu Netzwerk-Services zu kontrollieren:

```
<daemon list>: <client list> [: <option>: <option>: ...]
```

- `<daemon list>` — Eine durch Kommas getrennte Liste von Prozessnamen (*nicht* Service-Namen) oder dem `ALLE` *Wildcard* (siehe Abschnitt 15.2.1.1). Die Daemon-Liste akzeptiert auch *Operatoren*, in Abschnitt 15.2.1.3 aufgelistet, um größere Flexibilität zu gewähren.
- `<client list>` — Eine durch Kommas getrennte Liste von Hostnamen, Host IP-Adressen, speziellen *Patterns* (siehe Abschnitt 15.2.1.2), oder speziellen Wildcards (siehe Abschnitt 15.2.1.1), welche die von dieser Regel betroffenen Hosts identifizieren. Die Client-Liste akzeptiert auch Operatoren, wie in Abschnitt 15.2.1.3 aufgelistet, um größere Flexibilität zu gewähren.
- `<option>` — Eine optionale Aktion oder durch Doppelpunkte getrennte Liste von Aktionen, welche ausgeführt werden, wenn eine Regel angewendet wird. Option-Felder unterstützen *Expansionen* (siehe Abschnitt 15.2.3.4), und können verwendet werden, um Shell-Befehle auszuführen, Zugriff zu gewähren oder abzulehnen, und die Log-Methode zu ändern (siehe Abschnitt 15.2.3).

Folgend ist eine einfaches Beispiel einer Hosts-Zugriffsregel:

```
vsftpd : .example.com
```

Diese Regel leitet TCP Wrappers dazu an, für Verbindungen zum FTP Daemon (vsftpd), von jedem Host in der example.com Domain, Ausschau zu halten. Sollte diese Regel in hosts.allow auftreten, wird die Verbindung angenommen. Sollte diese Regel in hosts.deny vorkommen, wird die Verbindung abgelehnt.

Folgendes Beispiel einer Hosts-Zugriffsregel ist komplizierter und verwendet zwei Option-Felder:

```
sshd : .example.com  \
: spawn /bin/echo `/bin/date` access denied>>/var/log/sshd.log \
: deny
```

Beachten Sie, dass in diesem Beispiel jedem der Option-Felder ein Backslash (\) voransteht. Die Verwendung eines Backslash beugt einem Ausfallen auf Grund einer zu langen Zeile vor.

Warnung

Sollte die letzte Zeile einer Hosts-Zugriffsdatei keine Leerzeile sein (eine Leerzeile enthält lediglich ein Newline-Zeichen, und wurde durch Drücken der [Enter]-Taste erzeugt), wird die letzte Regel in der Datei nicht richtig abgearbeitet, und ein Fehler wird entweder nach /var/log/messages oder /var/log/secure geschrieben. Dies ist auch der Fall für Regelzeilen, welche auf mehrere Zeilen aufgeteilt werden, ohne den Backslash zu benutzen. Das folgende Beispiel zeigt den wichtigsten Teil einer Log-Meldung für eine durch genannte Gründe fehlerhafte Regel:

```
warning: /etc/hosts.allow, line 20: missing newline or line too long
```

Diese Beispielregel sagt, dass wenn ein Verbindungsversuch zum SSH Daemon (sshd) von einem Host in der example.com Domain stattfindet, führe den Befehl echo aus (welcher den Versuch in eine spezielle Log-Datei schreibt), und lehne die Verbindung ab. Da die optionale Anweisung deny verwendet wird, wird diese Zeile den Zugriff ablehnen, auch wenn sie in der Datei hosts.allow steht. Für einen detaillierteren Überblick der Optionen, sehen Sie Abschnitt 15.2.3.

15.2.1.1. Wildcards

Wildcards erlauben TCP Wrappers eine einfachere Suche von Gruppen von Daemons oder Hosts. Diese werden am häufigsten im Client-Listen-Feld der Zugriffsregel gefunden.

Die folgenden Wildcards können verwendet werden:

- ALL — Für Alle. Kann für beide verwendet werden, die Daemon-Liste und die Client-Liste.
- LOCAL — Für jeden Host-Rechner, der keinen Punkt (.) enthält, wie localhost.
- KNOWN — Für jeden Host-Rechner, dessen Hostname und Hostadresse oder der Benutzer bekannt sind.
- UNKNOWN — Für jeden Host-Rechner, dessen Hostname und Hostadresse oder der Benutzer nicht bekannt sind.
- PARANOID — Für jeden Host-Rechner, dessen Hostname nicht mit der Hostadresse übereinstimmt.

Achtung

Die Wildcards KNOWN, UNKNOWN und PARANOID sollten sehr vorsichtig verwendet werden, da eine Unterbrechung in der Namenauflösung eine Zugriffsverweigerung auf Netzwerkdienste für berechtigte Benutzer zur Folge haben kann.

15.2.1.2. Patterns

Patterns können im Client-Listen-Feld von Zugriffsregeln benutzt werden, um Gruppen von Client-Hosts genauer anzugeben.

Folgend ist eine Liste der am häufigsten akzeptierten Patterns für einen Eintrag in der Client-Liste:

- *Ein mit einem Punkt (`.`) beginnender Hostname* — Ein Punkt am Anfang eines Hostnamens bewirkt, dass für alle Host-Rechner, die in diesem Hostnamen enden, die Regel angewandt wird. Das folgende Beispiel wird auf jeden Host in der `example.com` Domain angewendet:
  ```
  ALL : .example.com
  ```
- *Eine mit einem Punkt (`.`) endende IP-Adresse* — Ein Punkt am Ende einer IP-Adresse bewirkt, dass auf alle Hosts, deren IP-Adresse dementsprechend beginnt, die Regel angewendet wird. Das folgende Beispiel trifft auf alle Hosts im `192.168.x.x` Netzwerk zu:
  ```
  ALL : 192.168.
  ```
- *IP Adresse/Netmask Paar* — Netmask-Ausdrücke können auch als ein Pattern verwendet werden, um den Zugriff zu einer bestimmten Gruppe von IP Adressen zu regeln. Das folgende Beispiel trifft auf alle Hosts mit einer Adresse zwischen `192.168.0.0` und `192.168.1.255` zu:
  ```
  ALL : 192.168.0.0/255.255.254.0
  ```

- *Ein Stern (`*`)* — Sterne können für komplette Gruppen von Hostnamen oder IP Adressen verwendet werden, solange diese nicht in einer Client-Liste verwendet werden, welche bereits andere Patterns verwendet. Das folgende Beispiel trifft auf alle Hosts in der `example.com` Domain zu:
  ```
  ALL : *.example.com
  ```
- *Der Slash oder Schrägstrich (`/`)* — Wenn die Client-Liste mit einem Schrägstrich beginnt, wird diese als Dateiname behandelt. Dies ist nützlich wenn Regeln, welche eine große Anzahl von Hosts angeben, nötig sind. Das folgende Beispiel nimmt Bezug auf TCP Wrappers zur Datei `/etc/telnet.hosts` für alle Telnet-Verbindungen:
  ```
  in.telnetd : /etc/telnet.hosts
  ```

Andere, weniger verwendete Patterns werden auch von TCP Wrappers angenommen. Sehen Sie die man 5 Seite von `hosts_access` für mehr Information.

Warnung

Seien Sie sehr vorsichtig beim Erzeugen von Regeln, welche eine Namensauflösung erfordern, wie Host- oder Domain-Names. Ein Angreifer könnte verschiedene Tricks verwenden, um Regeln zu umgehen, die sie durch Namen spezifizieren. Außerdem, wenn Ihr System selektiven Zugriff nach Host- und Domain-Namensinformationen gewährt, könnte bei einer Unterbrechung des DNS-Dienstes auch autorisierten Benutzern der Zugriff auf Netzwerkdienste verweigert werden.

Es ist am besten, IP Adressen zu verwenden, wenn immer dies möglich ist.

15.2.1.3. Operatoren

Die Zugriffskontrollregeln kennen zur Zeit einen Operator, `EXCEPT`. Dieser kann sowohl in der Daemon- als auch in der Client-List einer Regel verwendet werden.

Der `EXCEPT` Operator erlaubt spezifische Ausnahmen in einer Regel.

Im folgenden Beispiel der Datei `hosts.allow`, ist es allen `example.com` Hosts erlaubt zu verbinden, mit der Ausnahme von `cracker.example.com`:

```
ALL: .example.com EXCEPT cracker.example.com
```

In einem anderen Beispiel der Datei hosts.allow, können Clients des 192.168.0.*x* Netzwerks alle Services benutzen, mit der Ausnahme von FTP:

```
ALL EXCEPT vsftpd: 192.168.0.
```

Anmerkung

Aus organisatorischen Gründen ist es normalerweise besser, EXCEPT-Operatoren sparsam zu verwenden, und statt dessen die Erweiterungen der Regel in die andere Zugriffskontrolldatei einzufügen. Dadurch können alle Administratoren schnell die gewünschten Dateien durchsuchen, um zu sehen, welche Host-Rechner Zugriff und welche keinen Zugriff auf bestimmte Dienste haben sollen, ohne mehrere EXCEPT-Operatoren durchsuchen zu müssen.

15.2.2. Portmap und TCP Wrappers

Verwenden Sie keine Hostnamen beim Erzeugen von Zugriffskontrollregeln für portmap, da dessen Implementation von TCP Wrappers Host Look-Ups nicht unterstützt. Aus diesem Grund, verwenden Sie ausschließlich das Schlüsselwort ALL, wenn Sie Hosts in hosts.allow oder hosts.deny angeben.

Außerdem werden Änderungen der Host-Zugriffskontrollisten, die portmap betreffen, nicht sofort wirksam sein.

Da der Betrieb von weit verbreiteten Diensten wie NIS und NFS von portmap abhängt, bedenken Sie zuerst diese Einschränkungen.

15.2.3. Option-Felder

Zusätzlich zu den grundlegenden Regeln, welche Zugriff gewähren oder ablehnen, unterstützt die Red Hat Linux Implementation von TCP Wrappers Erweiterungen zu der Zugriffskontrollsprache durch Option-Felder. Durch Verwendung der Option-Felder innerhalb einer Hosts-Zugriffsregel, können Administratoren eine Reihe von Tasks erledigen, wie dem Ändern des Log-Verhaltens, Zusammenfassen der Zugriffskontrolle und dem Ausführen von Shell-Befehlen.

15.2.3.1. Logging

Option-Felder erlauben es Administratoren die Log-Einstellungen und den Schwierigkeitsgrad für eine Regel einfach zu ändern, indem die severity-Anweisung verwendet wird.

Im folgenden Beispiel, werden Verbindungen zum SSH Daemon von jedem Host in der example.com-Domain zu der Default Log authpriv geschrieben (da kein Wert angegeben ist), und dies mit einer Priorität von emerg:

```
sshd : .example.com : severity emerg
```

Es ist auch möglich, eine Log mit der severity-Option anzugeben. Das folgende Beispiel loggt alle Hosts aus der example.com Domain, welche versuchen zu einem SSH service zu verbinden, zu der local0 Log, mit einer Priorität von alert:

```
sshd : .example.com : severity local0.alert
```

Anmerkung

In der Praxis, wird dieses Beispiel nicht arbeiten, solange der Syslog-Daemon (`syslogd`) nicht dazu konfiguriert ist, Log-Meldungen zu `local0` zu schreiben. Sehen Sie die `syslog.conf` man-Seite für Informationen zum Konfigurieren von benutzerdefinierten Logs.

15.2.3.2. Zugriffskontrolle

Option-Felder erlauben es dem Administratoren, Hosts explizit anzunehmen oder abzulehnen, indem sie die `allow`- oder `deny`-Anweisung als letzte Option hinzufügen.

Die folgenden Regeln, zum Beispiel, erlauben SSH-Verbindungen von `client-1.example.com`, lehnen aber Verbindungsversuche von `client-2.example.com` ab:

```
sshd : client-1.example.com : allow
sshd : client-2.example.com : deny
```

Durch erlauben der Zugriffskontrolle auf einer pro-Regel Basis, erlaubt das Option-Feld Administratoren alle Zugriffsregeln in entweder `hosts.allow` oder `hosts.deny` zusammenzufassen. Einige halten dies für einen einfacheren Weg die Zugriffsregeln zu organisieren.

15.2.3.3. Shell-Befehle

Option-Felder erlauben Zugriffsregeln Shell-Befehle auszuführen, durch die zwei folgenden Anweisungen:

- `spawn` — Startet einen Shell-Befehl als Kind-Prozess. Diese Option-Anweisung kann Aufgaben wie die Verwendung von `/usr/sbin/safe_finger` durchführen, um weitere Informationen über den anfragenden Client zu erhalten, oder spezielle Log-Dateien mit dem `echo` Befehl erzeugen.

  Im folgenden Beispiel, versuchen Clients auf einen Telnet Service von der `example.com` Domain aus zuzugreifen, was in eine spezielle Log-Datei geschrieben wird:

  ```
  in.telnetd : .example.com \
    : spawn /bin/echo `/bin/date` from %h>>/var/log/telnet.log \
    : allow
  ```

- `twist` — Ersetzt den angeforderten Service mit dem angegebenen Befehl. Diese Anweisung wird oft verwendet, um Fallen für etwaige Angreifer (im Englischen auch "honey pots", Deutsch Honigtöpfe genannt) zu stellen. Diese kann auch verwendet werden um Nachrichten zu verbindenden Clients zu senden. Der twist-Befehl muss am Ende der Regelzeile stehen.

  Im folgenden Beispiel, wird Clients, welche versuchen auf FTP Services von der `example.com` Domain aus zuzugreifen, eine Nachricht mit Hilfe des `echo` Befehls gesendet:

  ```
  vsftpd : .example.com \
  : twist /bin/echo "421 Bad hacker, go away!"
  ```

Für mehr Informationen zur Verwendung von Shell-Befehl Optionen, sehen Sie die `hosts_options` man-Seite.

15.2.3.4. Expansionen

Expansionen, welche im Zusammenhang mit `spawn` und `twist`-Anweisungen verwendet werden, liefern Informationen über den Client, Server und die betreffenden Prozesse.

Folgend ist eine Liste der verfügbaren Expansionen:

- %a — Die IP-Adresse des Clients.
- %A — Die IP-Adresse des Servers.
- %c — Verschiedene Client-Informationen, wie zum Beispiel der Benutzer- und Hostname oder der Benutzername und die IP-Adresse.
- %d — Der Name des Daemon-Prozesses.
- %h — Der Hostname des Clients (oder IP-Adresse, wenn der Hostname nicht verfügbar ist).
- %H — Der Hostname des Servers (oder IP-Adresse, wenn der Hostname nicht verfügbar ist).
- %n — Der Hostname des Clients. Wenn dieser nicht verfügbar ist, wird unknown ausgegeben. Wenn der Hostname und die Hostadresse des Clients nicht übereinstimmen, paranoid ausgegeben.
- %N — Der Hostname des Servers. Wenn dieser nicht verfügbar ist, wird unknown ausgegeben. Wenn der Hostname und die Hostadresse des Servers nicht übereinstimmen, paranoid ausgegeben.
- %p — Die ID des Daemonprozesses.
- %s — Verschiedene Serverinformationen, wie zum Beispiel der Daemonprozess und die Host- oder IP-Adresse des Servers.
- %u — Der Benutzername des Clients. Wenn dieser nicht verfügbar ist, wird unknown ausgegeben.

Die folgende Beispielregel verwendet eine Expansion in Verbindung mit dem spawn Befehl, um den Host des Clients in einer benutzerdefinierten Log-Datei zu identifizieren.

Sie leitet TCP Wrappers an, sollte ein Verbindungsversuch zum SSH Daemon (sshd) von einem Host in der example.com Domain unternommen werden, mit dem Befehl echo den Versuch in eine spezielle Log-Datei zu schreiben, einschließlich Hostname des Client (unter Verwendung von %h):

```
sshd : .example.com  \
: spawn /bin/echo `/bin/date` access denied to %h>>/var/log/sshd.log \
: deny
```

Ähnlich, können Expansionen dazu verwendet werden, um Nachrichten auf bestimmte Clients abzustimmen. Im folgenden Beispiel, wird Clients, welche versuchen auf FTP Services von der example.com Domain aus zuzugreifen, mitgeteilt, dass diese vom Server ausgeschlossen wurden:

```
vsftpd : .example.com \
: twist /bin/echo "421 %h has been banned from this server!"
```

Für eine vollständige Erklärung der verfügbaren Expansionen, wie zusätzlichen Zugriffskontroll-Optionen, sehen Sie Abschnitt 5 der man-Seiten von hosts_access (man 5 hosts_access) und die man-Seite für hosts_options.

Für zusätzliche Ressourcen im Bezug zu TCP Wrappers, sehen Sie Abschnitt 15.5.

15.3. xinetd

Der xinetd-Daemon ist ein TCP-wrapped *Super Service*, der den Zugriff auf eine Anzahl beliebter Netzwerkservices wie FTP, IMAP und Telnet bereitstellt. Er bietet außerdem servicespezifische Konfigurationsoptionen zur Zugriffskontrolle, erweitertes Logging, Umleitungen und Ressourcen-Einsatzkontrolle.

Wenn sich ein Client Host mit einem von xinetd überwachten Netzwerkservice zu verbinden versucht, erhält der Super Service die Anfrage und prüft die TCP-Wrapper Zugriffsrechte. Wird der

Zugang gewährt, überprüft xinetd, dass die Verbindung auch entsprechend seinen Regeln für diesen Service erlaubt ist, und dass der Service nicht mehr als die zugewiesenen Ressourcen verbraucht bzw. jegliche Regeln einhält. Daraufhin wird eine Instanz des angeforderten Services geöffnet und die Überwachung der Verbindung übergeben. Sobald die Verbindung besteht, hält sich xinetd aus der Kommunikation zwischen Client Host und Server raus.

15.4. xinetd-Konfigurationsdateien

Die Konfigurationsdateien für xinetd sind folgende:

- /etc/xinetd.conf — Die globale xinetd Konfigurationsdatei.
- /etc/xinetd.d/ Verzeichnis — Das Verzeichnis, das alle servicespezifischen Dateien enthält.

15.4.1. Die /etc/xinetd.conf Datei

Die Datei /etc/xinetd.conf enthält allgemeine Konfigurationseinstellungen, die jeden Service unter Kontrolle von xinetd betreffen. Bei jedem Start des xinetd Service wird diese Datei gelesen, um also Konfigurationsänderungen wirksam werden zu lassen, muss der Administrator den xinetd Service neu starten. Unten ein Beispiel einer /etc/xinetd.conf Datei:

```
defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}
includedir /etc/xinetd.d
```

Diese Zeilen kontrollieren verschiedene Aspekte von xinetd:

- instances — Bestimmt die Höchstzahl der Anfragen, die xinetd gleichzeitig bearbeiten kann.
- log_type — Weist xinetd an, die Protokolldatei authpriv, die Log-Einträge in die Datei /var/log/secure zu verwenden. Das Hinzufügen einer Direktive wie FILE /var/log/xinetdlog würde eine benutzerdefinierte Log-Datei mit dem Namen xinetdlog im Verzeichnis /var/log/ erstellen.
- log_on_success — Konfiguriert xinetd zum Protokollieren, wenn die Verbindung erfolgreich ist. Standardmäßig werden die Remote-Host-IP-Adresse und die ID des Servers, der die Anfrage verarbeitet, aufgezeichnet.
- log_on_failure — Konfiguriert xinetd zum Protokollieren wenn die Verbindung fehlschlägt oder nicht zugelassen ist.
- cps — Konfiguriert xinetd, für einen bestimmten Dienst nicht mehr als 25 Verbindungen pro Sekunde zuzulassen. Wenn diese Grenze erreicht wird, wird der Dienst für 30 Sekunden zurückgezogen.
- includedir /etc/xinetd.d/ — Enthält Optionen der servicespezifischen Konfigurationsdateien im Verzeichnis /etc/xinetd.d/. Weitere Informationen zu diesem Verzeichnis finden Sie unter Abschnitt 15.4.2.

Anmerkung

Die Einstellungen `log_on_success` und `log_on_failure` in `/etc/xinetd.conf` werden oftmals von den servicespezifischen Logdateien geändert. Aus diesem Grund können mehr Informationen als von der Datei angezeigt im Servicelog enthalten sein. Weitere Informationen zu Protokoll-Optionen finden Sie unter Abschnitt 15.4.3.1.

15.4.2. Das `/etc/xinetd.d/` Verzeichnis

Die Dateien im Verzeichnis`/etc/xinetd.d/` enthalten die Konfigurationsdateien für jeden Service, der von `xinetd` verwaltet wird, sowie die Dateinamen, die zu dem Service gehören. Wie `xinetd.conf` wird diese Datei nur gelesen, wenn der `xinetd` Service gestartet wird. Um Änderungen wirksam werden zu lassen, muss der Administrator den `xinetd` Service neu starten.

Die Dateien in `/etc/xinetd.d/` verwenden dieselben Konventionen und Optionen wie `/etc/xinetd.conf`. Der Hauptgrund dafür, dass sich diese in eigenen Konfigurationsdateien befinden, ist, die Anpassung zu vereinfachen und andere Services damit weniger zu beeinflussen.

Um einen Überblick über die Struktur dieser Dateien zu erhalten, betrachten Sie die Datei `vsftpd`:

```
service ftp
{
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/vsftpd
        log_on_success          += DURATION USERID
        log_on_failure          += USERID
        nice                    = 10
        disable                 = no
}
```

Diese Zeilen kontrollieren verschiedene Aspekte des `vsftpd` Service:

- `service` — Definiert den Servicenamen, meistens entsprechend eines Services in der Datei `/etc/services` file.
- `socket_type` — Setzt den Netzwerk-Sockettyp auf `stream`.
- `wait` — Bestimmt, ob ein Service Single-Threaded (`yes`) oder Multi-Threaded (`no`) ist.
- `user` — Bestimmt die User ID, unter der der Prozess abläuft.
- `server` — Bestimmt die auszuführende Binärdatei.
- `log_on_success` — Bestimmt die Protokoll-Parameter für `log_on_success` zusätzlich zu den in `xinetd.conf` eingestellten.
- `log_on_failure` — Bestimmt die Protokoll-Parameter für `log_on_failure` zusätzlich zu den in `xinetd.conf` eingestellten.
- `nice` — Bestimmt den Server-Priority-Level.
- `disable` — Bestimmt, ob der Service aktiv oder inaktiv ist.

15.4.3. Ändern von xinetd Konfigurationsdateien

Es gibt eine große Anzahl an Direktiven für xinetd geschützte Dienste. Dieser Abschnitt beschreibt einige der häufig verwendeten Optionen.

15.4.3.1. Protokoll-Optionen

Die folgenden Protokoll-Optionen stehen für /etc/xinetd.conf und die servicespezifischen Konfigurationsdateien im Verzeichnis /etc/xinetd.d/ zur Verfügung.

Hier eine Liste der häufig verwendeten Protokoll-Optionen:

- ATTEMPT — Protokolliert einen fehlgeschlagenen Versuch (log_on_failure).
- DURATION — Protokolliert die Zeitdauer der Dienstnutzung seitens eines Remote-Systems (log_on_success).
- EXIT — protokolliert das Beenden oder das Endsignal des Dienstes (log_on_success).
- HOST — Protokolliert die IP-Adresse des Remote-Host-Rechners (log_on_failure und log_on_success).
- PID — Protokolliert die Prozess-ID des Servers, an den die Anfrage gesendet wird (log_on_success).
- RECORD — Zeichnet die Informationen über das Remote-System auf, wenn der Dienst nicht gestartet werden kann. Nur besondere Dienste, wie zum Beispiel login and finger, können diese Option verwenden (log_on_failure).
- USERID — Protokolliert den Remote- Benutzer mithilfe der in RFC 1413 definierten Methode für alle Multithreaded-Stream-Dienste (log_on_failure und log_on_success).

Eine vollständige Liste der Protokoll-Optionen finden Sie auf der man-Seite zu xinetd.conf.

15.4.3.2. Zugriffskontroll-Optionen

Benutzer von xinetd-Diensten können wählen, ob sie die TCP-Wrapper Host-Zugriffskontrolldateien, Zugriffskontrolle mittels xinetd -Konfigurationsdateien oder eine Mischung von beidem verwenden wollen. Informationen über den Gebrauch von TCP-Wrapper Host-Zugriffskontrolldateien finden Sie in Abschnitt 15.2. In diesem Teil wird der Einsatz von xinetd für die Kontrolle von Zugriffen auf bestimmte Dienste besprochen.

Anmerkung

Im Gegensatz zu TCP-Wrapper, muss der xinetd-Administrator nach jeder Änderung den xinetdService neu starten, damit diese wirksam werden.

Die xinetd-Host-Zugriffskontrolle unterscheidet sich von der von TCP-Wrapper verwendeten Methode. Während TCP-Wrapper die gesamte Zugriffskonfiguration in zwei Dateien ablegt, /etc/hosts.allow und /etc/hosts.deny, kann jede Dienstdatei in /etc/xinetd.d ihre eigenen Zugriffskontrollregeln enthalten.

Die folgenden Optionen werden in den xinetd-Dateien für die Host-Zugriffskontrolle unterstützt:

- only_from — Erlaubt nur den angegebenen Host-Rechnern die Nutzung des Dienstes.
- no_access — Sperrt aufgeführten Host-Rechnern den Zugriff auf den Dienst.

- access_times — Den Zeitraum, in dem ein bestimmter Dienst verwendet werden kann. Der Zeitraum muss im 24-Stunden Format (HH:MM-HH:MM) angegeben werden.

Die Optionen only_from und no_access können eine Liste von IP-Adressen oder Hostnamen verwenden, oder ein gesamtes Netzwerk spezifizieren. Wie TCP-Wrapper kann durch die Kombination der xinetd-Zugriffskontrolle und der entsprechenden Protokollierkonfiguration die Sicherheit durch das Sperren von Anfragen von gesperrten Hosts und das Protokollieren aller Verbindungsversuche erhöht werden.

Zum Beispiel kann die folgende /etc/xinetd.d/telnet-Datei verwendet werden, um den Telnet-Zugriff einer bestimmten Netzwerkgruppe auf ein System zu verweigern und den gesamten Zeitraum für die Anmeldung von zugelassenen Benutzern einzuschränken:

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        no_access       = 10.0.1.0/24
        log_on_success  += PID HOST EXIT
        access_times    = 09:45-16:15
}
```

In diesem Beispiel erhält jedes System des Unternetzes 10.0.1.0/24, wie zum Beispiel 10.0.1.2, beim Versuch, auf Telnet zuzugreifen, die folgende Meldung:

```
Connection closed by foreign host.
```

Außerdem werden diese Anmeldeversuche in /var/log/secure protokolliert:

```
May 15 17:38:49 boo xinetd[16252]: START: telnet pid=16256 from=10.0.1.2
May 15 17:38:49 boo xinetd[16256]: FAIL: telnet address from=10.0.1.2
May 15 17:38:49 boo xinetd[16252]: EXIT: telnet status=0 pid=16256
```

Wenn Sie TCP-Wrapper zusammen mit der Zugriffskontrolle von xinetd verwenden, müssen Sie die Beziehung dieser beiden Zugriffskontroll-Mechanismen verstehen.

Im folgenden wird die Abfolge der Vorgänge in xinetd beschrieben, wenn ein Client eine Verbindung anfordert:

1. Der xinetd-Daemon greift auf die Host-Zugriffsregeln der TCP-Wrapper durch einen libwrap.a Library-Aufruf zu. Besteht eine Dienstverweigerungs-Regel für den Client Host, wird die Verbindung nicht aufgebaut. Besteht eine Zugrifferlaubnis, wird die Verbindung an xinetd weitergegeben.
2. Der xinetd-Daemon überprüft seine eigenen Zugriffskontroll-Regeln für den xinetd-Service und den angeforderten Service. Besteht eine Dienstverweigerungs-Regel für den Client Host, wird die Verbindung nicht aufgebaut. Ansonsten startet xinetd eine Instanz des angeforderten Services und gibt die Kontrolle an diesen weiter.

Wichtig

Seien Sie vorsichtig beim Verwenden von TCP-Wrapper Zugriffskontrollen zusammen mit `xinetd` Zugriffskontrollen. Eine Fehlkonfiguration kann höchst unerwünschte Folgen nach sich ziehen.

15.4.3.3. Bindungs- und Umleitungs-Optionen

Die Dienstkonfigurationsdateien für `xinetd` unterstützen auch die Bindung des Dienstes an eine besondere IP-Adresse und Umleitung der eingehenden Anfragen für diesen Dienst an andere IP-Adressen, Hostnamen oder Ports.

Die Bindung wird von der `bind` -Option in den Dienstkonfigurationsdateien kontrolliert und verknüpft den Dienst mit einer IP-Adresse auf dem System. Nach der Konfiguration lässt die `bind` Option nur Anfragen für die richtige IP-Adresse zum Zugriff auf den Dienst zu. So kann jeder Dienst je nach Bedarf mit verschiedenen Netzwerkschnittstellen gebunden werden.

Dies ist besonders nützlich bei Systemen mit mehreren Netzwerkadaptern oder mehreren IP-Adressen. Sie können beispielsweise Telnet zum Abhören von Schnittstellen konfigurieren, die mit einem privaten Netzwerk und nicht mit dem Internet verbunden sind.

Die Option `redirect` akzeptiert eine IP-Adresse oder einen Hostnamen gefolgt von einer Port-Nummer. Sie konfiguriert den Service, alle alle Anfragen für diesen Dienst an eine bestimmte Adresse und Portnummer weiterzuleiten. Diese Eigenschaft kann verwendet werden, um auf eine andere Port-Nummer auf demselben System zu verweisen, die Anfrage an eine andere IP-Adresse auf demselben Rechner weiterzuleiten, die Anfrage an ein anderes System oder eine andere Port-Nummer zu verschieben. Die Eigenschaft kann auch für eine Kombination dieser Optionen verwendet werden. Auf diese Weise kann ein Benutzer, der sich für einen bestimmten Dienst an einem System anmeldet, ohne Unterbrechung umgeleitet werden.

Der `xinetd`-Daemon kann diese Umleitung durch Erzeugen eines Prozesses ausführen, der während der Verbindung des anfragenden Client-Rechners mit dem Host-Rechner, der den eigentlichen Dienst liefert, im Stay-Alive-Modus läuft, und Daten zwischen den zwei Systemen austauscht.

Der eigentliche Stärke der `bind` und `redirect` -Optionen liegt in deren kombinierten Verwendung. Durch Bindung eines Dienstes an eine bestimmte IP-Adresse auf einem System und dem darauffolgenden Umleiten der Anfragen für denselben Dienst an einen zweiten Rechner, der nur für den ersten Rechner sichtbar ist, können Sie ein internes System verwenden, um Dienste für vollkommen unterschiedliche Netzwerke zur Verfügung zu stellen. Ansonsten können diese Optionen verwendet werden, um die Zeit zu begrenzen, während derer ein Dienst auf einem Multihomed-Rechner einer bekannten IP-Adresse ausgesetzt ist, sowie jegliche Anfragen für diesen Dienst an einen anderen Rechner weiterzuleiten, der eigens für diesen Zweck konfiguriert ist.

Nehmen wir zum Beispiel ein System, das als Firewall mit diesen Einstellungen für seine Telnet-Dienste verwendet wird:

```
service telnet
{
        socket_type  = stream
        wait   = no
        server   = /usr/sbin/in.telnetd
        log_on_success  += DURATION USERID
        log_on_failure  += USERID
        bind                    = 123.123.123.123
        redirect                = 10.0.1.13 21 23
}
```

Die Optionen `bind` und `redirect` in dieser Datei stellen sicher, dass der telnet-Dienst auf dem Rechner für eine externe IP-Adresse (123.123.123.123) bestimmt ist, und zwar die Internet-seitige. Außer-

dem werden alle an 123.123.123.123 gesendete Telnet-Anfragen über einen zweiten Netzwerkadapter an eine interne IP-Adresse (10.0.1.13) weitergeleitet, auf die nur die Firewall und interne Systeme Zugriff haben. Die Firewall sendet dann die Kommunikation von einem System an das andere, und für das sich verbindende System sieht es so aus, als ob es mit 123.123.123.123 verbunden sei, während es in Wirklichkeit mit einem anderen Rechner verbunden ist.

Diese Eigenschaft ist besonders nützlich für Benutzer mit Breitbandverbindungen und nur für feste IP-Adressen. Wird Network Address Translation (NAT) verwendet, sind die Systems hinter dem Gateway-Rechner, die nur interne IP-Adressen verwenden, außerhalb des Gateway-Systems nicht zugängig. Wenn jedoch bestimmte Dienste, die mit `xinetd` kontrolliert werden, mit den Optionen `bind` und `redirect` konfiguriert sind, kann der Gateway-Rechner als eine Art Proxy zwischen externen Systemen und einem bestimmten internen Rechner fungieren, der konfiguriert ist, um den Dienst zur Verfügung zu stellen. Außerdem sind die verschiedenen `xinetd`-Zugriffskontroll- und Protokolloptionen auch für zusätzlichen Schutz, wie zum Beispiel Begrenzung der Anzahl von gleichzeitigen Verbindungen für den weitergeleiteten Dienst, verfügbar.

15.4.3.4. Ressourcen-Management-Optionen

Der `xinetd`-Daemon kann einen einfachen Grad an Schutz vor Denial of Service (DoS) Angriffen (Dienstverweigerungs-Angriffe) liefern. Untenstehend finden Sie eine Liste an Direktiven, die Ihnen beim Einschränken der Auswirkung dieser Angriffe helfen:

- `per_source` — Definiert die Höchstanzahl von Verbindungen von einer bestimmen IP-Adresse mit einem bestimmen Dienst. Es werden nur ganze Zahlen als Argument akzeptiert und er kann in `xinetd.conf` und in den servicespezifischen Konfigurationsdateien im Verzeichnis `xinetd.d/` verwendet werden.
- `cps` — Definiert die Höchstzahl der Verbindungen pro Sekunde. Diese Option akzeptiert zwei ganzzahlige Argumente getrennt durch eine Leerstelle. Die erste Zahl ist die Höchstzahl von Verbindungen zum Service pro Sekunde. Die zweite Zahl ist die Anzahl der Sekunden, die `xinetd` warten muss, bis der Service wieder aktiviert wird. Es werden nur ganze Zahlen akzeptiert, und die Option kann in `xinetd.conf` und in den servicespezifischen Konfigurationsdateien im Verzeichnis `xinetd.d/` verwendet werden.
- `max_load` — Definiert den Schwellenwert für die CPU-Nutzung eines Dienstes. Es werden Kommazahlen-Argumente.

Es gibt noch weitere Ressource-Management-Optionen für `xinetd`. Im Kapitel *Server Security* im *Red Hat Linux Security Guide* und auf der `xinetd.conf` man-Seite finden Sie weitere Informationen.

15.5. Zusätzliche Ressourcen

Weitere Informationen über TCP-Wrapper und `xinetd` finden Sie in der Systemdokumentation und im Internet.

15.5.1. Installierte Dokumentation

Die im Paket enthaltene Dokumentation auf Ihrem System ist ein guter Ausgangspunkt, wenn Sie weitere Informationen über TCP-Wrapper, `xinetd` und Zugriffskontroll-Konfigurationsoptionen suchen.

- /usr/share/doc/tcp_wrappers-<*version*>/ — Enthält eine README-Datei, in der die Funktionsweise von TCP-Wrapper und die verschiedenen Hostnamen- und Hostadressen-Spoofing-Risiken beschrieben werden.
- /usr/share/doc/xinetd-<*version*>/ — Enthält eine README-Datei, in der Aspekte der Zugriffskontrolle beschrieben sind und eine sample.conf-Datei mit Ideen zum Bearbeiten der Konfigurationsdateien im /etc/xinetd.d/ Verzeichnis.
- man 5 hosts_access — Die man-Seite für die TCP-Wrapper-Hostzugriffskontroll-Dateien.
- man hosts_options — Die man-Seite für die TCP-Wrapper Optionsfelder.
- man xinetd.conf — Die man-Seite mit einer Liste der xinetd Konfigurationsoptionen.
- man xinetd — Die man-Seite für den xinetd Super Service Daemon.

15.5.2. Hilfreiche Websites

- http://www.xinetd.org — Die Homepage von xinetd enthält Beispielkonfigurationsdateien, eine vollständige Liste von Eigenschaften und eine FAQ-Liste.
- http://www.macsecurity.org/resources/xinetd/tutorial.shtml — Eine ausführliche Anleitung mit Beispielen, in der viele Möglichkeiten beschrieben werden, standardmäßige xinetd-Konfigurationsdateien für bestimmte Sicherheitszwecke anzupassen.

15.5.3. Bücher zum Thema

- *Red Hat Linux Security Guide* ; Red Hat, Inc. — Bietet einen Überblick über Workstation-, Server- und Netzwerksicherheit mit speziellen Vorschlägen zu TCP-Wrapper und xinetd.
- *Hacking Linux Exposed* von Brian Hatch, James Lee und George Kurtz; Osbourne/McGraw-Hill — Eine exzellente Ressource für Sicherheit und Informationen TCP-Wrapper und xinetd.

Kapitel 16.

iptables

Red Hat Linux wird mit erweiterten Tools für die *Paket-Filterung* geliefert — den Prozess zur Kontrolle von Netzwerkpaketen, mit Zugang zu, durch und aus dem Netzwerkstack des Kernels. Die Kernelversionen vor 2.4 konnten Pakete mit `ipchains` manipulieren und verwendeten Regellisten für jedes Paket in jeder Phase des Filterungsprozesses. Die Einführung des 2.4-Kernels hat `iptables` mit sich gebracht (auch *netfilter* genannt), die den `ipchains` ähnlich sind, deren Wirkungsbereich und Kontrollmöglichkeiten bei der Filterung aber erweitern.

In diesem Kapitel werden die Grundlagen der Paketfilterung beschrieben, wobei die Unterschiede zwischen `ipchains` und `iptables` definiert und die verschiedenen, mit den `iptables`-Befehlen zur Verfügung stehenden Optionen erklärt werden. Es wird außerdem gezeigt, wie Filterungsregeln zwischen den Bootvorgängen des Systems erhalten bleiben.

Wenn Sie Anweisungen für das Erstellen von `iptables`-Regeln oder das Einrichten einer Firewall auf der Grundlage dieser Regeln benötigen, finden Sie weitere Informationen unter Abschnitt 16.5.

Warnung

Der standardmäßige Firewall-Mechanismus im 2.4-Kernel ist zwar `iptables`, `iptables` kann aber nicht benutzt werden, wenn die `ipchains` schon laufen. Wenn also beim Booten `ipchains` vorhanden sind, gibt der Kernel eine Fehlermeldung und kann `iptables` nicht starten.

Diese Bootfehler-Meldungen haben keinerlei Auswirkung auf das Funktionieren der `ipchains`.

16.1. Paket-Filterung

Die Daten werden über ein Netzwerk als *Pakete* übertragen. Ein Netzwerkpaket ist eine Sammlung von Daten einer bestimmten Größe und Format. Der sendende Computer teilt eine Datei in Pakete auf, die unter Verwendung bestimmter Netzwerkprotokolle über das Netzwerk gesendet werden. Jedes Paket enthält einen kleinen Teil der Dateidaten. Der andere Computer empfängt die Pakete und fügt sie wieder zu einer Datei zusammen.

Jedes Paket enthält Informationen, mit deren Hilfe es sich durch das Netzwerk zu seinem Bestimmungsort bewegt. Das Paket kann den Computern, die es passiert, als auch dem Computer, der sein Ziel ist, unter anderem mitteilen, woher es kam und wohin es geht und welche Paketart es ist. Die meisten Pakete sind dazu bestimmt, Daten zu transportieren, eine Protokolle verwenden Pakete jedoch auf ganz besondere Weise. Das *Transmission Control Protocol (TCP)* verwendet z.B. ein SYN-Paket, das keine Daten enthält, um eine Kommunikation zwischen zwei Systemen zu starten.

Der Linux-Kernel enthält die integrierte Fähigkeit, Pakete zu filtern und ermöglicht einigen von ihnen den Zugang zum System, während anderen dieser verwehrt wird. Der Netzfilter des 2.4-Kernels enthält integrierte *Tabellen* oder *Regellisten*. Dabei handelt es sich um folgende:

- `filter` — Die Standardtabelle zum Verwalten von Netzwerkpaketen.
- `nat` — Mithilfe dieser Tabelle werden Pakete geändert, die eine neue Verbindung herstellen.
- `mangle` — Diese Tabelle wird für spezielle Arten der Paketänderung verwendet.

Alle diese Tabellen verfügen über eine Gruppe integrierter *Chains* (Ketten), die den Aktionen entsprechen, die vom Netzfilter für das Paket durchgeführt werden.

Die für die `filter`-Tabelle integrierten Chains sind folgende:

- *INPUT* — Gilt für über eine Netzwerkschnittstelle empfangene Pakete.
- *OUTPUT* — Gilt für Pakete, die über dieselbe Netzwerkschnittstelle versendet werden, die die Pakete empfing.
- *FORWARD* — Gilt für Pakete, die auf einer Netzwerkschnittstelle empfangen, aber über eine andere versendet werden.

Die für die `nat`-Tabelle integrierten Chains sind folgende:

- *PREROUTING* — Ändert über eine Netzwerkschnittstelle empfangene Pakete beim Empfang.
- *OUTPUT* — Ändert lokal generierte Pakete, ehe sie über eine Netzwerkschnittstelle geleitet werden.
- *POSTROUTING* — Ändert Pakete vor dem Senden über eine Netzwerkschnittstelle.

Die für die `mangle`-Tabelle integrierten Chains sind folgende:

- *PREROUTING* — Ändert über eine Netzwerkschnittstelle empfangene Pakete vor dem Routen.
- *OUTPUT* — Ändert lokal generierte Pakete, ehe sie über eine Netzwerkschnittstelle geleitet werden.

Jedes von einem Linux-System empfangene oder gesendete Paket gehört zu mindestens einer Tabelle.

Ein Paket kann in allen Tabellen auf mehrere Regeln hin überprüft werden, bevor es am Ende der Chain austritt. Struktur und Zweck dieser Regeln können unterschiedlich sein, sie versuchen jedoch normalerweise ein Paket, das von einer oder an eine IP-Adresse bzw. mehrere IP-Adressen gesendet wurde, zu identifizieren, wenn dieses ein bestimmtes Protokoll und einen bestimmten Netzwerkdienst benutzt.

Unabhängig von ihrem Ziel sind Pakete, sobald sie einer bestimmten Regel einer Tabelle entsprechen, für ein bestimmtes *Ziel* bzw. für eine auf sie anzuwendende Aktion bestimmt. Wenn in der Regel für das Ziel eines entsprechenden Pakets ein `ACCEPT` (AKZEPTIEREN) angegeben ist, überspringt das Paket die restlichen Regelkontrollen und darf somit seinen Weg in Zielrichtung fortsetzen. Wenn aber in einer Regel für das Ziel `DROP` (AUSLASSEN) angegeben ist, wird das Paket "ausgelassen", d.h. das Paket erhält keinen Zugriff auf das System, und es wird nichts an den Host-Rechner zurückgesendet, von dem das Paket stammt. Wenn eine Regel `QUEUE` (WARTESCHLANGE) als Ziel angibt, wird das Paket zum Benutzerplatz geleitet. Wenn in einer Regel für das Ziel `REJECT` (ABLEHNEN) angegeben ist, wird das Paket ausgelassen und als Fehlerpaket wieder zu seinem Ursprungsort zurückgeschickt.

Jede Chain hat eine Default-Policy zu `ACCEPT`, `DROP`, `REJECT`, oder `QUEUE`. Wenn das Paket keiner der Regeln in der Chain entspricht, wird auf dieses Paket die standardmäßige Policy angewandt.

Der Befehl `iptables` ermöglicht Ihnen diese Tabellen zu konfigurieren, und, falls nötig, neue Tabellen zu erzeugen.

16.2. Unterschiede zwischen `iptables` und `ipchains`

Auf den ersten Blick scheinen sich `ipchains` und `iptables` sehr zu ähneln. Beide Methoden verwenden Regel-Chains für die Filterung von Paketen und arbeiten im Linux-Kernel, nicht nur um zu entscheiden, welche Pakete hinein-oder hinausgelassen werden sollen, sondern auch, wie mit diesen Paketen, die bestimmten Regeln entsprechen, verfahren werden soll. `iptables` stellt Ihnen jedoch eine deutlich erweiterbarere Paketfilterung zur Verfügung, da sie dem Administrator mehr Kontrolle gibt, ohne dass das gesamte System hierdurch zu kompliziert wird.

Insbesondere sollten Benutzer, die sich mit `ipchains` gut auskennen, auf folgende wichtige Unterschiede zwischen `ipchains` und `iptables` achten, bevor sie versuchen, `iptables` zu benutzen:

- *Mit iptables wird jedes gefilterte Paket nur durch Anwendung der Regeln einer einzigen Chain und nicht mit denen mehrerer Chains verarbeitet.* Beispiel: Ein FORWARD-Paket, das ein System betritt, würde mit ipchains den INPUT-, FORWARD-, und OUTPUT-Chains unterliegen, um sein Ziel zu erreichen. iptables hingegen sendet Pakete nur zur INPUT-Chain, wenn diese für das lokale System bestimmt sind, während Pakete nur an die OUTPUT-Chain gesendet werden, wenn das lokale System die Pakete erzeugt hat. Aus diesem Grund müssen Sie sicherstellen, dass sich die Regel für das Abfangen eines bestimmten Pakets in der richtigen Chain befindet, die das Paket auch wirklich sieht.
- *Das DENY-Ziel wurde auf DROP geändert.* Mit ipchains können Pakete, die einer Regel in einer Chain entsprachen, an das DENY-Ziel weitergeleitet werden, welches unbemerkt das Paket ausgelassen hat. Dieses Ziel muss mit iptables auf DROP geändert werden, damit derselbe Effekt erzielt wird.
- *Die Reihenfolge ist wichtig, wenn Optionen in eine Chainregel eingefügt werden.* Bisher war mit ipchains die Reihenfolge der Optionen bei der Eingabe einer Regel nicht so wichtig. Der iptables-Befehl ist ein wenig empfindlicher dafür, an welcher Stelle Optionen eingefügt werden. Sie müssen nun z.B. den Ursprungs- oder Zielport nach dem in einer Chainregel zu verwendenden Protokoll (ICMP, TCP, oder UDP) spezifizieren.
- *Bei der Spezifizierung von Netzwerkschnittstellen, auf die eine bestimmte Regel angewandt werden soll, müssen Sie Eingangsschnittstellen (-i option) nur mit INPUT- oder FORWARD-Chains und Ausgangsschnittstellen (-o option) nur mit FORWARD- oder OUTPUT-Chains verwenden.* Dies ist notwendig, weil OUTPUT-Chains nicht mehr für Eingangsschnittstellen verwendet werden und INPUT-Chains für Pakete, die durch eine Schnittstelle treten, nicht gesehen werden.

Dies sind auf keinen Fall alle Änderungen, da iptables ein von Grund auf neu geschriebener Netzwerkfilter ist. Genauere Einzelheiten finden Sie im *Linux 2.4 Packet Filtering HOWTO* und in den unter Abschnitt 16.5 angegebenen Quellen.

16.3. Mit iptables-Befehlen verwendete Optionen

Regeln, die es ermöglichen, dass Pakete vom Kernel gefiltert werden, werden durch Ausführen des iptables-Befehls erstellt. Beim Verwenden des iptables-Befehls müssen Sie folgende Optionen angeben:

- *Pakettyp* — Diese Option legt fest, welche Art von Paketen der Befehl filtert.
- *Paketquelle oder -ziel* — Diese Option legt fest, welche Pakete vom Befehl auf Grundlage der Paketquelle oder des Paketziels gefiltert werden.
- *Ziel* — Diese Option legt fest, welche Aktion ausgeführt wird, wenn die Pakete die oben genannten Kriterien erfüllen.

Die mit der iptables-Regel verwendeten Optionen müssen logisch gruppiert sein, d.h., auf Grundlage des Zwecks und der Bedingungen der Gesamtregel, damit die Regel gültig ist.

16.3.1. Tabellen

Eine leistungsstarke Eigenschaft von iptables ist die Möglichkeit der Verwendung mehrerer Tabellen, mit denen entschieden wird, wie mit einem speziellen Paket verfahren werden soll. Dank der erweiterbaren Struktur von iptables können bestimmte Tabellen erstellt und im Verzeichnis /etc/modules/<*Kernel-Version*> /kernel/net/ipv4/netfilter/ abgelegt werden, um bestimmte Ziele zu erreichen. <*Kernel-Version*> steht hierbei für die Version des Kernel.

Die Standardtabelle filter enthält die standardmäßig integrierten INPUT-, OUTPUT-, und FORWARD-Chains. Dies ist vergleichbar mit den standardmäßigen Chains, die mit ipchains verwendet werden. iptables enthält jedoch standardmäßig auch zwei zusätzliche Tabellen, die spezifische Vorgänge zum Filtern von Paketen ausführen. Mit der nat-Tabelle können die in Paketen

aufgezeichneten Ursprungs- und Zieladressen verändert werden, und mit der mangle-Tabelle können Pakete in sehr spezieller Weise verändert werden.

Jede Tabelle enthält standardmäßige Chains, die gemäß dem Tabellenzweck nötige Aufgaben ausführen. Sie können aber in jeder Tabelle auf einfache Art und Weise auch neue Chains erstellen.

16.3.2. Struktur

Viele iptables-Befehle haben folgende Struktur:

```
iptables [-t <table-name>] <command> <chain-name> <parameter-1> \
         <option-1> <parameter-n> <option-n>
```

In diesem Beispiel ermöglicht die Option *<table-name>* dem Benutzer, eine andere Tabelle als die standardmäßige filter-Tabelle auszuwählen, die mit dem Befehl verwendet werden soll. Die Option *<command>* löst einen bestimmten Vorgang aus, wie z.B. das Anhängen oder Löschen einer Regel in einer Chain, die in der Option *<chain-name>* spezifiziert ist. Nach der Option *<chain-name>* befinden sich Parameterpaare und Optionen, die letztendlich darüber entscheiden, wie die Regel angewandt wird und was passiert, wenn ein Paket einer Regel entspricht.

Bei der Betrachtung der Struktur eines iptables-Befehls ist es wichtig, daran zu denken, dass sich anders als bei den meisten anderen Befehlen Länge und Komplexität eines iptables-Befehls je nach seinem Zweck verändern können. Ein einfacher Befehl für das Entfernen einer Regel aus einer Chain kann z.B. sehr kurz sein, während ein Befehl für das Filtern von Paketen aus einem bestimmten Sub-Netz aufgrund verschiedener spezifischer Parameter und Optionen sehr lang sein kann. Bei iptables-Befehlen sollten Sie berücksichtigen, dass manche Parameter und Optionen, die verwendet werden, unter Umständen die Notwendigkeit nach sich ziehen, weitere Parameter und Optionen zu erstellen, damit die Anforderungen der ersten Option weiter spezifiziert werden können. Um eine gültige Regel zu erstellen, muss diese weitergeführt werden, bis jeder Parameter und jede Option, die einen weiteren Optionensatz erfordert, erfüllt ist.

Wenn Sie iptables -h eingeben, erhalten Sie eine vollständige Liste der iptables-Befehlsstrukturen.

16.3.3. Befehle

Mit Befehlen wird iptables angewiesen, einen bestimmten Vorgang auszuführen. Nur ein einziger Befehl pro iptables-Befehlszeichenkette ist zugelassen. Mit Ausnahme des Hilfebefehls sind alle Befehle in Großbuchstaben geschrieben.

Die iptables-Befehle sind:

- -A — Hängt die iptables-Regel an das Ende der spezifizierten Chain an. Dies ist der Befehl, mit dem eine Regel einfach hinzugefügt wird, wenn die Reihenfolge der Regeln in der Chain nicht ausschlaggebend ist.
- -C — Kontrolliert eine bestimmte Regel, bevor sie zur benutzerdefinierten Chain hinzugefügt wird. Dieser Befehl kann Ihnen dabei helfen, komplizierte iptables-Regeln zu erstellen, indem er Sie jeweils durch Aufforderungen dazu bringt, zusätzliche Parameter und Optionen einzugeben.
- -D — Entfernt eine Regel in einer bestimmten Chain nach ihrer Ziffer (z.B. 5 für die 5. Regel einer Chain). Sie können ebenfalls die gesamte Regel eingeben, woraufhin iptables dann die entsprechende Regel aus der Chain, mit der die Regel übereinstimmt, entfernt.
- -E — Benennt eine benutzerdefinierte Chain um. Dies hat allerdings keine Auswirkung auf die Tabellenstruktur.

- `-F` — Löscht die gewählte Chain, woraufhin effektiv jede Regel in der Chain entfernt wird. Wenn keine Chain angegeben wird, löscht dieser Befehl jede Regel jeder Chain.
- `-h` — Liefert eine Liste mit Befehlsstrukturen sowie eine kurze Zusammenfassung der Befehlsparameter und -Optionen.
- `-I` — Fügt eine Regel an einem bestimmten Punkt in eine Chain ein, welcher ein ganzzahliger Wert ist. Wenn kein Wert angegeben ist, setzt `iptables` den Befehl an den Anfang der Regelliste.

  
  Achtung

  Achten Sie darauf, welche Option (`-A` oder `-I`) Sie beim Hinzufügen von Regeln verwenden. Die Reihenfolge der Regeln kann sehr wichtig sein, wenn Sie bestimmen, ob ein bestimmtes Paket dieser oder jeder Regel entsprechen soll.
- `-L` — Listet alle Regeln in der nach dem Befehl spezifizierten Chain auf. Um alle Regeln in allen Chains in der Standardtabelle `filter` aufzulisten, spezifizieren Sie nicht eine Chain oder eine Tabelle. Ansonsten sollte folgende Satzstruktur verwendet werden, um die Regeln in einer spezifischen Chain in einer bestimmten Tabelle aufzulisten:
  `iptables -L <chain-name> -t <table-name>`

  Leistungsstarke Optionen für den `-L`-Befehl, die Regelziffern liefern und ausführlichere Regelbeschreibungen ermöglichen, sind unter anderem in Abschnitt 16.3.7 beschrieben.
- `-N` — Erstellt eine neue Chain mit benutzerdefiniertem Namen.
- `-P` — Setzt die standardmäßige Policy für eine bestimmte Chain, damit bei der Durchquerung von Paketen durch eine Chain, die Pakete, wie bei ACCEPT oder DROP, ohne Übereinstimmung mit einer Regel an ein bestimmtes Ziel weitergeleitet werden können.
- `-R` — Ersetzt eine Regel in einer bestimmten Chain. Sie müssen eine Regelnummer nach dem Namen der Chain verwenden, um die Regel zu ersetzen. Die erste Regel einer Chain bezieht sich auf die Regelziffer `1`.
- `-X` — Entfernt eine benutzerdefinierte Chain. Das Entfernen einer integrierten Chain für eine Tabelle ist nicht zugelassen.
- `-Z` — Stellt Byte- und Paketzähler in allen Chains für eine bestimmte Tabelle auf Null.

16.3.4. Parameter

Sobald gewisse `iptables`-Befehle spezifiziert worden sind, einschließlich derer zum Hinzufügen, Anhängen, Entfernen, Einfügen oder Ersetzen innerhalb einer bestimmten Chain, müssen Sie Parameter definieren, um mit der Erstellung einer Paketfilterungsregel beginnen zu können.

- `-c` — Setzt die Zähler für eine bestimmte Regel zurück. Dieser Parameter akzeptiert die `PKTS`- und `BYTES`-Optionen zur Spezifizierung der zurückzusetzenden Zähler.
- `-d` — Stellt Ziel-Hostnamen, IP-Adresse oder Netzwerk eines Pakets ein, das mit der Regel übereinstimmt. Wenn das Paket mit einem Netzwerk übereinstimmt, sind die folgenden Formate für IP-Adressen/Netmasks unterstützt:
  - *`N.N.N.N/M.M.M.M`* — Wobei *`N.N.N.N`* der Bereich der IP-Adresse und *`M.M.M.M`* die Netmask ist.
  - *`N.N.N.N/M`* — Wobei *`N.N.N.N`* der Bereich der IP-Adresse und *`M`* die Netmask ist.
- `-f` — Wendet diese Regel nur auf fragmentierte Pakete an.

  Durch Verwendung der `!`-Option nach diesem Parameter werden nur unfragmentierte Parameter abgefangen.

- `-i` — Setzt die Schnittstelle des Eingangsnetzwerks, z.B. `eth0` oder `ppp0`, die für eine bestimmte Regel benutzt werden soll. Mit `iptables` sollte dieser zusätzliche Parameter nur mit INPUT- und FORWARD-Chains in Verbindung mit der `filter`-Tabelle und der PREROUTING-Chain mit den `nat`- und `mangle`-Tabellen verwendet werden.

  Dieser Parameter unterstützt auch folgende spezielle Optionen:

  - `!` — Weist diesen Parameter an, keine entsprechenden Übereinstimmungen zu suchen bzw. jede spezifizierte Schnittstelle von dieser Regel auszuschließen.
  - `+` — Ein Platzhalterzeichen, das verwendet wird, um alle Schnittstellen zu kontrollieren, die einer bestimmten Zeichenkette entsprechen. Der `-i eth+`-Parameter würde diese Regel z.B. für alle Ethnernet-Schnittstellen Ihres Systems anwenden, aber alle anderen Schnittstellen, wie z.B. `ppp0` auslassen.

  Wenn der `-i`-Parameter ohne Spezifizierung einer Schnittstelle verwendet wird, ist jede Schnittstelle von dieser Regel betroffen.

- `-j` — Weist `iptables` an, ein bestimmtes Ziel zu übergehen, wenn ein Paket einer bestimmten Regel entspricht. Gültige Ziele, die nach der `-j`-Option verwendet werden können, sind unter anderem die Standardoptionen `ACCEPT`, `DROP`, `QUEUE` und `RETURN` sowie erweiterte Optionen, die über Module verfügbar sind, die standardmäßig mit mit dem Red Hat Linux `iptables`RPM-Paket geladen werden, wie z.B. unter anderem `LOG`, `MARK` und `REJECT`. Weitere Informationen zu diesen und anderen Zielen sowie Regeln zu deren Verwendung finden Sie auf der `iptables`-man-Seite.

  Sie können ein Paket, das dieser Regel entspricht, auch an eine benutzerdefinierte Chain außerhalb der aktuellen Chain weiterleiten. Dadurch können Sie andere Regeln auf dieses Paket anwenden und es mit Hilfe spezieller Kriterien noch intensiver filtern.

  Wenn kein Ziel festgelegt ist, bewegt sich das Paket an der Regel vorbei, ohne dass etwas passieren würde. Der Zähler für diese Regel springt jedoch um eine Stelle weiter, so als ob das Paket der festgelegten Regel entsprechen würde.

- `-o` — Setzt die Schnittstelle des Ausgangsnetzwerks für eine bestimmte Regel fest, die nur mit OUTPUT- un d FORWARD-Chains in der `filter`-Tabelle und mit der POSTROUTING-Chain in den `nat`- und `mangle`-Tabellen verwendet werden kann. Die Optionen dieses Parameters sind dieselben wie die des Parameters der Schnittstelle des Eingangsnetzwerks (`-i`).

- `-p` — Setzt das IP-Protokoll für die Regel, die entweder `icmp`, `tcp`, `udp` oder `all` sein kann, um allen möglichen Protokollen zu entsprechen. Außerdem können weniger verwendete Protokolle, die in `/etc/protocols` aufgelistet sind, ebenfalls verwendet werden. Wenn diese Option beim Erstellen einer Regel ausgelassen wird, ist die `all`-Option der Standard.

- `-s` — Setzt die Quelle eines bestimmten Pakets mit Hilfe derselben Satzstrukturen, die der Zielparameter (`-d`) verwendet.

16.3.5. Übereinstimmungsoptionen

Verschiedene Netzwerkprotokolle ermöglichen spezielle Übereinstimmungsoptionen, die auf spezifische Weise gesetzt werden können, um ein bestimmtes Paket mit Hilfe dieses Protokolls zu kontrollieren. Das Protokoll muss natürlich zuerst im `iptables`-Befehl spezifiziert werden, z.B. durch die Verwendung von `-p tcp` *<Protokollname>* (wobei *<Protokollname>* das Ziel-Protokoll ist) die Optionen für dieses Protokoll verfügbar zu machen.

16.3.5.1. TCP-Protokoll

Folgende Übereinstimmungsoptionen stehen für das TCP-Protokoll zur Verfügung (`-p tcp`):

- `--dport` — Setzt den Zielport für das Paket. Für die Konfiguration dieser Option können Sie entweder den Namen eines Netzwerkdienstes verwenden (z.B. `www` oder `smtp`) und eine oder mehrere

Portnummern verwenden. Um die Namen und Alias-Namen der Netzwerkdienste und die Portnummern, die Sie verwenden, nachzulesen, sehen Sie sich bitte die Datei `/etc/services` an. Sie können auch `--destination-port` verwenden, um diese Übereinstimmungsoption zu spezifizieren.

Um eine spezifische Reihe von Portnummern anzugeben, trennen Sie die zwei Ziffern durch einen Doppelpunkt (`:`), z.B.: `-p tcp --dport 3000:3200`. Die längstmögliche Reihe ist `0:65535`.

Sie können auch ein Ausrufezeichen (`!`) als Flag nach der `--dport`-Option verwenden, um `iptables` anzuweisen, alle Pakete, die *nicht* diesen Netzwerkdienst oder diesen Port verwenden, zu kontrollieren.

- `--sport` — Setzt den Ursprungsport des Pakets unter Verwendung der selben Optionen wie `--dport`. Sie können auch `--source-port` verwenden, um diese Übereinstimmungsoption zu spezifizieren.
- `--syn` — Kontrolliert alle TCP-Pakete, die eine Kommunikation initialisieren sollen, allgemein *SYN-Pakete* genannt, auf Übereinstimmung mit dieser Regel. Alle Pakete, die einen Daten-Payload enthalten, werden nicht bearbeitet. Wird ein Ausrufezeichen (`!`) als Flag hinter die `--syn`-Option gesetzt, werden alle Nicht-SYN-Pakete kontrolliert.
- `--tcp-flags` — Ermöglicht die Verwendung von TCP-Paketen mit bestimmten Bits oder Flags, damit sie einer Regel entsprechen. Die Übereinstimmungsoption `--tcp-flags` akzeptiert nachstehend zwei Parameter, die Flags für bestimmte Bits in einer Liste mit Kommatrennung sind. Der erste Parameter ist eine Maske, die die zu untersuchenden Flags des Pakets bestimmt. Der zweite Parameter bezieht sich auf die Flags, die im Paket gesetzt werden müssen, um eine Übereinstimmung zu erhalten.

  Mögliche Flags sind:

  - `ACK`
  - `FIN`
  - `PSH`
  - `RST`
  - `SYN`
  - `URG`
  - `ALL`
  - `NONE`

  Eine `iptables`-Regel, die `-p tcp --tcp-flags ACK,FIN,SYN SYN` enthält, überprüft beispielsweise nur TCP-Pakete, in denen das SYN-Flag aktiviert und die ACK - und FIN-Flags deaktiviert sind.

  Wie bei vielen anderen Optionen auch, wird die Auswirkung der Überprüfungsoptionen durch Einfügen eines Ausrufezeichens (`!`) hinter `--tcp-flags` umgekehrt, so dass für deren Überprüfung die Flags des zweiten Parameters nicht in Reihenfolge gesetzt werden müssen.
- `--tcp-option` — Versucht mit Hilfe von TCP-spezifischen Optionen zu überprüfen, die innerhalb eines bestimmten Pakets aktiviert werden können. Diese Übereinstimmungsoption kann ebenfalls mit dem Ausrufezeichen (`!`) umgekehrt werden.

16.3.5.2. UDP-Protokoll

Für das UDP-Protokoll stehen folgende Übereinstimmungsoptionen zur Verfügung(`-p udp`):

- `--dport` — Spezifiziert den Zielport des UDP-Pakets unter Verwendung von Dienstnamen, Portnummer oder einer Reihe von Portnummern. Die `--destination-port`-Übereinstimmungsoption kann an Stelle von `--dport` benutzt werden.

Vgl. hierzu die --dport-Übereinstimmungsoption in Abschnitt 16.3.5.1 für die verschiedenen Verwendungsmethoden dieser Option.

- --sport — Bestimmt den Ursprungsport des UDP-Pakets unter Verwendung von Dienstnamen, Portnummer oder einer Reihe von Portnummern. Die --source-port-Übereinstimmungsfunktion kann an Stelle von --sport verwendet werden.

  Vgl. hierzu die --dport- Übereinstimmungsfunktion in Abschnitt 16.3.5.1 für die vielen unterschiedlichen Verwendungsmöglichkeiten dieser Option.

16.3.5.3. ICMP-Protokoll

Diese Match-Optionen sind für das Internet Control Message Protocol (ICMP) (-p icmp) verfügbar:

- --icmp-type — Bestimmt den Namen oder die Nummer des ICMP-Typs, der mit der Regel übereinstimmen soll. Durch Eingabe des Befehls iptables -p icmp -h wird eine Liste aller gültigen ICMP-Namen angezeigt.

16.3.5.4. Module mit zusätzlichen Übereinstimmungsoptionen

Zusätzliche Übereinstimmungsoptionen, die sich nicht spezifisch auf ein Protokoll beziehen, sind ebenfalls mithilfe von Modulen verfügbar, die geladen werden, wenn der iptables- Befehl sie aufruft. Um ein Übereinstimmungsmodul anzuwenden, müssen Sie das Modul mit dessen Namen laden, indem beim Erstellen einer Regel der -m <*Modulname*> (wobei <*Modulname*> durch den Namen des Moduls ersetzt wird) in den iptables-Befehl eingefügt wird.

Standardmäßig stehen zahlreiche Module zur Verfügung. Sie können auch Ihre eigenen Module erstellen, um die Funktionalität der Übereinstimmungsoptionen zu erweitern.

Es gibt viele Module; an dieser Stelle werden wir Ihnen allerdings nur die bekanntesten vorstellen.

- limit-Modul — Mit diesem Modul können Sie eine Grenze setzen für die Anzahl der in Übereinstimmung mit einer Regel zu überprüfenden Pakete. Dies ist besonders nützlich, wenn Regelübereinstimmungen protokolliert werden. Auf diese Weise verhindern Sie, dass die zahlreichen übereinstimmenden Pakete Ihre Protokolldateien nicht mit wiederholten Nachrichten überfüllen oder zu viele Systemressourcen beanspruchen.
  - --limit — Bestimmt die Zahl der Übereinstimmungen innerhalb eines bestimmten Zeitraums, der mit einem Anzahl- und Zeitbearbeiter in dem Format <*number*> /<*Zeit*> angegeben wird. Mit --limit 5/hour wird z.B. nur fünf Mal stündlich nach einer Übereinstimmung mit einer Regel gesucht.

    Wenn keine Anzahl- und Zeitarbeiter angegeben sind, wird der Standardwert 3/hour angenommen.
  - --limit-burst — Setzt eine Grenze für die Anzahl von Paketen, deren Übereinstimmung mit einer Regel gleichzeitig geprüft --limit-Option verwendet werden. Man kann außerdem einen maximalen Grenzwert setzen.

    Wenn keine Zahl festgelegt wird, können anfangs nur fünf Pakete in Übereinstimmung mit der Regel überprüft werden.

- state-Modul — Dieses Modul, welches die --state-Übereinstimmungsoptionen definiert, kann ein Paket auf die nachfolgenden, bestimmten Verbindungszustände überprüfen:
  - ESTABLISHED — Das übereinstimmende Paket wird anderen Paketen in einer bestimmten Verbindung zugeordnet.

- INVALID — Das übereinstimmende Paket kann nicht mit einer bekannten Verbindung verknüpft werden.
- NEW — Das übereinstimmende Paket stellt entweder eine neue Verbindung her oder ist Teil einer Zwei-Weg-Verbindung, die vorher nicht gesehen wurde.
- RELATED — Ein übereinstimmendes Paket stellt eine neue Verbindung her, die auf irgendeine Weise mit einer bestehenden Verbindung zusammenhängt.

Die Verbindungsstatus können untereinander miteinander verbunden werden, indem sie durch Kommata voneinander getrennt werden, wie z.B. in `-m state --state INVALID,NEW`.

- mac-Modul — Dieses Modul ermöglicht die Übereinstimmung einer bestimmten Hardware-MAC-Adresse zu überprüfen.

  Das mac-Modul hat folgende Option:

  - --mac-source — Überprüft auf die MAC-Adresse der NIC, welche das Paket gesendet hat. Um eine MAC-Adresse von einer Regel auszuschließen, fügen Sie nach der --mac-source-Übereinstimmungsoption ein Ausrufezeichen (!) hinzu.

Weitere, über Module verfügbare Übereinstimmungsoptionen finden Sie auf der man-Seite zu iptables.

16.3.6. Zieloptionen

Sobald ein Paket mit einer bestimmten Regel übereinstimmt, kann die Regel das Paket an viele verschiedene Ziele senden, an denen dann eventuell weitere Vorgänge erfolgen. Außerdem hat jede Chain ein standardmäßiges Ziel, das verwendet wird, wenn ein Paket keiner Regel entspricht oder wenn in der Regel, mit dem das Paket übereinstimmt, ein Ziel angegeben ist.

Die Folgenden sind die Standardziele:

- *<user-defined-chain>* — *<user-defined-chain>* steht hier für den Namen der benutzerdefinierten Chain. Dieses Ziel leitet das Paket zur Ziel-Chain weiter.
- ACCEPT — Das Paket gelangt erfolgreich an sein Ziel oder an eine andere Chain.
- DROP — Das Paket wird "ausgelassen". Das System, das dieses Paket gesendet hat, wird nicht über das "Ausfallen" des Pakets benachrichtigt.
- QUEUE — Das Paket wird zur Warteschlange für die Bearbeitung durch eine Benutzerraum-Applikation hinzugefügt.
- RETURN — Hält die Überprüfung der Übereinstimmung des Pakets mit Regeln in der aktuellen Chain an. Wenn das Paket mit einem RETURN-Ziel mit einer Regel in einer Chain übereinstimmt, die von einer anderen Chain aufgerufen wurde, wird das Paket an die erste Chain zurückgesendet, damit die Überprüfung wieder dort aufgenommen werden kann, wo sie unterbrochen wurde. Wenn die RETURN-Regel in einer integrierten Chain verwendet wird und das Paket nicht zu seiner vorherigen Chain zurückkehren kann, entscheidet das Standardziel für die aktuelle Chain, welche Maßnahme getroffen wird.

Zusätzlich zu diesen Standardzielen können auch noch verschiedene andere Ziele mit Erweiterungen verwendet werden, sogenannte *Zielmodulen*. Weitere Informationen zu Übereinstimmungsoptionsmodulen finden Sie unter Abschnitt 16.3.5.4.

Es gibt viele erweiterte Zielmodule, von denen sich die meisten auf bestimmte Tabellen oder Situationen beziehen. Einige der bekanntesten Zielmodule, die standardmäßig in Red Hat Linux enthalten sind:

- LOG — Protokolliert alle Pakete, die dieser Regel entsprechen. Da die Pakete vom Kernel protokolliert werden, bestimmt die /etc/syslog.conf-Datei, wo diese Protokolldateien geschrieben werden. Standardmäßig werden sie in der /var/log/messages-Datei abgelegt.

  Nach dem LOG-Ziel können verschiedene Optionen verwendet werden, um die Art des Protokolls zu bestimmen:

  - --log-level — Bestimmt die Prioritätsstufe eines Protokolliervorgangs. Auf der syslog.conf-man-Seite finden Sie eine Liste der Prioritätsstufen.
  - --log-ip-options — Alle in den Kopfzeilen eines IP-Pakets enthaltenen Optionen werden protokolliert.
  - --log-prefix — Fügt beim Schreiben einer Protokollzeile eine Zeichenkette vor der Protokollzeile ein. Es werden bis zu 29 Zeichen nach der --log-prefix- Option akzeptiert. Dies ist auch beim Schreiben von syslog-Filtern im Zusammenhang mit der Paketprotokollierung sehr nützlich.
  - --log-tcp-options — Alle in den Kopfzeilen eines TCP-Pakets enthaltenen Optionen werden protokolliert.
  - --log-tcp-sequence — Schreibt die TCP- Sequenznummer für das Paket in der Protokolldatei.

- REJECT — Sendet ein Fehlerpaket an das System zurück, das das Paket gesendet hat, und lässt dieses dann "aus" (DROP).

  Mit dem REJECT-Ziel kann die --reject-with <*Typ*> -Option verwendet werden, um mehrere Details zusammen mit dem Fehlerpaket zu senden. Die Meldung port-unreachable ist die standardmäßige <*type*>-Fehlermeldung (wobei <*type*> die Art der Zurückweisung angibt), die angezeigt wird, wenn keine andere Option angewandt wurde. Eine vollständige Liste der verwendbaren <*type*>-Optionen finden Sie auf der iptables-man-Seite.

Andere Zielerweiterungen, die für die Maskierung unter Verwendung der nat-Tabelle oder für Paketänderung mithilfe der mangle-Tabelle nützlich sind, finden Sie auf der iptables-man-Seite.

16.3.7. Auflistungsoptionen

Der standardmäßige Auflistungsbefehl iptables -L bietet eine sehr allgemeine Übersicht über die standardmäßigen aktuellen Regel-Chains der Filtertabelle. Es gibt aber auch noch zusätzliche Optionen mit weiteren Informationen:

- -v — Zeigt eine ausführliche Ausgabe an, wie z.B. die Anzahl der Pakete und Bytes, die jede Chain gesehen hat, die Anzahl der Pakete und Bytes, die von jeder Regel auf Übereinstimmung überprüft wurden und auf deren Schnittstellen eine bestimmte Regel angewandt werden.
- -x — Erweitert die Zahlen auf ihre exakten Werte. In einem arbeitenden System kann die Anzahl der Pakte und Bytes, die von einer bestimmten Chain oder Regel gesehen werden, unter Verwendung der Abkürzungen K (Tausender), M (Millionen) und G (Milliarden) am Ende der Zahl wiedergegeben werden. Mit dieser Option muss zwangsläufig die vollständige Zahl angezeigt werden.
- -n — Zeigt IP-Adressen und Portnummern im numerischen Format an, und nicht im standardmäßigen Hostnamen- und Netzwerkdienst-Format.
- --line-numbers — Listet Regeln in jeder Chain in Nähe derer numerischer Reihenfolge in der Chain auf. Diese Option ist nützlich, wenn man versucht, eine bestimmte Regel aus einer Chain zu entfernen oder zu bestimmen, wo eine Regel in einer Chain eingefügt werden soll.
- -t — Gibt einen Tabellennamen an.

16.4. Das Speichern von iptables-Informationen

Regeln, die mit dem iptables-Befehl erstellt wurden, werden nur im RAM gespeichert. Wenn das System nach Erstellung der iptables-Regeln neu gestartet wird, gehen diese verloren. Wenn Sie möchten, dass Netzfilterregeln bei jedem Booten Ihres Systems erneut wirksam werden, müssen Sie sich als root anmelden und folgendes eingeben:

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

Dadurch wird das iptables-Init-Skript angewiesen, das aktuelle /sbin/iptables-save-Programm auszuführen und die aktuelle iptables-Konfiguration in die /etc/sysconfig/iptables-Datei geschrieben. Diese Datei sollte nur von root gelesen werden können.

Beim nächsten Systemstart wendet das iptables-Init-Skript die in /etc/sysconfig/iptables gespeicherten Regeln durch die Verwendung des /sbin/iptables-restore-Befehls erneut an.

Es ist grundsätzlich empfehlenswert, eine neue iptables-Regel immer erst zu testen, bevor sie in die /etc/sysconfig/iptables-Datei eingefügt wird. Sie können die iptables-Regeln aber auch von der Dateiversion eines anderen Systems in diese Datei kopieren, wodurch sie in kurzer Zeit ganze Sätze von iptables-Regeln an verschiedene Rechner verteilen können.

Wichtig

Wenn Sie die /etc/sysconfig/iptables-Datei an andere Rechner verteilen, müssen Sie /sbin/service iptables restart eingeben, damit die neuen Regeln wirksam werden.

16.5. Zusätzliche Informationsquellen

Zusätzliche Informationen zur Paketfilterung mit iptables finden Sie in den weiter unten aufgeführten Quellen.

16.5.1. Installierte Dokumentation

- man iptables — Enthält eine vollständige Beschreibung verschiedener Befehle, Parameter und anderer Optionen.

16.5.2. Hilfreiche Websites

- http://netfilter.samba.org — Enthält ausgewählte Informationen zu iptables sowie FAQ zu spezifischen Problemen, denen Sie unter Umständen begegnen, verschiedene hilfreiche Handbücher von Rusty Russell, dem Linux-IP-Firewall-Warter. In diesen Anleitungen werden Themen, wie z.B. Netzwerkgundlagen, 2.4-Kernel-Paketfilterung und NAT-Konfigurationen besprochen.
- http://www.linuxnewbie.org/nhf/Security/ IPtables_Basics.html — Ein sehr allgemeiner Überblick darüber, wie sich Pakete durch den Linux-Kernel bewegen, plus eine Einleitung zur Erstellung von einfachen iptables-Befehlen.
- http://www.redhat.com/support/resources/networking/firewall.html — Auf dieser Webseite finden Sie die aktuellsten Links zu Informationsquellen zum Thema Paketfilterung.

Kapitel 17.

Kerberos

Kerberos ist ein von MIT erstelltes Authentifizierungsprotokoll für Netzwerke, das geheime Schlüssel zum Sichern von Passwörtern verwendet — ohne Passwörter über das Netzwerk senden zu müssen. Das Authentifizieren mit Hilfe von Kerberos hält effizient unautorisierte Benutzer vom Versuch ab, Passwörter im Netzwerk abzufangen.

17.1. Vorteile von Kerberos

Die meisten herkömmlichen Netzwerksysteme verwenden passwortbasierte Authentifizierungs- schemata. Wenn sich ein Benutzer an einem Netzwerkserver authentifiziert, muss er einen Benutzernamen und Passwort für jeden Dienst angeben, der Authentifizierung erfordert. Unglücklicherweise, erfolgt die Übertragung von Authentifizierungsinformationen bei vielen Diensten im Klartext. Damit ein solches Schemata sicher ist, muss das Netzwerk vor Zugriff von Außen geschützt werden, und alle Computer und Benutzer auf dem Netwerk müssen sicher sein.

Auch wenn dies der Fall sein sollte, ist das Netzwerk erst einmal mit dem Internet verbunden, kann dessen Sicherheit nicht länger angenommen werden. Jeder Hacker, der Zugriff auf das Netzwerk und einen Paket-Analysierer (Packet Sniffer) hat, kann auf diese Weise versendete Passwörter knacken, was Benutzeraccounts und die Integrität der gesamten Sicherheitsinfrastruktur komprimitiert.

Primäres Ziel von Kerberos ist es, die Übertragung der Authentifizierungsinformationen über das Netzwerk zu beseitigen. Die richtige Verwendung von Kerberos vermindert spürbar die Gefahr, die Packet-Sniffer andernfalls für das Netzwerk bedeuten.

17.1.1. Nachteile von Kerberos

Dank Kerberos wird eine Bedrohung, die ganz allgemein für die Sicherheit im Netzwerk besteht, ausgeschaltet. Allerdings kann sich die Implementierung aus folgenden Gründen schwierig gestalten:

- Das Migrieren von Benutzerpasswörtern von einer standardmäßigen UNIX-Passwortdatenbank wie zum Beispiel `/etc/passwd` oder `/etc/shadow` in eine Kerberos-Passwortdatenbank kann langwierig sein, da es zum Durchführen dieser Aufgabe keine automatisierten Mechanismen gibt. Für detailliertere Informationen, sehen Sie Frage Nummer 2.23 in den Kerberos FAQ, Online unter:

  http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html.

- Kerberos ist nur teilweise mit dem Pluggable Authentication Modules-System (PAM-System) kompatibel, das die meisten Server unter Red Hat Linux verwenden. Weitere Informationen hierzu siehe Abschnitt 17.4.

- 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 kann dies aufgrund der Größe wie auch der Häufigkeit, mit der die krb-Bibliotheken aufgerufen werden müssen, recht problematisch sein. Für andere Anwendungen wiederum muss die Art und Weise geändert werden, in der Server und Clients miteinander kommunizieren. Auch dies kann unter Umständen einen zu großen Aufwand bedeuten. Hierbei stellen die Closed Source-Anwendungen ohne standardmäßigen Kerberos-Support den problematischsten Teil dar.

- Kerberos nimmt an, dass Sie sichere Hosts auf einem unsicheren Netzwerk verwenden. Seine wichtigste Aufgabe ist es zu vermeiden, dass Passwörter im Klartext über das Netzwerk versendet werden. Wenn jedoch noch ein anderer als der richtige Benutzer Zugriff auf den Host hat, welcher die Tickets zur Authentifizierung ausstellt — *Key Distribution Center* (*KDC*) genannt — besteht die Gefahr, dass das gesamte Kerberos-Authentifizierungssystem komprimitiert wird.

- Bei Kerberos handelt es sich um eine Alles-oder-Nichts-Lösung. Wenn Sie sich für den Einsatz von Kerberos im Netzwerk entscheiden, müssen Sie sich die Passwörter merken, die an einen Dienst übertragen werden, der Kerberos nicht zur Authentifizierung verwendet. Gleichzeitig besteht die Gefahr, dass die Passwörter von Packet Sniffern erfasst werden. 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*, oder Sie müssen ganz auf die Verwendung dieser Anwendungen in Ihrem Netzwerk verzichten.

17.2. Kerberos-Terminologie

Wie jedes andere System verfügt Kerberos über seine eigene Terminologie zur Definition verschiedener Aspekte des Dienstes. Ehe die Funktionsweise des Dienstes erläutert wird, sollten Sie mit folgenden Begriffen vertraut sein.

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

Eine Datei, die die Schlüssel zum Verschlüsseln der Kommunikation zwischen einem Benutzer und verschiedenen Netzwerkdiensten enthält. Kerberos 5 unterstützt einen Rahmen für die Verwendung anderer Cache-Typen wie zum Beispiel gemeinsam genutzten Speicher. Die Dateien werden allerdings besser unterstützt.

Crypt-Hash

Ein unidirektionaler Hash, der zum Authentifizieren von Benutzern verwendet wird. Auch wenn dies sicherer als Klartext ist, ist das Entschlüsseln für einen erfahrenen Hacker ein Kinderspiel.

GSS-API

Die generische API des Sicherheitsservice [RFC-2743] ist eine Sammlung von Funktionen, welche Sicherheitsservices bereitstellen. Clients können diese Funktionen benutzen um zu Servern, und Server können diese Funktionen benutzen um zu Clients zu authentifizieren, ohne ein spezifisches Wissen der zugrundeliegenden Mechanismen zu benötigen. Sollte ein Netzwerk-Service (wie IMAP) die GSS-API verwenden, kann dieser unter Verwendung von Kerberos authentifizieren.

Key (Schlüssel)

Daten, die zum Verschlüsseln bzw. Entschlüsseln von Daten verwendet werden. Verschlüsselte Daten lassen sich ohne den richtigen Schlüssel nicht bzw. nur durch wirklich leistungfähige Programme zum Herausfinden von Passwörtern entschlüsseln.

Key Distribution Center (KDC)

Ein Dienst, der Kerberos-Tickets ausgibt (normalerweise auf dem gleichen Host wie Ticket Granting Server)

Key Table oder Keytab

Eine Datei, die eine unverschlüsselte Liste aller Principals und ihrer Schlüssel enthält. Server holen sich die benötigten Keys aus keytab-Dateien, statt `kinit` zu verwenden. Die standardmäßige keytab-Datei ist `/etc/krb5.keytab`, wobei `/usr/kerberos/sbin/kadmind` der einzige bekannte Service ist, der eine andere Datei verwendet (er verwendet `/var/kerberos/krb5kdc/kadm5.keytab`).

`kinit`

Der Befehl `kinit` erlaubt einem Principal, welcher bereits angemeldet ist, das anfängliche Ticket Granting Ticket (TGT) zu erhalten und im Cache abzulegen. Für mehr zur Verwendung des Befehls `kinit`, sehen Sie dessen man-Seite.

Principal

Ein eindeutiger Name für einen Benutzer oder Service, der sich mit Hilfe von Kerberos authentifizieren kann. Der Name eines Principal hat das Format `root[/instance]@REALM`. Bei einem typischen Benutzer entspricht root der Login-ID, während `instance` optional ist. Wenn der Principal über eine Instanz verfügt, ist diese von root durch einen Schrägstrich ("/") getrennt. Bei leerem String ("") handelt es sich zwar um eine gültige Instanz (die sich von der Standardinstance *NULL* unterscheidet), allerdings kann deren Verwendung zu Verwirrung führen. Alle Principals innerhalb eines Realms verfügen über deren eigenen Schlüssel, welcher sich entweder aus deren Passwort ableitet oder bei Services nach dem Zufallsprinzip erzeugt wird.

Realm

Ein Netzwerk, das Kerberos verwendet und aus einem oder einigen Servern (auch als KDCs bezeichnet) sowie einer potenziell sehr großen Zahl von Clients besteht.

Service

Ein Programm, auf das über das Netzwerk zugegriffen wird.

Ticket

Ein temporärer Satz an elektronischen Berechtigungsnachweisen, die die Identität eines Client für einen bestimmten Dienst verifizieren.

Ticket Granting Service (TGS)

Ein Server, der Benutzern der Reihe nach Tickets für den Zugriff auf den gewünschten Service ausgibt. TGS wird üblicherweise auf demselben 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.

Unencrypted Password

Ein im Klartext lesbares Passwort.

17.3. Funktionsweise von Kerberos

Kerberos unterscheidet sich von anderen Authentifizierungsmethoden. Die Authentifizierung erfolgt nicht von jedem Benutzer zu jedem Netzwerk-Service, anstelle verwendet Kerberos die symmetrische Verschlüsselung und einen vertrauenswürdigen Dritten — das so genannte Key Distribution Center oder KDC — um Benutzer auf einem Netzwerk für mehrere Dienste zu authentifizieren. Nach der Authentifizierung speichert Kerberos ein für diese Sitzung spezifisches Ticket auf dem Rechner des

Benutzers. Kerberisierte Dienste suchen dieses Ticket, bevor sie den Benutzer zur Authentifizierung mittels eines Passwortes auffordern.

Wenn sich ein Benutzer in einem kerberisierten Netzwerk an seiner Workstation anmeldet, wird sein Principal für die Anforderung eines Ticket Granting Ticket (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 Schlüssels und sendet es an den Benutzer zurück.

Das Anmeldeprogramm auf dem Client oder `kinit` entschlüsselt das TGT mit Hilfe des Benutzerschlüssels (den es aus dem Passwort des Benutzers errechnet). Der Benutzerschlüssel wird lediglich auf der Client-Maschine benutzt und wird *nicht* über das Netzwerk versendet.

Das TGT ist nur eine bestimmte Zeitspanne gültig und wird im Credential-Cache des Client gespeichert. Die Gültigkeitsdauer ist so eingerichtet, dass ein TGT immer nur während einer bestimmten Zeitspanne verwendet werden kann. Ist das TGT erst einmal erstellt, muss der Benutzer das Passwort für das KDC bis zum Ablauf der Gültigkeit des Passworts nicht erneut eingeben bzw. bis sich der Benutzer ab- und neu anmeldet.

Wenn der Benutzer auf einen Netzwerkdienst zugreifen möchte, verwendet der Client das TGT, um vom Ticket Granting Service (TGS) ein Ticket für den Service anzufordern, der auf dem KDC ausgeführt wird. Der TGS stellt ein Ticket für den gewünschten Service aus, das zur Authentifizierung des Benutzers verwendet wird.

Warnung

Das Kerberos-System kann jederzeit kompromitiert werden, wenn ein Benutzer auf dem Netzwerk gegen einen nicht kerberisierten Service authentifiziert und ein Passwort als Klartext gesendet wird. Von der Verwendung von nicht kerberisierten Services wird daher abgeraten. Diese Services umfassen Telnet und FTP. Andere sichere Protokolle wie zum Beispiel SSH oder SSL Secured Services können dagegen verwendet werden.

Dies ist selbstverständlich nur ein grober Überblick über die typische Funktionsweise der Kerberos-Authentifizierung in einem Netzwerk. Weiterführende Informationen zur Kerberos-Authentifizierung finden Sie unter Abschnitt 17.7.

Anmerkung

Kerberos benötigt verschiedene Netzwerk-Services, um fehlerfrei zu arbeiten. Zunächst ist für Kerberos eine Zeitsynchronisierung zwischen den Rechnern im Netzwerk erforderlich. Für das Netzwerk sollte daher ein Programm zur Zeitsynchronisierung wie zum Beispiel `ntpd` eingerichtet werden. Für weiterführende Informationen zum Konfigurieren von `ntpd`, und zum Einrichten von NTP (Network Time Protocol) Servern, sehen Sie `/usr/share/doc/ntp-<version-number>/index.htm`.

Da Kerberos zum Teil auch auf den Domain Name Service (DNS) angewiesen ist, müssen Sie sich außerdem vergewissern, dass die DNS-Einträge und Hosts im Netzwerk richtig eingerichtet sind. Sehen Sie die *Kerberos V5 System Administrator's Guide*, welche unter `/usr/share/doc/krb5-server-<version-number>` in den Formaten PostScript und HTML zur Verfügung steht für mehr Information.

17.4. Kerberos und PAM

Derzeit verwenden die kerberisierten Dienste keinerlei PAM (Pluggable Authentication Modules) — Kerberisierte Server überspringen PAM vollständig. Anwendungen, die PAM verwenden, können Kerberos jedoch zur Authentifizierung nutzen, sofern das Modul `pam_krb5` (im Paket `pam_krb5` enthalten) installiert ist. Das 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 oder über Dienste vorgenommen wird, die GSS-API verwenden, wie z.B. IMAP, kann das Netzwerk als relativ sicher bezeichnet werden.

Administratoren sollten vorsichtig sein, es Benutzern nicht zu erlauben zu den meisten Services mit Kerberos-Passwörtern zu authentifizieren. Viele der von diesen Services verwendeten Protokolle verschlüsseln die Passwörter nicht, bevor sie diese über das Netzwerk versenden. Dies hebt die Vorteile eines Kerberos Systems auf. Benutzern sollte es, zum Beispiel, nicht erlaubt sein, deren Kerberos-Passwörter über Telnet zu authentifizieren.

Im nächsten Abschnitt wird das Einrichten eines Kerberos-Servers beschrieben.

17.5. Konfigurieren eines Kerberos 5-Servers

Installieren Sie zuerst den Server, wenn Sie Kerberos einrichten. Wenn Sie Slave-Server einrichten müssen, finden Sie Detailinformationen zum Festlegen der Beziehungen zwischen den Master- und Slave-Servern im *Kerberos 5 Installation Guide* (im Verzeichnis `/usr/share/doc/krb5-server-<Versionsnummer>`).

Führen Sie diese Schritte aus, um einen Kerberos-Server zu konfigurieren:

1. Stellen Sie sicher, dass die Zeitsynchronisierung und DNS auf dem Server funktionieren, ehe Sie Kerberos 5 installieren. Schenken Sie der Zeitsynchronisierung zwischen dem Kerberos-Server und seinen verschiedenen Clients besondere Aufmerksamkeit. Überschreitet die Zeitdifferenz zwischen der Server- und den Clientuhren fünf Minuten (der Standardwert kann in Kerberos 5 konfiguriert werden), sind die Kerberos-Clients nicht in der Lage, sich am Server anzumelden. Diese Zeitsynchronisierung ist notwendig, um Angreifer davon abzuhalten, ein altes Kerberos-Ticket zu verwenden, um sich als gültigen Benutzer auszugeben.

   Selbst wenn Sie Kerberos nicht verwenden, sollten Sie ein NTP-kompatibles Client-Server-Netzwerk einrichten. Red Hat Linux umfasst das leicht zu installierende `ntp`-Paket. Sehen Sie `/usr/share/doc/ntp-<version-number>/index.htm` für Details zum Einrichten eines NTP Servers und http://www.eecis.udel.edu/~ntp für zusätzliche Informationen zu NTP.

2. Installieren Sie auf dem dafür abgestellten Rechner, auf dem KDC ausgeführt wird, die Pakete `krb5-libs`, `krb5-server` und `krb5-workstation`. Dieser Rechner muss extrem sicher sein — wenn möglich, sollten außer KDC keine anderen Services ausgeführt werden.

   Wenn Sie Kerberos mit einem GUI-Utility verwalten möchten, sollten Sie auch das `gnome-kerberos`-Paket installieren. Es enthält `krb5`, ein GUI-Tool zum Verwalten von Tickets.

3. Bearbeiten Sie die Konfigurationsdateien `/etc/krb5.conf` und `/var/kerberos/krb5kdc/kdc.conf`, um den Realm-Namen sowie die Domäne-Realm-Zuordnungen anzugeben. Ein einfacher Realm kann durch das Ersetzen von Instanzen von *`BEISPIEL.COM`* und *`Beispiel.com`* durch Ihren Domänennamen erstellt werden — beachten Sie die Groß- und Kleinschreibung — sowie durch Ändern des KDC von *`Kerberos.Beispiel.com`* in den Namen des Kerberos-Servers. Hierbei gilt, dass alle Realm-Namen groß und alle DNS-Hostnamen und Domänennamen klein geschrieben werden. Weitere Informationen zum Format dieser Dateien finden Sie auf den jeweiligen man-Seiten.

4. Erstellen Sie die Datenbank mit Hilfe des Dienstprogramms `kdb5_util` von einem Shell-Prompt:

```
/usr/kerberos/sbin/kdb5_util create -s
```

Der Befehl `create` erstellt die Datenbank, die zum Speichern der Schlüssel für den Kerberos-Realm verwendet wird. Der Switch `-s` erzwingt die Erstellung einer *stash*-Datei, in der der Master-Server-Schlüssel gespeichert wird. Ist keine stash-Datei vorhanden, von der der Schlüssel gelesen werden kann, fordert der Kerberos-Server (`krb5kdc`) die Benutzer bei jedem Start zur Eingabe des Passwortes des Master-Servers auf (wodurch der Schlüssel erneut generiert werden kann).

5. Bearbeiten Sie die Datei `/var/kerberos/krb5kdc/kadm5.acl`. Diese Datei wird von `kadmind` zum Ermitteln der Principals mit Zugriff auf die Kerberos-Datenbank sowie deren Zugriffslevel verwendet. Die meisten Organisationen kommen mit einer einzigen Zeile aus:
   ```
   */admin@EXAMPLE.COM  *
   ```

   Die meisten Benutzer werden in der Datenbank durch einen einzelnen Principal dargestellt (mit einer *NULL* oder leeren Instanz wie zum Beispiel *joe@EXAMPLE.COM*). Mit dieser Konfiguration können Benutzer mit einem zweiten Principal mit einer *admin*-Instanz (zum Beispiel *joe/admin@EXAMPLE.COM*) kompletten Zugriff auf die Kerberos-Datenbank des Realm erhalten.

   Sobald `kadmind` auf dem Server gestartet ist, können alle Benutzer auf die Dienste zugreifen, indem sie auf einem beliebigen Client oder Server im Realm `kadmin` ausführen. Allerdings können nur die in der Datei `kadm5.acl` genannten Benutzer die Datenbank ändern - das eigene Passwort ausgenommen.

   

   Anmerkung

   Das `kadmin`-Utility kommuniziert mit dem `kadmind`-Server über das Netzwerk, wobei Kerberos für die Authentifizierung verwendet wird. Sie müssen natürlich den ersten Principal erstellen, ehe Sie eine Verbindung mit dem Server über das Netzwerk herstellen können, um ihn zu verwalten. Erstellen Sie den ersten Principal mit dem Befehl `kadmin.local`, der speziell für den Gebrauch auf demselben Host wie KDC entworfen ist und Kerberos nicht zur Authentifizierung verwendet.

   Geben Sie am KDC-Terminal den folgenden `kadmin.local`-Befehl ein, um den ersten Principal zu erstellen:
   ```
   /usr/kerberos/sbin/kadmin.local -q "addprinc username/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 Principals für Ihre Benutzer mit Hilfe des Befehls `addprinc` mit `kadmin` hinzu. `kadmin` und `kadmin.local` auf dem Master-KDC sind die Befehlszeilenschnittstellen zum KDC. Insofern stehen viele Befehle nach dem Starten des `kadmin`-Programms zur Verfügung. Weitere Informationen finden Sie auf der man-Seite zu `kadmin`.

8. Überprüfen Sie, ob der Server Tickets ausgibt. Führen Sie zuerst `kinit` aus, um ein Ticket zu erhalten, und speichern Sie es in einer Credential-Cache-Datei. Zeigen Sie dann mit `klist` eine Referenzenliste im Cache an und verwenden Sie `kdestroy`, um den Cache sowie die enthaltenen Referenzen zu zerstören.

   

   Anmerkung

   Standardmäßig versucht `kinit`, Sie mit Hilfe des Anmeldenamens des Kontos zu authentifizieren, das Sie zur ersten Anmeldung am System verwendeten (nicht am Kerberos-Server). Entspricht der Systembenutzername keinem Principal in der Kerberos- Datenbank, erhalten

Sie eine Fehlermeldung. Geben Sie in diesem Fall `kinit` den Namen Ihres Principal als Argument auf der Befehlszeile an (`kinit` *`Principal`*).

Wenn Sie oben genannte Schritte ausgeführt haben, sollte Ihr Kerberos-Server korrekt funktionieren. Anschließend müssen Sie den Kerberos-Client einrichten.

17.6. Konfigurieren eines Kerberos 5-Clients

Das Einrichten eines Kerberos 5-Client ist wesentlich einfacher als das Einrichten eines Servers. Sie sollten zumindest die Clientpakete installieren und den Clients eine gültige `krb5.conf`-Konfigurationsdatei zur Verfügung stellen. Kerberisierte Versionen von `rsh` und `rlogin` erfordern ebenfalls einige Konfigurationsänderungen.

1. Stellen Sie sicher, dass zwischen dem Kerberos-Client und KDC Zeitsynchronisierung vorhanden ist. Weitere Informationen finden Sie unter Abschnitt 17.5. Zudem sollten Sie prüfen, dass DNS auf dem Kerberos-Client fehlerfrei läuft, bevor die Kerberos-Clientprogramme installiert werden.
2. Installieren Sie die Pakete `krb5-libs` und `krb5-workstation` auf allen Client-Rechnern. Für jeden Client müssen Sie eine Version von `/etc/krb5.conf` zur Verfügung stellen; dies kann normalerweise dieselbe `krb5.conf` sein, die von KDC verwendet wird.
3. Ehe eine bestimmte Workstation im Realm Benutzern das Herstellen einer Verbindung mit Hilfe der kerberisierten Befehle `rsh` und `rlogin` erlaubt, muss auf der Workstation zum einen das `xinetd`-Paket installiert sein und zum anderen muss sie ihren eigenen Hostprincipal in der Kerberos-Datenbank haben. Die Serverprogramme `kshd` und `klogind` benötigen ebenfalls Zugriff auf die Schlüssel für den Dienstprincipal.

   Mit Hilfe von `kadmin` fügen Sie einen Hostprincipal für die Workstation auf dem KDC hinzu. Die Instanz ist in diesem Fall der Hostname der Workstation. Sie können die Option `-randkey` für den kadmin-Befehl `addprinc` verwenden, um den Principal zu erstellen und ihm einen zufällig ausgewählten Schlüssel zuzuweisen:

   ```
   addprinc -randkey host/blah.example.com
   ```

   Nachdem der Principal erstellt ist, können Sie die Schlüssel für die Workstation extrahieren, indem Sie `kadmin` *auf der Workstation selbst* ausführen und den Befehl `ktadd` in `kadmin` verwenden:

   ```
   ktadd -k /etc/krb5.keytab host/blah.example.com
   ```
4. Sollten Sie andere kerberisierten Netzwerk-Services benutzen wollen, müssen diese gestartet werden. Folgend ist eine Liste der gebräuchlicheren kerberisierten Services und Anleitungen zum Einschalten dieser:
   - `rsh` und `rlogin` — Um die kerberisierten Versionen von `rsh` und `rlogin` zu verwenden, müssen Sie `klogin`, `eklogin`, und `kshell` aktivieren.
   - Telnet — Um den kerberisierten Befehl `telnet` verwenden zu können, müssen Sie `krb5-telnet` aktivieren.
   - FTP — Zum Bereitstellen von FTP-Zugriff müssen Sie einen Schlüssel für einen Principal mit einem root von `ftp` erstellen und extrahieren. Dabei muss die Instanz auf den Hostnamen des FTP-Servers festgelegt sein. Aktivieren Sie dann `gssftp`.
   - IMAP — Der IMAP-Server, im `imap`-Paket enthalten, verwendet die GSS-API-Authentifizierung unter Verwendung von Kerberos 5, wenn es den richtigen Key in `/etc/krb5.keytab` findet. Der root für den Principal sollte `imap` sein.
   - CVS — CVS's kerberisierter `gserver` verwendet einen Principal mit `cvs` als root. Andernfalls stimmt er mit `pserver` überein.

Für detaillierte Informationen zum Aktivieren von Services, sehen Sie das Kapitel *Zugriffskontrolle für Dienste* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

17.7. Zusätzliche Ressourcen

Weitere Informationen zu Kerberos finden Sie in folgenden Ressourcen.

17.7.1. Installierte Dokumentation

- `/usr/share/doc/krb5-server-<version-number>` — Die *Kerberos V5 Installation Guide* und die *Kerberos V5 System Administrator's Guide* in den Formaten PostScript und HTML. Das `krb5-server`-Paket muss installiert sein.
- `/usr/share/doc/krb5-workstation-<version-number>` — Die *Kerberos V5 UNIX User's Guide* in den Formaten PostScript und HTML. Das `krb5-workstation`-Paket muss installiert sein.

17.7.2. Hilfreiche Webseiten

- http://web.mit.edu/kerberos/www — *Kerberos: The Network Authentication Protocol* Webseite vom 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 — Die 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 — *How to Kerberize your site* ist eine gute Referenz zur Kerberisierung eines Netzwerks.
- http://www.networkcomputing.com/netdesign/kerb1.html — *Kerberos Network Design Manual* gibt eine ausführliche Übersicht über Kerberos.

Kapitel 18.

SSH-Protokoll

SSH™ erlaubt es Benutzern, sich als Remote in Host-Systeme anzumelden. Im Gegensatz zu FTP oder Telnet verschlüsselt SSH die Anmeldung. Auf diese Weise wird das Sicherheitsrisiko für Ihr System und das Remote System reduziert, und Eindringlinge können keine Passwörter im Klartext erkennen.

SSH wurde als Ersatz für ältere, weniger sichere Terminalanwendungen, die zum Anmelden in Remote-Hosts wie **telnet** oder **rsh** verwendet werden, entwickelt. Das Programm `scp` ersetzt ältere Programme, wie **rcp**, die zum Kopieren von Dateien zwischen Hosts verwendet wurden. Da diese älteren Programme Passwörter zwischen dem Client und dem Server nicht verschlüsseln, sollten Sie möglichst vermeiden, sie zu verwenden. Die Verwendung von sicheren Methoden zum Anmelden verringert das Sicherheitsrisiko Ihres Systems und des Systems, in dem Sie sich anmelden.

18.1. SSH-Merkmale

SSH (oder *S*ecure *SH*ell) ist ein Protokoll für die Erstellung einer sicheren Verbindung zwischen zwei Systemen, die eine Client-Server-Architektur verwenden.

Das SSH-Protokoll liefert folgende Schutzmöglichkeiten:

- Nach einer ersten Verbindung prüft der Client, ob er sich auch in der Folge mit dem gleichen Server verbindet.
- Der Client überträgt die Authentifizierungsinformationen in verschlüsselter Form an den Server, unter Verwendung von 128-Bit Verschlüsselung.
- Alle während der Verbindung gesendeten und empfangenen Daten sind mit der 128 Bit-Verschlüsselung so komplex verschlüsselt, dass es äußerst schwierig ist, abgefangene Übertragungen zu entschlüsseln und zu lesen.
- Der Client kann X11 [1] Applikationen vom Server weiterleiten. Diese Technik, *X11 forwarding* genannt, gewährleistet die sichere Verwendung grafischer Applikationen über ein Netzwerk.

Das das SSH Protokoll alles verschlüsselt, können damit unsichere Protokolle verschlüsselt werden. Mit *port forwarding* kann ein SSH Server zum Verschlüsseln unsicherer Protokolle (z.B.POP) verwendet werden und die Sicherheit des Systems und der Daten erhöhen.

Red Hat Linux enthält die allgemeinen OpenSSH Pakete (`openssh`), den OpenSSH Server (`openssh-server`) und Client (`openssh-clients`) Pakete. Weitere Informationen über die Installation und den Gebrauch von OpenSSH finden Sie im Kapitel *OpenSSH* des *Red Hat Linux Handbuchs benutzerdefinierter Konfiguration*. Bitte beachten Sie, dass die OpenSSH-Pakete das OpenSSL-Paket (`openssl`) erfordern. OpenSSL installiert verschiedene wichtige kryptographische Bibliotheken, die OpenSSH bei der Erstellung mit verschlüsselten Meldungen unterstützt.

Eine große Anzahl an Client- und Serverprogrammen können das SSH-Protokoll verwenden, einschließlich vieler Open-Source und kostenlos erhältlicher Anwendungen. Verschiedenste SSH Client-Versionen stehen für fast alle der heute gebräuchlichsten Betriebssysteme zur Verfügung.

---

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.

18.1.1. Wozu dient SSH?

Skrupellosen Computerbenutzern stehen eine Reihe von Tools zur Verfügung, um die Netzwerkkommunikation zu stören, abzufangen und umzuleiten und um auf diese Weise Zugriff auf Ihr System zu erhalten. 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.

  Dieser mögliche Angriff kann durch die Verwendung eines Packet-Sniffers — einem gewöhnlichen Netzwerk-Dienstprogramm gemountet werden.

- *Imitation eines bestimmten Hosts* — Mit dieser Strategie ist ein drittes System so konfiguriert, dass es vorgibt, der eigentliche Empfänger einer Übertragung zu sein. Ist sie erfolgreich, bemerkt das Benutzersystem nicht, dass es mit dem falschen Host kommuniziert.

  Dieser mögliche Angriff kann anhand von Techniken, die unter dem Namen DNS-Poisoning [2] oder IP-Spoofing [3] bekannt sind, gemounted werden.

Bei beiden Methoden werden möglicherweise wichtige Informationen abgefangen. Wenn dies aus unlauteren Gründen erfolgt, können die Ergebnisse katastrophal sein.

Wenn SSH für Fernanmeldungen über eine Shell und für das Kopieren von Dateien verwendet wird, können diese Sicherheitsrisiken erheblich gemindert werden. Das ist darauf zurückzuführen, dass der SSH-Client und Server digitale Unterschriften verwenden, um gegenseitig ihre Identität zu prüfen. Außerdem sind alle Mitteilungen zwischen Client und Server verschlüsselt. Dabei nutzen auch Versuche, sich als das eine oder andere System auszugeben, nichts, da der Schlüssel hierfür nur dem lokalen und dem remote-System bekannt ist.

18.2. SSH Protokoll Versionen

Das SSH-Protokoll erlaubt jedem Client- und Server-Programm, welches zu den Spezifikationen des Protokolls gebaut wurde, sicher zu kommunizieren und austauschbar verwendet werden zu können.

Zur Zeit, gibt es zwei Versionen von SSH. SSH Version 1 verwendet verschiedenste patentierte Verschlüsselungsalgorithmen (einige dieser Patente sind allerdings abgelaufen), hat allerdings ein Sicherheitsrisikio, welches unter Umständen erlaubt Daten in den Datenfluss einzufügen. Die OpenSSH-Suite unter Red Hat Linux verwendet SSH Version 2 bei Default, unterstützt allerdings Version 1.

Wichtig

Es ist empfohlen nur SSH Version 2-kompatible Server und Clients zu verwenden, sofern dies möglich ist.

2. DNS-Poisoning erfolgt, wenn ein Eindringling einen DNS-Server "knackt" und Client-Systeme auf einen böswillig vervielfältigten Host zu lenken.
3. IP-Spoofing erfolgt, wenn ein Eindringling Netzwerk-Pakete versendet, die irrtümlicherweise von einem vertrauenswürdigen Host auf dem Netzwerk erscheinen.

18.3. Die Abfolge der Vorgänge einer SSH-Verbindung

Die folgende Abfolge von Vorgängen tragen zu einer unversehrten SSH-Kommunikation zwischen zwei Hosts bei:

- Zunächst wird eine sichere Transportschicht geschaffen, die dem Client-System anzeigt, dass es mit dem korrekten Server in Verbindung steht.
- Die Transportschicht zwischen den beiden Rechnern ist mit einer symmetrischen Kodierung verschlüsselt.
- Der Client authentifiziert sich gegenüber dem Server.
- Der Remote-Client kann nun sicher mit dem Remote-Host über die verschlüsselte Verbindung kommunizieren.

18.3.1. Transportschicht

Die wichtigste Aufgabe der Transportschicht ist es, die sichere und verschlüsselte Kommunikation zwischen zwei Rechnern bei und nach der Authentifizierung zu gewährleisten. Die 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 der Schlüssel
- Zu verwendenden Algorithmus für den öffentlichen Schlüssel bestimmen
- Zu verwendenden Algorithmus für die symmetrische Verschlüsselung bestimmen
- Zu verwendenden Algorithmus für die Authentifizierung der Mitteilungen bestimmen
- Zu verwendenden Hash-Algorithmus bestimmen

Beim Austausch der Schlüssel identifiziert sich der Server gegenüber dem Client mithilfe eines eindeutigen *Host-Schlüssel*. Wenn nie zuvor eine Verbindung zwischen dem Client und diesem Server bestanden hatte, ist der Server-Schlüssel dem Client unbekannt, und es wird keine Verbindung hergestellt. OpenSSH umgeht dieses Problem, indem es den Host-Schlüssel des Servers akzeptiert, nachdem der Benutzer benachrichtigt wurde und prüt, dass dieser den neuen Host-Schlüssel akzeptieren 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. Sollte der Host-Schlüssel in Zukunft nicht mehr passen, muss der Benutzer die gespeicherte Version des Client entfernen, bevor eine Verbindung zustande kommen kann.

Achtung

Die von OpenSSH verwendete Kontrolle des Host-Schlüssels 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. Um das zu vermeiden, sollten Sie die Integrität eines neuen SSH-Servers verifizieren, indem Sie sich vor dem ersten Kontakt oder nachdem sich der Host-Schlüssel geändert hat, mit dem Server-Administrator in Verbindung setzen.

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.

Nachdem eine bestimmte Datenmenge mithilfe eines vorgegebenen Schlüssels und Algorithmus übertragen wurde (die genaue Menge hängt von der SSH-Implementation ab), erfolgt ein weiterer Schlüsselaustausch, der wiederum einen neuen Hash-Wert und einen neuen gemeinsam genutzten,geheimen Wert generiert. Auch wenn eine unbefugte Person diese beiden Werte ermitteln sollte, müsste sie diese Information bei jedem neuen Schlüsselaustausch ermitteln um die Verbindung zu überwachen.

18.3.2. Authentifizierung

Nachdem die Transportschicht einen sicheren Kanal 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 Signatur oder die Eingabe eines Passworts). Der Client wird anschließend versuchen, sich anhand einer der unterstützten Methoden gegenüber dem Server zu identifizieren.

SSH Server und Clients 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, wie Host- und Passwort-basierte Authentifizierung, sicher.

18.3.3. Verbindungskanäle

Nach der erfolgreichen Authentifizierung über die SSH- Transportschicht werden mehrere *Kanäle* (channels) unter Verwendung von Multiplexing[4] geöffnet. Jeder der Kanäle bearbeitet die Mitteilungen für eine andere Terminal- oder weitergeleitete X11-Sitzung.

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.

Der Client und Server übertragen automatisch die Eigenschaften jedes Kanals, je nachdem, welche Art von Dienst der Client abruft und wie der Benutzer mit dem Netzwerk verbunden ist. Dadurch ergibt sich eine größere Flexibilität bei der Handhabung der verschiedenen Arten von Remote-Verbindungen ohne die Basis-Infrastruktur des Protokolls ändern zu müssen.

4. 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.

18.4. OpenSSH-Konfigurationsdateien

OpenSSH verfügt über zwei verschiedene Arten von Konfigurationsdateien: eine für Clientprogramme (`ssh`, `scp`, `sftp`) und eine andere für den Server-Daemon (`sshd`).

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

- `moduli` — Hier sind Diffie-Hellmann Gruppen für den Austausch des Diffie-Hellmann Schlüssels enthalten. Wenn der Austausch dieser Schlüssel zu Beginn einer SSH-Sitzung erfolgt, wird ein gemeinsam genutzter, geheimer Wert erstellt, der von keiner Seite allein erstellt werden kann. Dieser Wert wird zur Host-Authentifizierung verwendet.
- `ssh_config` — Hierbei handelt es sich um eine Datei für die Konfiguration des SSH-Clients. Wenn einem Benutzer eine eigene Konfigurationsdatei in seinem Home-Verzeichnis (`~/.ssh/config`) zur Verfügung steht, werden die hier enthaltenen Werte überschrieben.
- `sshd_config` — Die Konfigurationsdatei für den `sshd` Daemon.
- `ssh_host_dsa_key` — Der private DSA-Schlüssel, der vom `sshd` Daemon verwendet wird.
- `ssh_host_dsa_key.pub` — Der öffentliche DSA-Schlüssel, der vom `sshd` Daemon verwendet wird.
- `ssh_host_key` — Der private RSA Schlüssel, der vom `sshd` Daemon für die Version 1 des SSH-Protokolls verwendet wird.
- `ssh_host_key.pub` — Der öffentliche RSA Schlüssel, der vom `sshd` Daemon für die Version 1 des SSH-Protokolls verwendet wird.
- `ssh_host_rsa_key` — Der private RSA Schlüssel, der von `sshd` Daemon für die Version 2 des SSH-Protokolls verwendet wird.
- `ssh_host_rsa_key.pub` — Der öffentliche RSA Schlüssel, der von `sshd` für die Version 2 des SSH-Protokolls verwendet wird.

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

- `authorized_keys` — In dieser Datei ist eine Liste der autorisierten öffentlichen Schlüssel für Server enthalten. Stellt ein Client eine Verbindung zu einem Server her, wird er von diesem durch Prüfen seines unterschriebenen öffentlichen Schlüssels, der in dieser Datei gespeichert ist, authentifiziert.
- `id_dsa` — Diese Datei enthält den privaten Schlüssel des Benutzers.
- `id_dsa.pub` — Der öffentliche DSA- Schlüssel des Benutzers.
- `id_rsa` — Der private RSA-Schlüssel, welcher von `ssh` für Version 2 des SSH-Protokolls verwendet wird.
- `id_rsa.pub` — Der öffentliche RSA-Schlüssel, welcher von `ssh` für Version 2 des SSH-Protokolls verwendet wird.
- `identity` — Der private RSA-Schlüssel, welcher von `ssh` für Version 1 des SSH-Protokolls verwendet wird.
- `identity.pub` — Der öffentliche RSA-Schlüssel, welcher von `ssh` für Version 1 des SSH-Protokolls verwendet wird.
- `known_hosts` — In dieser Datei können die DSA-Host-Schlüssel der Server gespeichert werden, mit denen sich der Benutzer über SSH anmeldet. Diese Datei ist sehr wichtig, um festzustellen, ob der SSH-Client mit dem richtigen SSH-Server verbunden ist.

Wichtig

Wenn der Host-Schlüssel eines SSH-Servers geändert wurde, wird der Client den Benutzer darauf hinweisen, dass die Verbindung nicht fortgesetzt werden kann, bevor nicht der Host-Schlüssel aus der Datei `known_hosts` gelöscht wurde. Dies kann mit einem Texteditor geschehen. Bevor dies geschieht, sollten Sie sich allerdings zuerst mit dem System-Administrator des SSH-Servers in Verbindung setzen, um sicherzustellen, dass der Server nicht kompromitiert wurde.

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

18.5. 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-Sitzungen über einen SSH-Kanal verwaltet werden. Mithilfe von TCP/IP-Forwarding können bisher unsichere Port-Verbindungen zwischen Systemen auf spezifische SSH-Kanäle gemappt werden.

18.5.1. X11 Forwarding

Eine X11-Sitzung über eine bestehende SSH-Verbindung zu öffnen ist so einfach wie das Ausführen eines X-Programms, während Sie bereits einen X-Client auf Ihrem Host ausführen. Wird ein X-Programm von einem 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.

Sie können sich sicherlich vorstellen, wie nützlich X11-Forwarding sein kann. Sie können hiermit zum Beispiel eine sichere, interaktive Sitzung mithilfe von `up2date` auf dem Server erstellen. 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.

18.5.2. Port Forwarding

Mit SSH können Sie unsichere TCP/IP Protokolle via Port Forwarding sichern. Bei dieser Technik wird der SSH-Server zu einer verschlüsselten Verbindung zum SSH-Client.

Beim Port Forwarding wird ein lokaler Port in einem Client zu einem remote Port auf dem Server gemappt. Mit SSH können Sie jeden Port des Servers auf jeden Port des Clients übertragen; die Portnummern müssen hierfür nicht übereinstimmen.

Um einen TCP/IP Port Forwarding Kanal zu erstellen, der nach Verbindungen im lokalen Host sucht, verwenden Sie folgenden Befehl:

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

Anmerkung

Für das Einrichten von TCP/IP-Forwarding-Kanälen für Ports mit weniger als 1024 Zylindern 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 über eine verschlüsselte Verbindung abrufen möchten, verwenden Sie folgenden Befehl:

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

Nachdem TCP/IP-Forwarding zwischen Ihrem Rechner und dem Mailserver eingerichtet wurde, können Sie einen 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 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.example.com:110 other.example.com
```

In diesem Beispiel leiten Sie Ihre POP-Anforderung von Port 1100 Ihres Rechners über die SSH-Verbindung auf Port 22 an den ssh-Server weiter. Anschließend verbindet sich `other.domain.com` mit Port 110 auf `mail.domain.com`, so dass Sie neue E-Mails abrufen können. Beachten Sie, dass bei Verwendung dieser Methode nur die Verbindung zwischen Ihrem System und dem `other.domain.com` SSH Server sicher ist.

Dies 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.

Anmerkung

Die Verwendung von Port 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.

System-Administratoren können diese Funktion auf dem Server deaktivieren, indem sie in der AllowTcpForwarding Zeile `No` in `/etc/ssh/sshd_config` eingeben und den `sshd` Dienst neu starten.

18.6. Anfordern von SSH für Fernverbindungen

Damit SSH Ihre Netzwerkverbindungen effektiv schützt, dürfen Sie keine unsicheren Verbindungsprotokolle wie Telnet und FTP verwenden. Andernfalls wird das Passwort eines Benutzers mithilfe von `ssh` für eine Sitzung zwar geschützt, kann jedoch später, während Sie sich mit Telnet anmelden, erfasst werden.

Einige Dienste zum Deaktivieren enthalten:

- `telnet`
- `rsh`
- `ftp`
- `rlogin`
- `vsftpd`

Deaktivieren Sie unsichere Verbindungsmethoden Ihres Systems mithilfe des Befehlszeilenprogramms `chkconfig`, des ncurses- basierten Programms **ntsysv** oder der grafischen Applikation **Services-Konfigurationstool** (`redhat-config-services`). Alle diese Tools erfordern root-Zugriff.

Weitere Informationen über Runlevels und das Konfigurieren von Diensten mit `chkconfig`, **ntsysv** und **Services-Konfigurationstool** finden Sie im Kapitel *Zugriffskontrolle zu Diensten* des *Red Hat Linux Handbuchs benutzerdefinierter Konfiguration.*

Kapitel 19.

Tripwire

Tripwire Datenintegritäts-Software überwacht die Verlässlichkeit von kritischen Systemdateien und Verzeichnissen, indem es Änderungen dieser erkennt. Es tut dies über eine automatische Verifikation, welche in regelmäßigen Intervallen ausgeführt wird. Sollte Tripwire erkennen, dass eine überwachte Datei geändert wurde, wird es den Systemadministrator per E-Mail benachrichtigen. Da Tripwire feststellen kann, welche Dateien hinzugefügt, geändert oder gelöscht wurden, ist es in der Lage ein schnelles Recovery nach einem unbefugten Eindringen in das System zu ermöglichen, indem es die Anzahl der wiederherzustellenden Dateien klein hält. Diese Eigenschaften machen Tripwire ein ausgezeichnetes Tool für Systemadministratoren zum Überwachen von unbefugten Zugriffen und zum Ermittlen vom Grad des Schadens an den Servern.

Tripwire vergleicht die Dateien und Verzeichnisse mit einer Datenbank aus Speicherplätzen, geänderten Daten sowie anderen Informationen. Die Datenbank enthät *Baselines*, wobei es sich um Momentaufnahmen bestimmter Dateien und Verzeichnisse handelt. Der Inhalt der Baseline-Datenbank sollte erstellt werden, bevor das System das Risiko eines unberechtigten Zugriffs läuft. Nachdem die Baseline-Datenbank erstellt wurde, vergleicht Tripwire dann das aktuelle System mit der Datenbank und liefert einen Bericht aller Änderungen, Zusätze oder Löschvorgänge.

Obwohl Tripwire ein sehr geschätztes Tool für die Prüfung der Sicherheit von Red Hat Linux ist, wird Tripwire nicht von Red Hat, Inc. unterstützt. Für weitere Informationen zu Tripwire, die Tripwire-Projekt-Webseite unter http://www.tripwire.com ist ein guter Platz zum Starten.

19.1. Der Gebrauch von Tripwire

Das folgende Flussdiagramm zeigt, wie Tripwire funktioniert:

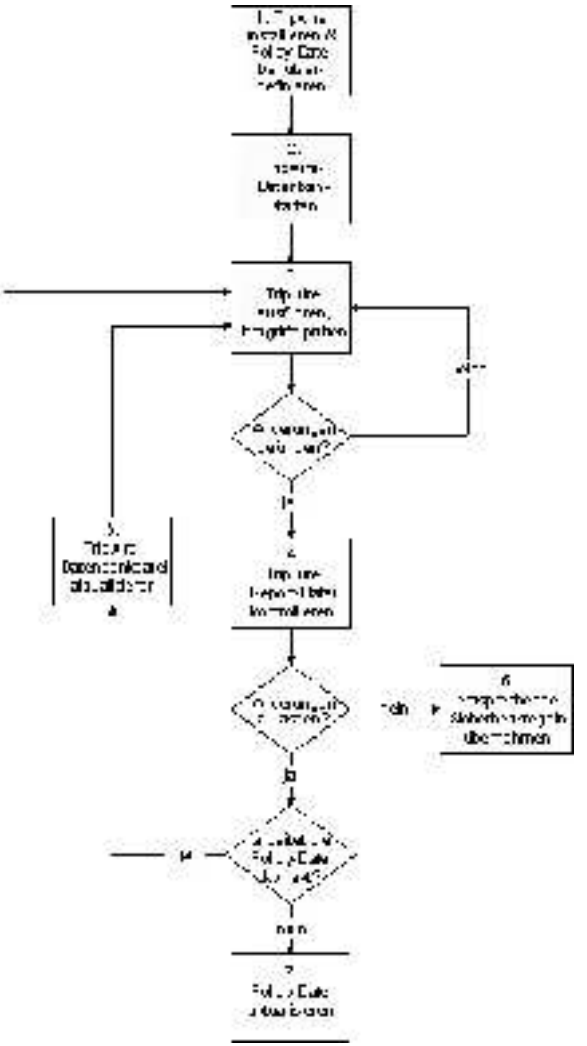

Abbildung 19-1. Der Gebrauch von Tripwire

Folgende Schritte beschreiben im Detail die in Abbildung 19-1 gezeigten numerierten Blöcke.

1. Installieren von Tripwire und benutzerdefiniertes Einstellen der Policy-Datei

Installieren Sie die Tripwire RPM (siehe Abschnitt 19.2). Benutzerdefinieren Sie anschließend die Beispielkonfigurations- und Policydateien (jeweils `/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 19.3.

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 19.4.

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 19.5.

4. Analyse der Tripwire Berichtdatei

Zeigen Sie die Tripwire Berichtdatei mithilfe von `twprint` an, um Differenzen zu ermitteln. Weitere Informationen finden Sie unter Abschnitt 19.6.1.

5. Ergreifen Sie im Falle unberechtigter Intergritätsverletzungen die angemessenen Sicherheitsmaßnahmen.

Wurden überwachte Dateien auf nicht angemessene Weise verändert, können Sie entweder die Originaldateien durch Backup-Kopieren ersetzen und das Programm neu starten oder das Betriebssystem vollkommen neu installieren.

6. Waren die Dateiveränderungen gütig, prüfen und aktualisieren Sie die Tripwire-Datenbankdatei.

Waren die Änderungen an überwachten Dateien beabsichtigt, bearbeiten Sie die Tripwire-Datenbankdatei so, dass sie diese Änderungen in zukünftigen Berichten ignoriert. Weitere Informationen finden Sie unter Abschnitt 19.7.

7. Scheitert die Policy-Datei bei der Prüfung, aktualisieren Sie die Tripwire Policy-Datei.

Um die die Liste der von Tripwire geprüften Dateien oder die Art und Weise ändern möchten, wie Integritätsverletzungen behandelt werden, aktualisieren Sie die Policy-Datei (`/etc/tripwire/twpol.txt`), erstellen eine unterzeichnete Kopie (`/etc/tripwire/tw.pol`) und aktualisieren Sie die Tripwire Datenbank. Weitere Informationen finden Sie unter Abschnitt 19.8.

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

19.2. Installation von Tripwire-RPM

Die einfachste Art, Tripwire zu installieren, ist bei der Installation von Red Hat Linux 9 die Tripwire RPM zu wählen. Sollten Sie Red Hat Linux 9 bereits installiert haben, können Sie `rpm` oder **Paketverwaltungstool** (`redhat-config-packages` verwenden, um Tripwire-RPM von den Red Hat Linux 9 CD-ROMs aus zu installieren.

Wenn Sie sich nicht sicher sind, ob Tripwire installiert ist, geben Sie folgenden Befehl an einem Shell-Prompt ein:

```
rpm -q tripwire
```

Ist Tripwire installiert, erhalten Sie folgende Rückmeldung:

```
tripwire-<version-number>
```

In der vorhergehenden Ausgabe ist *<version-number>* die Versionsnummer des Pakets.

Sollte Tripwire nicht installiert sein, kehrt der Prompt zurück.

Folgende Schritte legen dar, wie Tripwire anhand der RPM-Befehlszeilenanwendung mit CD-ROM gefunden und installiert werden kann:

1. Legen Sie *CD 2* der Red Hat Linux 9 Installations-CD-ROMs ein.
2. Mounted die CD-ROM nicht automatisch, geben Sie folgenden Befehl ein:
   `mount /mnt/cdrom`
3. Prüfen Sie, dass sich die Tripwire RPM auf der CD-ROM befindet, indem Sie eingeben:
   `ls /mnt/cdrom/RedHat/RPMS/ | grep tripwire`

   Befindet sich RPM auf der CD-ROM, zeigt dieser Befehl den Paketnamen an.

   Befindet sich RPM *nicht* auf der CD-ROM, kehrt das Shell-Prompt zurück. In diesem Fall müssen Sie die anderen CDs prüfen und, wenn möglich *CD 1* der Red Hat Linux 9 Installations-CD-ROMs indem Sie zunächst die CD-ROM unmounten und dann die Schritte eins bis drei wiederholen.

   Unmounten Sie die CD-ROM durch Klicken mit der rechten Maustaste auf die CD-ROM-Ikone und wählen Sie **Auswerfen** oder geben Sie folgenden Befehl am Shell-Prompt ein:
   `umount /mnt/cdrom`
4. Nachdem Sie Tripwire RPM gefunden haben installieren Sie ihn durch Eingabe folgenden Befehls als root-Benutzer:
   `rpm -Uvh /mnt/cdrom/RedHat/RPMS/tripwire*.rpm`

Im Verzeichnis `/usr/share/doc/tripwire-<version-number>/` finden Sie Anmerkungen zur Release und README-Dateien für Tripwire. Diese Dokumente enthalten wichtige Informationen zu Standard-Policydateien und anderen Themen.

19.3. Tripwire benutzerdefinieren

Nachdem Sie Tripwire RPM installiert haben, müssen Sie folgende Schritte zur Initialisierung der Software durchführen:

19.3.1. `/etc/tripwire/twcfg.txt` bearbeiten

Obwohl es nicht von Ihnen verlangt wird, diese Beispiel-Tripwire-Konfigurationsdatei zu bearbeiten, könnte es in Ihrer Situation notwendig sein. Sie möchten vielleicht den Speicherplatz der Tripwire-Dateien ändern, E-Mail-Einstellungen benutzerdefinieren oder die Detailebene für Berichte benutzerdefinieren.

Untenstehend befindet sich eine Liste von *erforderlichen* benutzerkonfigurierbaren Variablen in der `/etc/tripwire/twcfg.txt` Datei:

- `POLFILE` — gibt den Speicherplatz der Policy-Datei an; `/etc/tripwire/tw.pol` ist der Standardwert.
- `DBFILE` — gibt den Speicherplatz der Datenbank-Datei an; `/var/lib/tripwire/$(HOSTNAME).twd` ist der Standardwert.
- `REPORTFILE` — gibt den Speicherplatz der Berichtdateien an. Standardmäßig ist dieser Wert auf `/var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr` gesetzt.
- `SITEKEYFILE` — gibt den Speicherplatz der Site-Schlüsseldatei an; `/etc/tripwire/site.key` ist der Standardwert.
- `LOCALKEYFILE` — gibt den Speicherplatz der lokalen Schlüsseldatei an; `/etc/tripwire/$(HOSTNAME)-local.key` ist der Standardwert.

Wichtig

Wenn Sie die Konfigurationsdatei bearbeiten und eine der o.g. Variablen nicht definieren, ist die Konfigurationsdatei ungültig. In diesem Fall erscheint bei Eingabe des Befehls `tripwire` eine Fehlermeldung ausgegeben und die Datei verlassen.

Der Rest der Konfigurationsvariablen in der Beispieldatei `/etc/tripwire/twcfg.txt` sind fakultativ. Dazu gehören folgende:

- `EDITOR` — gibt den von Tripwire aufgerufenen Texteditor an. Standardwert ist `/bin/vi`.
- `LATEPROMPTING` — wenn auf `true` gesetzt, konfiguriert diese Variable Tripwire so, dass Tripwire so lange wie möglich wartet, bevor sie den Benutzer nach einem Passwort fragt und reduziert dabei den Zeitraum währen dem sich das Passwort im Speicher befindet auf ein Minimum. Standardwert ist `false`.
- `LOOSEDIRECTORYCHECKING` — wenn auf `true` gesetzt, konfiguriert diese Variable Tripwire so, dass eine Meldung ausgegeben wird, wenn sich eine Datei in einem beobachteten Verzeichnis ändert, und nicht die Änderung für das Verzeichnis selbst zu melden. Dies begrenzt Überladungen in Tripwire-Berichten. Der Standardwert ist `false`.
- `SYSLOGREPORTING` — wenn auf `true` gesetzt, konfiguriert diese Variable Tripwire so, dass Tripwire über die "Benutzer" Einrichtung Informationen an den Syslog-Daemon meldet. Die Log-Ebene ist auf `notice` gesetzt.Weitere Informationen erhalten Sie auf den man-Seiten `syslogd`. Der Standardwert ist `false`.
- `MAILNOVIOLATIONS` — wenn auf `true` gesetzt, konfiguriert diese Variable Tripwire so, dass Tripwire in regelmäßigen Abständen einen Bericht per E-Mail sendet, unabhängig davon, ob Verletzungen aufgetreten sind oder nicht. Standardwert ist `true`.
- `EMAILREPORTLEVEL` — gibt die Detail-Ebene für gemailte Berichte an. Gültige Werte für diese Variable sind `0` bis `4`. Standardwert ist `3`.
- `REPORTLEVEL` — gibt die Detailebene für Berichte an, die vom `twprint` Befehl erzeugt wurden. Dieser Wert kann auf der Befehlszeile missachtet werden, ist aber standardmäßig auf `3` gesetzt.
- `MAILMETHOD` — gibt an, welches Mail-Protokoll Tripwire verwenden sollte. Gütige Werte sind `SMTP` und `SENDMAIL`. Standardwert ist `SENDMAIL`.
- `MAILPROGRAM` — gibt an, welches Mail-Programm Tripwire verwenden sollte. Standardwert ist `/usr/sbin/sendmail -oi -t`.

Nach Bearbeitung der Beispiel-Konfigurationsdatei müssen Sie die Beispiel-Policydatei konfigurieren.

Warnung

Aus Sicherheitsgründen sollten Sie sämtliche Kopien der reinen Textdatei `/etc/tripwire/twcfg.txt` entweder löschen oder in einem sicheren Speicherplatz hinterlegen nachdem Sie das Installations-Skript ausgeführt oder eine unterzeichnete Konfigurationsdatei neu generiert haben. Alternativ hierzu können Sie die Berechtigungen ändern, so dass sie nicht auf der ganzen Welt lesbar ist.

19.3.2. `/etc/tripwire/twpol.txt` bearbeiten

Obwohl es nicht verlangt wird, sollten Sie diese vielkommentierte Beispiel-Tripwire-Policydatei bearbeiten, um die speziellen Anwendungen, Dateien und Verzeichnisse in Ihrem System in Betracht zu ziehen. Sich allein auf die unveränderte Beispiel-Konfiguration von RPM zu verlassen, könnte eventuell kein ausreichender Schutz für Ihr System sein.

Eine Änderung der Policy-Datei erhöht die Nützlichkeit der Tripwire-Berichte, da falsche Alerts für Dateien und Programme, die Sie nicht verwenden auf ein Minimum reduziert und Funktionalitäten wie E-Mail-Zustellung hinzugefügt werden.

Anmerkung

Zustellung über E-Mail ist nicht standardmäßig konfiguriert. Weitere Informationen zur Konfiguration dieses Merkmals erhalten Sie unter Abschnitt 19.8.1.

Ändern Sie die Beispiel-Policydatei nach Durchführung des Konfigurations-Skripts finden Sie unter Abschnitt 19.8 Anweisungen zur Neugenerierung einer unterzeichneten Policy-Datei.

Warnung

Aus Sicherheitsgründen sollten Sie sämtliche Kopien der reinen Textdatei `/etc/tripwire/twpol.txt` entweder löschen oder in einem sicheren Speicherplatz hinterlegen nachdem Sie das Installations-Skript ausgeführt oder eine unterzeichnete Konfigurationsdatei neu generiert haben. Alternativ hierzu können Sie die Berechtigungen ändern, so dass sie nicht auf der ganzen Welt lesbar ist.

19.3.3. Durchführen des `twinstall.sh` Skripts

Geben Sie als root `/etc/tripwire/twinstall.sh` am Shell-Prompt ein um das Konfigurations-Skript durchzuführen. Das `twinstall.sh` Skript fragt Sie nach den lokalen und Site-Passworten. Diese Passwörter werden dazu verwendet, kryptographische Schlüssel zum Schutz der Tripwire-Dateien zu generieren. Das Skript erstellt und unterzeichnet daraufhin diese Dateien.

Bei der Auswahl der lokalen und Site-Passwörter sollten sie folgende Richtlinien befolgen:

- Verwenden Sie mindestens acht alphanumerische und symbolische Zeichen, aber überschreiten Sie 1023 nicht für die einzelnen Passwörter.
- Verwenden Sie keine Anführungszeichen im Passwort.
- Die Tripwire-Passwörter sollten sich vollkommen vom root oder allen anderen Passwörtern des Systems unterscheiden.
- Verwenden Sie sowohl für den Site-Schlüssel als auch für den lokalen Schlüssel einmalige Passwörter.

Das Passwort für den Site-Schlüssel schützt die Konfigurations- und Policy-Dateien von Tripwire. Das Passwort für den lokalen Schlüssel schützt die Datenbank- und Bericht-Dateien von Tripwire.

Warnung

Es gibt keine Möglichkeit, eine unterzeichnete Datei zu entschlüsseln, wenn Sie Ihr Passwort vergessen. Wenn Sie Passwörter vergessen, können die Dateien nicht mehr verwendet werden, und Sie müssen das Konfigurations-Skript erneut durchführen.

Durch Verschlüsselung der Konfigurations-, Policy-, Datenbank- und Bericht-Dateien schützt Tripwire sie davor, dass sie jemandem angezeigt werden, der die lokalen und Site-Passwörter nicht kennt. Dies bedeutet, dass selbst wenn eine unbefugte Person root-Zugriff zum System bekommt, wird es ihr nicht gelingen, die Tripwire-Dateien so zu ändern, dass sie nicht mehr gefunden werden.

Nachdem sie verschlüsselt und unterzeichnet wurden, sollten die Konfigurations- und Policy-Dateien, die anhand der Durchführung des `twinstall.sh` Skript generiert wurde, nicht mehr umbenannt oder verschoben werden.

19.4. Initialisieren der Tripwire-Datenbank

Bei der Initialisierung der Datenbank erstellt Tripwire eine Sammlung von Dateisystemobjekten, die auf den Regeln in der Policy-Datei beruhen. Diese Datenbank dient als Basis für Integritätsprüfungen.

Initialsisieren Sie die Tripwire-Datenbank mit folgendem Befehl:

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

Die Ausführung dieses Befehls kann einige Minuten dauern.

Wurden diese Schritte erfolgreich durchgeführt, hat Tripwire einen Basisüberblick Ihres Dateisystems, der zur Prüfung von Änderungen in kritischen Dateien notwendig ist. Nach Initialisierung der Tripwire-Datenbank sollten Sie eine erste Integritätsprüfung durchführen. Diese Prüfung sollte erfolgen bevor der Computer an das Netzwerk angeschlossen wird und zu Arbeiten anfängt. Anweisungen dazu finden Sie unter Abschnitt 19.5.

Nachdem Tripwire zu Ihrer Zufriedenheit konfiguriert wurde, kann der Rechner mit seiner Arbeit beginnen.

19.5. Ausführen einer Integritätsprüfung

Standardmäßig fügt Tripwire RPM dem `/etc/cron.daily/` Verzeichnis ein Shell-Skript mit dem Namen `tripwire-check` hinzu. Dieses führt automatisch ein Mal täglich eine Integritätsprüfung durch.

Sie können jedoch durch Eingabe des folgenden Befehls jederzeit eine Tripwire-Integritätsprüfung durchführen:

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

Bei der Integritätsprüfung vergleicht Tripwire den aktuellen Stand der Dateisystem-Objekte mit den in der Datenbank gespeicherten Eigenschaften. Eventuelle Differenzen werden ausgedruckt, und in `/var/lib/tripwire/report/` wird eine verschlüsselte Kopie des Berichtes erstellt. Sie können den Bericht anhand des Befehls `twprint` wie in Abschnitt 19.6.1 angegeben, anzeigen.

Wünschen Sie, dass Ihnen eine E-Mail zugestellt wird, wenn bestimmte Arten von Differenzen bei der Integritätsprüfung ermittelt wurden, kann dies in der Policy-Datei konfiguriert werden. Hinweise dazu, wie dieses Merkmal eingerichtet und getestet werden kann, finden Sie in Abschnitt 19.8.1.

19.6. Untersuchen von Tripwire-Berichten

Der Befehl `/usr/sbin/twprint` wird dazu verwendet, verschlüsselte Tripwire-Berichte und Datenbanken anzuzeigen.

19.6.1. Anzeige von Tripwire-Berichten

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:

```
/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
```

19.6.2. 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 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.

19.7. Aktualisieren der Tripwire Datenbank

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 korrekt auf Differenzen bei der Integritätsprüfung 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, das Programm neu installieren oder im Ernstfall das Betriebssystem vollkommen neu installieren. müssen.

Um Ihre Tripwire dahingehend zu aktualisieren, dass sie gültige Policy-Differenzen akzeptiert, vergleicht Tripwire zunächst eine Berichtdatei mit der Datenbank und integriert sie daraufhin mit gültigen Differenzen aus der Berichtdatei. Achten Sie darauf, beim Aktualisieren der Datenbank den neuesten Bericht zu verwenden.

Verwenden Sie folgenden Befehl, um die Tripwire-Datenbank zu aktualisieren, wobei *Name* der Name der neuesten Berichtdatei ist:

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

Tripwire zeigt die gewünschte Berichtdatei 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.

Wichtig

Wichtig ist, dass Sie nur *autorisierte* Integritätsdifferenzen in der Datenbank ändern.

Alle der Tripwire Datenbank vorgelegten Aktualisierungen sind mit einem `[x]` vor dem Dateinamen gekennzeichnet, ähnlich, wie im folgenden Beispiel:

```
Added:
[x] "/usr/sbin/longrun"

Modified:
[x] "/usr/sbin"
[x] "/usr/sbin/cpqarrayd"
```

Möchten Sie ausdrücklich ausschließen, dass eine gültige Differenz der Tripwire-Datenbank aufgenommen wird, entfernen Sie das `x`.

Um Dateien im standardmäßigen Texteditor `vi` zu bearbeiten, geben Sie `i` ein und drücken [Enter] um den Eingabemodus einzugeben und nehmen Sie die notwendigen Änderungen vor. Wenn Sie fertig sind, drücken Sie den Schlüssel [Esc], geben Sie `:wq` ein und drücken Sie [Enter].

Nachdem der Editor geschlossen wurde, geben Sie Ihr lokales Passwort ein. Daraufhin wird die Datenbank neu erstellt und unterzeichnet.

Nachdem eine neue Tripwire Datenbank geschrieben wurde, erscheinen die neu autorisierten Integritätsdifferenzen nicht mehr als Warnmeldungen.

19.8. Aktualisieren der Tripwire-Policy-Datei

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

Führen Sie zunächst alle notwendigen Änderungen am Beispiel der Policy-Datei (`/etc/tripwire/twpol.txt`) aus. Haben Sie diese Datei gelöscht, (was der Fall sein sollte, wann immer Sie mit der Konfiguration von Tripwire fertig sind), können Sie sie durch Eingabe des folgenden Befehls neu generieren:

```
twadmin --print-polfile > /etc/tripwire/twpol.txt
```

Eine gängige Änderung an dieser Policy-Datei ist das Auskommentieren sämtlicher Dateien, 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 anweisen durch Auskommentieren der entsprechenden Zeile in `twpol.txt` mit dem Zeichen `#`, wie in folgendem Beispiel angegeben, nicht nach dieser Datei zu suchen:

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

Anschließend müssen Sie eine neue, unterzeichnete `/etc/tripwire/tw.pol` Datei und eine aktualisierte Datenbankdatei aufgrund dieser Policy-Information erstellen. Angenommen `/etc/tripwire/twpol.txt` ist die bearbeitete Policy-Datei, verwenden Sie 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 verschlüsselt 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 Tripwire Datenbankdatei den Namen `wilbur.domain.com.twd` trägt:

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

Geben Sie anschließend den Befehl ein, um eine neue Datenbank anhand der aktualisierten Policy-Datei zu erstellen:

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

Um sicherzustellen, dass die Datenbank korrekt geändert wurde, sollten Sie die erste Integritätsprüfung starten und den Inhalt des generierten Berichts kontrollieren. Unter Abschnitt 19.5 und Abschnitt 19.6.1 finden Sie mehr zur Durchführung dieser Aufgaben.

19.8.1. Tripwire und E-Mail

Sie können Tripwire so konfigurieren, dass es eine E-Mail an ein oder mehrere Accounts versendet, wenn eine bestimmte Art der Policy verletzt wurde. Dazu benötigen Sie die Policy-Regel, die überwacht werden soll und den Namen der Person, die die E-Mail bekommen soll, wenn gegen diese Regeln verstoßen wird. Beachten Sie, dass es in großen Systemen mit mehreren Administratoren je nach Art der Differenzen mehrere Personengruppen geben kann, die zu benachrichtigen sind.

Nachdem Sie festgelegt haben, wer zu benachrichtigen ist und welche Regelverstöße gemeldet werden sollen, bearbeiten Sie die Datei `etc/tripwire/twpol.txt` und fügen Sie dann 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, gefolgt von einer oder mehreren E-Mail-Adressen. Es kann mehr als eine E-Mail-Adresse angegeben werden, wenn diese durch ein Semikolon getrennt werden.

Wenn zum Beispiel zwei Administratoren, hier Johnray und Bob, benachrichtigt werden sollen, 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 = johnray@domain.com;bob@domain.com
)
```

Folgen Sie nach Änderung der Policy-Datei den Anweisungen in Abschnitt 19.8 um eine aktualisierte, verschlüsselte und unterzeichnete Kopie der Tripwire Policy-Datei zu erstellen.

19.8.1.1. Senden von Probe-E-Mails

Geben Sie den folgenden Befehl ein, um die Konfiguration der Benachrichtigung von Tripwire E-Mails zu testen:

```
/usr/sbin/tripwire --test --email your@email.address
```

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

19.9. Aktualisieren der Tripwire-Konfigurationsdatei

Wenn Sie die Konfigurationsdatei von Tripwire ändern möchten, sollten Sie zunächst die Beispiel-Konfigurationsdatei `/etc/tripwire/twcfg.txt` bearbeiten. Haben Sie diese Datei gelöscht, (was der Fall sein sollte, wann immer Sie mit der Konfiguration von Tripwire fertig sind), können Sie sie durch Eingabe des folgenden Befehls neu generieren:

```
twadmin --print-cfgfile > /etc/tripwire/twcfg.txt
```

Tripwire erkennt solange keine Änderungen der Konfiguration bis die Konfigurationstextdatei nicht korrekt unterzeichnet und mit dem Befehl `twadmin` in `/etc/tripwire/tw.pol` konvertiert wurde.

Verwenden Sie folgenden Befehl, um eine Konfigurationsdatei aus der Textdatei `/etc/tripwire/twcfg.txt` neu zu generieren:

```
/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 Tripwire-Datenbank neu zu generieren.

19.10. Hinweis zum Tripwire Datei-Speicherplatz

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

- Im Verzeichnis `/usr/sbin` finden Sie folgende Programme:
  - `tripwire`
  - `twadmin`
  - `twprint`

- Im Verzeichnis `/etc/tripwire/` finden Sie folgende Dateien:
  - `twinstall.sh` — Initialisierungs-Skript für Tripwire.
  - `twcfg.txt` — Von Tripwire RPM gelieferte Beispielkonfigurationsdatei.
  - `tw.cfg` — Vom `twinstall.sh` Skript erstellte unterzeichnete Konfigurationsdatei.
  - `twpol.txt` — Von Tripwire RPM gelieferte Beispiel-Policy-Datei.
  - `tw.pol` — Vom `twinstall.sh` Skript erstellte unterzeichnete Policy-Datei.
  - Schlüsseldateien — Vom Skript `twinstall.sh` erstellte Lokal-und Site-Schlüssel, die mit einer `.key` Dateierweiterung enden.

- Nach Durchführen des `twinstall.sh` Installationskripts finden Sie folgende Dateien im `/var/lib/tripwire/` Verzeichnis:
  - Tripwire-Datenbank — Datenbank Ihrer Systemdateien, die eine `.twd` Dateierweiterung hat.
  - Tripwire-Berichte — Im `report/` Verzeichnis werden Tripwire-Berichte hinterlegt.

Der nächste Abschnitt erklärt Näheres über die Rollen dieser Dateien im Tripwire-System.

19.10.1. Tripwire Komponenten

Die folgende Beschreibung enthält Einzelheiten zu den Rollen, die die im vorhergehenden Abschnitt aufgeführten Dateien im Tripwire-System spielen.

`/etc/tripwire/tw.cfg`

Dies ist die verschlüsselte Tripwire-Konfigurationsdatei, in der systemspezifische Informationen, wie der Speicherplatz von Tripwire-Datendateien, hinterlegt werden. Das `twinstall.sh` Installationsskript und `twadmin` Befehl erzeugen diese Datei anhand von Informationen in der Textversion der Konfigurationsdatei `/etc/tripwire/twcfg.txt`.

Nach Durchführen des Installations-Skripts kann der Systemadministrator die Parameter durch Bearbeiten von `/etc/tripwire/twcfg.txt` ändern und anhand des `twadmin` Befehls eine unterzeichnete Kopie der `tw.cfg` Datei neu erzeugen. Weitere Informationen hierzu finden Sie unter Abschnitt 19.9.

/etc/tripwire/tw.pol

Die aktive Tripwire Policy-Datei ist eine verschlüsselte Datei 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 Beispiel-Text-Policydatei `/etc/tripwire/tw.pol` verwendet, um die aktive Tripwire-Policydatei zu generieren.

Nach Durchführen des Installations-Skripts kann der Systemadministrator die Parameter durch Bearbeiten von `/etc/tripwire/twcfg.txt` ändern und anhand des `twadmin` Befehls eine unterzeichnete Kopie der `tw.cfg` Datei neu erzeugen. Weitere Informationen hierzu finden Sie unter Abschnitt 19.9.

/var/lib/tripwire/host_name.twd

Nach der ersten Initialisierung verwendet Tripwire die Regeln der unterzeichneten Policy-Dateien, um diese Datenbankdatei 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*.

/var/lib/tripwire/report/host_name-date_of_report-time_of_report.twr

Bei der Integritätsprüfung erstellt Tripwire Berichtdateien im `/var/lib/tripwire/report` Verzeichnis. In diesen Dateien sind kurz die Änderungen dargestellt, die während der Intergriätsprüfung nicht den Regeln der Policy-Dateien entsprechen. Tripwire-Berichte werden unter Beachtung folgender Konventionen benannt: *host_name-date_of_report-time_of_report*`.twr`. Diese Berichte führen die Unterschiede zwischen der Tripwire-Datenbank und Ihren aktuellen System-Dateien im Einzelnen auf.

19.11. Zusätzliche Ressourcen

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

19.11.1. Installierte Dokumentation

- `/usr/share/doc/tripwire-`<*Versionsnummer*> — 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.

19.11.2. Hilfreiche Websites

- http://www.tripwire.org — Die Homepage des Tripwire Open Source Projekts. Hier finden Sie die aktuellsten Neuigkeiten über die Anwendung sowie eine hilfreiche FAQ-Liste.
- http://sourceforge.net/project/showfiles.php?group_id=3130 — Diese stellen ein Link her zur neuesten offiziellen Tripwire-Projektdokumentation.

IV. Anhang

Inhaltsverzeichnis

Anhang A.

Allgemeine Parameter und Module

Dieser Anhang soll *einige* der möglichen Parameter erklären, die für bestimmte, häufig verwendete Hardware-Gerätetreiber[1], welche unter Red Hat Linux Kernel-*Module* genannt werden, zur Verfügung stehen. In den meisten Fällen sind diese zusätzlichen Parameter nicht notwendig, da der Kernel das Gerät bereits ohne sie verwenden kann. Es könnte jedoch vorkommen, dass zusätzliche Modul-Parameter notwendig sind, damit ein Gerät richtig arbeitet, oder wenn Sie die Standardparameter für das Gerät überschreiben möchten.

Während der Installation verwendet Red Hat Linux eine eingeschränkte Teilmenge von Gerätetreibern um eine robuste Installationsumgebung zu erzeugen. Obwohl das Installationsprogramm die Installation auf vielen verschiedenen Typen von Hardware unterstützt, sind manche Treiber (einschließlich der Treiber für SCSI-Adapter, Netzwerkkarten und vieler CD-ROMs) nicht in den Linux-Kernel integriert, der vom Installationsprogramm verwendet wird. Anstelle, sind diese als Module verfügbar, welche während dem Bootvorgang vom Benutzer geladen werden müssen. Für Informationen, wo diese zusätzlichen Kernel-Module während dem Installationsprozess gefunden werden können, sehen Sie den Abschnitt über alternative Bootmethoden im Kapitel *Schritte für den erfolgreichen Start* im *Red Hat Linux Installationshandbuch*.

Nach Abschluss der Installation, besteht eine Unterstützung für eine große Anzahl von Geräten durch Kernel-Module.

A.1. Spezifizieren der Modulparameter

In einigen Situationen kann es notwendig sein, Parameter für ein Modul beim Laden dieses anzugeben. Die kann auf zwei verschiedene Arten geschehen:

- Sie können einen vollständigen Parametersatz mit nur einer Anweisung spezifizieren. Der Parameter `cdu31=0x340,0` könnte z.B. mit einem Sony CDU 31 oder 33 am Port 340 ohne IRQ verwendet werden.
- Sie können die Parameter auch individuell spezifizieren. Diese Methode wird benutzt, wenn ein oder mehrere Parameter aus dem ersten Satz nicht benötigt werden. Beispiel: `cdu31_port=0x340 cdu31a_irq=0` kann z.B. als Parameter für das gleiche CD-ROM Laufwerk verwendet werden. Ein *ODER* in den CD-ROM-, SCSI-, und Ethernettabellen in diesem Anhang zeigt an, wo die erste Parameter-Methode aufhört und wo die zweite einsetzt.

Anmerkung

Verwenden Sie nur eine der beiden Methoden zum Laden eines Moduls mit bestimmten Parametern.

Achtung

Wenn ein Parameter Kommas beinhaltet, achten Sie darauf, dass Sie nach dem Komma *KEIN* Leerzeichen setzen.

1. Unter einem *Treiber* versteht man Software, die Ihrem System die Verwendung bestimmter Hardware-Geräte ermöglicht. Ohne den Treiber kann der Kernel die jeweiligen Geräte unter Umständen nicht richtig benutzen.

A.2. CD-ROM-Modulparameter

Anmerkung

Nicht alle aufgeführten CD-ROM-Laufwerke werden unterstützt. Überprüfen Sie daher in der Hardware-Kompatibilitätsliste auf der Website von Red Hat Linux http://hardware.redhat.com, ob Ihr CD-ROM-Laufwerk unterstützt wird.

Selbst wenn die Parameter nach dem Laden der Treiberdiskette spezifiziert werden und das Gerät angegeben wird, *kann* der am häufigsten verwendete Parameter `hd`*`X`*`=cdrom` (wobei *`X`* für den entsprechenden Buchstaben des Laufwerks steht) auch während der Installation am Bootprompt eingegeben werden. Diese Ausnahme von der Regel ist erlaubt, weil dieser Parameter sich auf die im Kernel integrierte Unterstützung von IDI/ATAPI CD-ROMs bezieht, also bereits Teil des Kernels ist.

Die meisten der in den nachfolgenden Tabellen ohne Parameter aufgeführten Module können entweder automatisch die Hardware erkennen, oder Sie müssen die Einstellungen im Modulquellcode manuell ändern und neu kompilieren.

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=*`I/O_Port`*
Sony CDU-31A CD-ROM	`cdu31a.o`	cdu31a=*`I/O_Port`*,*`IRQ`* ***ODER*** cdu31a_port=*`Basisadresse`* cdu31a_irq=*`IRQ`*
Philips/LMS-CD-ROM-Laufwerk 206 mit cm260 Hostadapterkarte	`cm206.o`	cm206=*`I/O_Port`*`,`*`IRQ`*
Goldstar R420 CD-ROM	`gscd.o`	gscd=*`I/O_Port`*
ISP16-, MAD16- oder Mozart-Soundkarte CD-ROM-Schnittstelle (OPTi 82C928 und OPTi 82C929) mit Sanyo/Panasonic-, Sony- oder Mitsumi-Laufwerken	`isp16.o`	isp16=*`I/O_Port`*,*`IRQ`*, *`DMA`*, *`Laufwerktyp`* ***ODER*** isp16_cdrom_base=*`I/O_Port`* isp16_cdrom_irq=*`IRQ`* isp16_cdrom_dma=*`DMA`* isp16_cdrom_type=*`Laufwerktyp`*
Mitsumi CD-ROM, Standard	`mcd.o`	mcd=*`I/O_Port`*,*`IRQ`*
Mitsumi CD-ROM, Experimentalversion	`mcdx.o`	mcdx=*`I/O_Port_1`*,*`IRQ_1`*, *`I/O_Port_N`*,*`IRQ_N`*

Hardware	Modul	Parameter
Optics storage 8000 AT "Dolphin"-Laufwerk, Lasermate CR328A	`optcd.o`	
Parallel-Port IDE-CD-ROM	`pcd.o`	
SB Pro 16-kompatibel	`sbpcd.o`	sbpcd=*I/O_Port*
Sanyo CDR-H94A	`sjcd.o`	sjcd=*I/O_Port* *ODER* sjcd_base=*I/O_Port*
Sony CDU-535 & 531 (einige Procomm-Laufwerke)	`sonycd535.o`	sonycd535=*I/O_Port*

Tabelle A-1. Hardware-Parameter

Nachfolgend einige Beispiele zur Verwendung dieser Module:

Konfiguration	Beispiel
ATAPI CD-ROM, Jumpereinstellung als Master im zweiten IDE- Kanal	hdc=cdrom
nicht-IDE Mitsumi CD-ROM an Port 340, IRQ 11	mcd=0x340,11
Drei nicht-IDE Mitsumi CD-ROM-Laufwerke mit experimentellem Treiber, I/O-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 an Port 220	aztcd=0x220
Panasonic-ähnliche CD-ROM an einer SoundBlaster- Schnittstelle an Port 230	sbpcd=0x230,1
Phillips/LMS cm206 und cm260 an I/O 340 und IRQ 11	cm206=0x340,11
Goldstar R420 an I/O 300	gscd=0x300
Mitsumi-Laufwerk an einer MAD16-Soundkarte an I/O 330 und IRQ 1, DMA-Erkennung	isp16=0x330,11,0,Mitsumi
Sony CDU 531 an I/O 320	sonycd535=0x320

Tabelle A-2. Konfigurationsbeispiele für Hardware-Parameter

Anmerkung

Die meisten neueren Soundblaster-Karten verfügen über IDE-Schnittstellen. Für diese Karten sind keine `sbpcd`-Parameter notwendig; Verwenden Sie nur `hdX`-Parameter (wobei *X* für den entsprechenden Buchstaben des Laufwerks steht).

A.3. SCSI-Parameter

Hardware	Modul	Parameter
Adaptec 28xx, R9xx, 39xx	`aic7xxx.o`	
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`	
Mylex DAC960 RAID Controller	`DAC960.o`	
MCR53c406a-basiertes SCSI	`NCR53c406a.o`	
Initio INI-A100U2W	`a100u2w.o`	a100u2w=*I/O*,*IRQ*, *SCSI_ID*
Adaptec AACRAID	`aacraid.o`	
Advansys SCSI-Karten	`advansys.o`	
Adaptec AHA-152x	`aha152x.o`	aha152x=*I/O*,*IRQ*, *SCSI_ID*
Adaptec AHA 154x amd 631x-basiert	`aha1542.o`	
Adaptec AHA 1740	`aha1740.o`	
Adaptec AHA-274x, AHA-284x, AHA-29xx, AHA-394x, AHA-398x, AHA-274x, AHA-274xT, AHA-2842, AHA-2910B, AHA-2920C, AHA-2930/U/U2, AHA-2940/W/U/UW/AU/, U2W/U2/U2B/, U2BOEM, AHA-2944D/WD/UD/UWD, AHA-2950U2/W/B, AHA-3940/U/W/UW/, AUW/U2W/U2B, AHA-3950U2D, AHA-3985/U/W/UW, AIC-777x, AIC-785x, AIC-786x, AIC-787x, AIC-788x , AIC-789x, AIC-3860	`aic7xxx.o`	
ACARD ATP870U PCI-SCSI-Controller	`atp870u.o`	
Compaq Smart Array 5300 Controller	`cciss.o`	
Compaq Smart/2 RAID Controller	`cpqarray.o`	

Hardware	Modul	Parameter
Compaq FibreChannel Controller	`cpqfc.o`	
Domex DMX3191D	`dmx3191d.o`	
Data Technology Corp DTC3180/3280	`dtc.o`	
DTP-SCSI-Hostadapter (EATA/DMA) PM2011B/9X ISA, PM2021A/9X ISA, PM2012A, PM2012B, PM2022A/9X EISA, PM2122A/9X, PM2322A/9X, SmartRAID PM3021, PM3222, PM3224	`eata.o`	
DTP-SCSI-Adapter PM2011, PM2021, PM2041, PM3021, PM2012B, PM2022, PM2122, PM2322, PM2042, PM3122, PM3222, PM3332, PM2024, PM2124, PM2044, PM2144, PM3224, PM3334	`eata_dma.o`	
Sun Enterprise Network Array (FC-AL)	`fcal.o`	
Future Domain TMC-16*xx* SCSI	`fdomain.o`	
NCR5380 (generischer Treiber)	`g_NCR5380.o`	
ICP RAID Controller	`gdth.o`	
I2O Blocktreiber	`i2o_block.o`	
IOMEGA MatchMaker paralleler SCSI-Anschlussadapter	`imm.o`	
Always IN2000 ISA SCSI-Karte	`in2000.o`	in2000=*`Setupzeichenfolge`*:*`Wert`* *ODER* in2000 *`Setupzeichenfolge=Wert`*
Initio INI-9X00U/UW SCSI-Hostadapter	`initio.o`	
IBM ServeRAID	`ips.o`	
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	
NCR-SCSI-Controller mit 810/810A/815/ 825/825A/860/875/876/895-Chipsätzen	`ncr53c8xx.o`	ncr53c8xx=*`Option1`*:*`Wert1`*, *`Option2`*:*`Wert2`*,... *ODER* ncr53c8xx="*`Option1`*:*`Wert1 option2`*:*`Wert2...`*"
Pro Audio Spectrum/Studio 16	`pas16.o`	
PCI-2000 IntelliCache	`pci2000.o`	

Hardware	Modul	Parameter
PCI-2220I EIDE RAID	`pci2220i.o`	
IOMEGA PPA3 paralleler SCSI-Anschlussadapter	`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-Karten IQ-PCI, IQ-PCI-10, IQ-PCI-D	`qlogicisp.o`	
Qlogic ISP1020 SCSI SBUS	`qlogicpti.o`	
Future Domain TMC-885, TMC-950 Seagate ST-01/02, Future Domain TMC-8*xx*	`seagate.o`	controller_type=2 base_address=*Basisadresse* irq=*IRQ*
Karten mit dem sym53c416-Chipsatz	`sym53c416.o`	sym53c416=*PORTBASIS*,*[IRQ]* *ODER* sym53c416 io=*PORTBASIS* irq=*IRQ*
Trantor T128/T128F/T228 SCSI-Hostadapter	`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-Serie	`wd7000.o`	

Tabelle A-3. SCSI-Parameter

Nachfolgend einige Beispiele zur Verwendung dieser Module:

Konfiguration	Beispiel
Adaptec AHA1522 an Port 330, IRQ 11, SCSI ID 7	aha152x=0x330,11,7
Adaptec AHA1542 an Port 330	bases=0x330
Future Domain TMC-800 an CA000, IRQ 10	controller_type=2 base_address=0xca000 irq=10

Tabelle A-4. Konfigurationsbeispiele für SCSI-Parameter

A.4. Ethernet-Parameter

Wichtig

Die meisten modernen Ethernet-basierten Netzwerk-Schnittstellen-Karten (NICs), erfordern keine Modul-Parameter um Einstellungen zu ändern. Diese können Anstelle mit `ethtool` oder `mii-tool` konfiguriert werden. Nur wenn der Versuch mit diesen Tools fehlschlägt, sollten Modul-Parameter angepasst werden.

Zu Information über die Verwendung dieser Tools, sehen Sie die man-Seiten von `ethtool` und `mii-tool`.

Hardware	Modul	Parameter
3Com 3c501	`3c501.o`	3c501=*I/O_Port,IRQ*
3Com 3c503 und 3c503/16	`3c503.o`	3c503=*I/O_Port*,*IRQ* ***ODER*** 3c503 io=*I/O_Port_1*,*I/O_Port_N* irq=*IRQ_1,IRQ_N*
3Com EtherLink Plus (3c505)	`3c505.o`	3c505=*I/O_Port,IRQ* ***ODER*** 3c505 io=*I/O_Port_1*,*I/O_Port_N* irq=*IRQ_1*,*IRQ_2*
3Com EtherLink 16	`3c507.o`	3c507=*I/O_Port,IRQ* ***ODER*** 3c507 io=*I/O_Port* irq=*IRQ*
3Com EtherLink III	`3c509.o`	3c509=*I/O_Port,IRQ*
3Com ISA EtherLink XL "Corkscrew"	`3c515.o`	
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	full_duplex= *0* ist ausgeschaltet *1* ist eingeschaltet
RTL8139, SMC EZ Card Fast Ethernet	`8139too.o`	
RealTek-Karten mit RTL8129- oder RTL8139 Fast Ethernet-Chipsätzen	`8139too.o`	
Apricot 82596	`82596.o`	
Ansel Communications Model 3200	`ac3200.o`	ac3200=*I/O_Port*,*IRQ* ***ODER*** ac3200 io=*I/O_Port_1*,*I/O_Port_N* irq=*IRQ_1*,*IRQ_N*
Alteon AceNIC Gigabit	`acenic.o`	
Aironet Arlan 655	`arlan.o`	
Allied Telesis AT1700	`at1700.o`	ac1700=*I/O_Port*,*IRQ* ***ODER*** at1700 io=*I/O_Port* irq=*IRQ*

Hardware	Modul	Parameter
Broadcom BCM5700 10/100/1000 Ethernet-Adapter	`bcm5700.o`	
Crystal SemiconductorCS89[02]0	`cs89x0.o`	
EtherWORKS DE425 TP/COAX EISA, DE434 TP PCI, DE435/450 TP/COAX/AUI PCI DE500 10/100 PCI Kingston, LinkSys, SMC8432, SMC9332, Znyx31[45]- und Znyx346 10/100-Karten mit DC21040 (no SROM), DC21041[A], DC21140[A], DC21142, DC21143-Chipsätzen	`de4x5.o`	de4x5=*I/O_Port* *ODER* de4x5 io=*I/O_Port* de4x5 args='eth*X[fdx]* autosense=*MEDIENZEICHENFOLGE*'
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=*I/O_Port*,*IRQ* *ODER* depca io=*I/O_Port* irq=*IRQ*
Digi Intl. RightSwitch SE-X EISA und PCI	`dgrs.o`	
Davicom DM9102(A)/DM9132/ DM9801 Fast Ethernet	`dmfe.o`	
Intel Ether Express/100-Treiber	`e100.o`	e100_speed_duplex=*X* *Wenn X* = 0 = automatisches Finden Geschwindigkeit und Duplex 1 = 10Mbps, half duplex 2 = 10Mbps, full duplex 3 = 100Mbps, half duplex 4 = 100Mbps, full duplex
Intel EtherExpress/1000 Gigabit	`e1000.o`	
Cabletron E2100	`e2100.o`	e2100=*I/O_Port*,*IRQ*,*Mit* *ODER* e2100 io=*I/O_Port* irq=*IRQ* mem=*Mit*
Intel EtherExpress Pro10	`eepro.o`	eepro=*I/O_Port*,*IRQ* *ODER* eepro io=*I/O_Port* irq=*IRQ*

Hardware	Modul	Parameter
Intel i82557/i82558 PCI EtherExpressPro-Treiber	`eepro100.o`	
Intel EtherExpress 16 (i82586)	`eexpress.o`	eexpress=*I/O_Port*,*IRQ* *ODER* eexpress io=*I/O_Port* irq=*IRQ* options= 0x10 10base T half duplex 0x20 10base T full duplex 0x100 100base T half duplex 0x200 100baseT full duplex
SMC EtherPower II 9432 PCI (83c170/175 EPIC-Serie)	`epic100.o`	
Racal-Interlan ES3210 EISA	`es3210.o`	
ICL EtherTeam 16i/32 EISA	`eth16i.o`	eth16i=*I/O_Port*,*IRQ* *ODER* eth16i ioaddr=*I/O_Port* IRQ=*IRQ*
EtherWORKS 3 (DE203, DE204 und DE205)	`ewrk3.o`	ewrk=*I/O_Port*,*IRQ* *ODER* ewrk io=*I/O_Port* irq=*IRQ*
A Packet Engines GNIC-II Gigabit	`hamachi.o`	
HP PCLAN/plus	`hp-plus.o`	hp-plus=*I/O_Port*,*IRQ* *ODER* hp-plus io=*I/O_Port* irq=*IRQ*
HP LAN-Ethernet	`hp.o`	hp=*I/O_Port*,*IRQ* *ODER* hp io=*I/O_Port* irq=*IRQ*
100VG-AnyLan-Netzwerkadapter HP J2585B, J2585A, J2970, J2973, J2573 Compex ReadyLink ENET100-VG4, FreedomLine 100/VG	`hp100.o`	hp100=*I/O_Port*,*Name* *ODER* hp100 hp100_port=*I/O_Port* hp100_name=*Name*
IBM Token Ring 16/4, Shared-Memory IBM Token Ring 16/4	`ibmtr.o`	ibmtr=*I/O_Port* *ODER* io=*I/O_Port*
AT1500, HP J2405A, die meisten NE2100/clone	`lance.o`	
Mylex LNE390 EISA	`lne390.o`	
NatSemi DP83815 Fast Ethernet	`natsemi.o`	
NE1000 / NE2000 (nicht-pci)	`ne.o`	ne=*I/O_Port*,*IRQ* *ODER* ne io=*I/O_Port* irq=*IRQ*

Hardware	Modul	Parameter
PCI-NE2000-Karten RealTEk RTL-8029, Winbond 89C940, Compex RL2000, PCI NE2000 clones, NetVin, NV5000SC, Via 82C926, SureCom NE34	`ne2k-pci.o`	
Novell NE3210 EISA	`ne3210.o`	
MiCom-Interlan NI5010	`ni5010.o`	
NI5210-Karte (i82586 Ethernet-Chip)	`ni52.o`	ni52=*I/O_Port*,*IRQ* *ODER* ni52 io=*I/O_Port* irq=*IRQ*
NI6510 Ethernet	`ni65.o`	
IBM Olympic-basierter PCI-Token Ring	`olympic.o`	
AMD PCnet32 und AMD PCnetPCI	`pcnet32.o`	
SIS 900/701G PCI Fast Ethernet	`sis900.o`	
SysKonnect SK-98*XX* Gigabit	`sk98lin.o`	
SMC Ultra und SMC EtherEZ ISA-Etherkarte (8K, 83c790)	`smc-ultra.o`	smc-ultra=*I/O_Port*,*IRQ* *ODER* smc-ultra io=*I/O_Port* irq=*IRQ*
SMC Ultra32 EISA-Ethernetkarte (32K)	`smc-ultra32.o`	
Sun BigMac Ethernet	`sunbmac.o`	
Sundance ST201 Alta	`sundance.o`	
Sun Happy Meal Ethernet	`sunhme.o`	
Sun Quad Ethernet	`sunqe.o`	
ThunderLAN	`tlan.o`	
Digital 21x4x Tulip PCI-Ethernetkarten SMC EtherPower 10 PCI(8432T/8432BT) SMC EtherPower 10/100 PCI(9332DST) DEC EtherWorks 100/10 PCI(DE500-XA) DEC EtherWorks 10 PCI(DE450) DEC QSILVER's, Znyx 312 etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	io=*I/O_Port*

Hardware	Modul	Parameter
VIA Rhine PCI Fast Ethernetkarten mit VIA VT86c100A Rhine-II PCI oder 3043 Rhine-I D-Link DFE-930-TX PCI 10/100	via-rhine.o	
AT&T GIS (nee NCR) WaveLan ISA-Karte	wavelan.o	wavelan=*[IRQ,0],io_port, NWID*
WD8003- und WD8013-kompatible Ethernetkarten	wd.o	wd=*I/O_Port*,*IRQ*,*Mit*,*Mit_Ende* *ODER* wd io=*I/O_Port* irq=*IRQ* mem=*Mit* mem_end=*Ende*
Compex RL100ATX-PCI	winbond.o	
Packet Engines Yellowfin	yellowfin.o	

Tabelle A-5. Ethernet-Modulparameter

Nachfolgend einige Beispiele zur Verwendung dieser Module:

Konfiguration	Beispiel
NE2000 ISA-Karte an IO 300 und IRQ 11	ne=0x300,11 ether=0x300,11,eth0
Wavelan-Karte an IO 390, Auto Detect für IRQ und Verwendung von NWID zu 0x4321	wavelan=0,0x390,0x4321 ether=0,0x390,0x4321,eth0

Tabelle A-6. Konfigurationsbeispiele für Ethernet-Parameter

A.4.1. Verwendung mehrerer Ethernet-Karten

Sie können auf einem Rechner mehrere Ethernet-Karten benutzen. Wenn die Karten jeweils mit unterschiedlichen Treibern arbeiten (z.B. einen 3c509 und einen DE425), müssen Sie lediglich `alias` (und ggf. `options`)-Zeilen für jede Karte der `/etc/modules.conf`-Datei hinzufügen. Weitere Informationen finden Sie im Kapitel *Kernelmodule* im *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*.

Wenn zwei Ethernet-Karten denselben Treiber verwenden (z.B. zwei 3c509-Karten oder einen 3c595 und einen 3c905), müssen Sie den beiden Karten entweder in der Optionszeile des Treibers Adressen zuweisen (bei ISA-Karten) oder Sie fügen einfach für jede Karte eine `alias`-Zeile hinzu (bei PCI-Karten).

Weitere Informationen zur Verwendung mehrerer Ethernet-Karten finden Sie unter *Linux Ethernet-HOWTO* unter der URL http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

Stichwortverzeichnis

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

Colophon

Die Red Hat Linux-Handbücher wurden im Format DocBook SGML v4.1 erstellt. Die HTML- und PDF-Formate werden unter Verwendung benutzerdefinierter DSSSL Stylesheets und benutzerdefinierten Jade Wrapper Scripts angelegt. Die DocBook SGML-Dateien wurden in **Emacs** mithilfe von PSGML Mode geschrieben.

Garrett LeSage schuf das Design der Grafiken für Meldungen (Anmerkung, Tipp, Wichtig, Achtung und Warnung). Diese dürfen frei zusammen mit der Red Hat-Dokumentation vertrieben werden.

Das Team der Red Hat Linux-Produktdokumentation besteht aus:

Sandra A. Moore — Verantwortliche Autorin des *Red Hat Linux x86-Installationshandbuch*; Co-Autorin des *Red Hat Linux Handbuch Erster Schritte*

Tammy Fox — Verantwortliche Autorin des *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*; Co-Autorin des *Red Hat Linux Handbuch Erster Schritte*; Autorin/Bearbeiterin der benutzerdefinierten DocBook Stylesheets und Skripte

Edward C. Bailey — Autor des *Red Hat Linux System Administration Primer*; Co-Autor des *Red Hat Linux x86-Installationshandbuch*

Johnray Fuller — Verantwortlicher Autor des *Red Hat Linux Referenzhandbuch*; Co-Autor des *Red Hat Linux Security Guide*; Co-Autor des *Red Hat Linux System Administration Primer*

John Ha — Verantwortlicher Autor des *Red Hat Linux Handbuch Erster Schritte*; Co-Autor des *Red Hat Linux Security Guide*; Co-Autor des *Red Hat Linux System Administration Primer*

Dr. Bernd R. Groh — Verantwortlicher Übersetzer/Bearbeiter des *Red Hat Linux x86-Installationshandbuch*; *Red Hat Linux Handbuch Erster Schritte*; *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*; *Red Hat Linux Referenzhandbuch*

Nadine Richter, Dipl.-Technikübersetzerin (FH) — Verantwortliche Übersetzerin/Bearbeiterin des *Red Hat Linux x86-Installationshandbuch*; *Red Hat Linux Handbuch Erster Schritte*; *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*; *Red Hat Linux Referenzhandbuch*